Residual Risk

An Account of Events in Nuclear Power Plants Since the Chernobyl Accident in 1986

April 2007

Authors

Dr. Georgui Kastchiev
Senior Scientist
Institute of Risk Research, University of Vienna, Austria

Prof. Wolfgang Kromp
Director
Institute of Risk Research, University of Vienna, Austria

Dipl.-Ing. Stephan Kurth
Nuclear Engineering & Plant Safety Division
Öko-Institut (Institute for Applied Ecology), Darmstadt, Germany

Mr. David Lochbaum
Director, Nuclear Safety Project
Union of Concerned Scientists, Washington, D.C., USA

Dr. Ed Lyman
Senior Staff Scientist
Union of Concerned Scientists, Washington, D.C., USA

Dipl.-Ing. Michael Sailer
Deputy Director
Öko-Institut (Institute for Applied Ecology)
Darmstadt, Germany

Mr. Mycle Schneider
International Consultant
Mycle Schneider Consulting, Paris, France

Project Coordinator: **Mycle Schneider**

Commissioned by **Rebecca Harms,** Member of the European Parliament

With the support of: Altner Combecher Stiftung für Ökologie und Frieden and Hatzfeldt Stiftung

The Greens | European Free Alliance
in the European Parliament

Picture credit cover page : Oak Ridge National Laboratory

Download

Please note that the present report can be downloaded free of charge at:

http://www.greens-efa.org/cms/topics/dokbin/181/181995.residual_risk@en.pdf

Contacts

Rebecca Harms MEP
European Parliament
Rue Wiertz 60
B-1074 Brussels
Phone: +32-2-284 5695
E-mail: rharms@europarl.eu.int

MYCLE SCHNEIDER CONSULTING
45, allée des deux cèdres
F-91210 Draveil (Paris)
Phone: +33-1-69 83 23 79
Skype: mycleschneider
E-mail: mycle@wanadoo.fr

Acknowledgments

The coordinator of the Residual Risk Project wishes to thank all of the authors for their combined efforts to bring this endeavour to fruition. Special thanks to John Large who put significant work into peer reviewing the report as well as to Antony Froggatt for additional proof reading. However, the responsibility for any potential errors remain with the authors.

The authors are grateful for any comments you might wish to transmit.

"Die Menschen lernen nur aus Katastrophen. Schade!"
[People only learn from catastrophes. Too bad!]
Graffiti on a wall close to the
Gorleben Nuclear Site
in Germany

Preface

Proponents of nuclear fission are trying to jump on the climate change bandwagon to resuscitate nuclear power after decades of stagnation. Unfortunately, some UN climate change strategists, as well as parts of the European Commission, have bought into the nuclear lobby's arguments. While we clearly need to reform our wasteful and polluting energy industry to meet today's energy and environmental challenges, however, grasping at even more dangerous straws cannot be the answer.

It is wrong to try and counteract the risk of global warming through an expansion of nuclear energy and the consequential nuclear risks. Promoting nuclear as a sustainable energy source, as the nuclear lobby in Brussels and elsewhere is trying to do, is misleading. Any technology that can produce such devastating consequences as those in 1986 from the Chernobyl disaster can never be sustainable. Nuclear energy is a high risk technology.

We can lull ourselves into a false sense of security by trying to forget about past catastrophes. However, the fact that there has not been another accident with a core meltdown since Three Mile Island does not mean that it will never happen again. Every year there are thousands of incidents, occurrences and events in nuclear installations and, simply because there was no catastrophic radioactive leakage, the world reacts as if there was no problem.

The Forsmark incident last summer shattered this complacent approach to nuclear incidents. It may have only been a matter of minutes by which an accident on the scale of Chernobyl was prevented from happening in Sweden. The main difference between Forsmark and previous incidents is that the real risk of Forsmark was publicised, whereas previous incidents were brushed under the table.

The Forsmark incident triggered the commissioning of the 'Residual Risk' Project. Why are there reports on Forsmark but not on Maanshan in Taiwan? Why is it that a hydrogen explosion that threatens safety relevant equipment at the German nuclear power plant Brunsbüttel, did not attract more than regional attention? How long did the huge hole in the reactor vessel head of the American Davis Besse plant remained undiscovered? Who has ever heard the story of the man that, with his vehicle, broke through all the gates at the Three Mile Island (USA) plant, entered the turbine hall and remained undiscovered for four hours? The collective repression of risks also results from lacking, false or incomplete information.

The publication of 'Residual Risk' is aimed at raising public awareness on the risks of nuclear power. It must be taken into consideration that the incidents, which were dealt with by experts from various countries, are not necessarily the most serious

ones that there have been. The incidents presented in the study are particularly significant and they were made public. This illustrates how frequently we have been at the edge of disaster.

The International Atomic Energy Agency (IAEA) created International Nuclear Event Scale (INES) as a communication tool for operators and safety authorities, with incidents classified on a scale from 1 to 7. However, most countries either do not supply any or supply very incomplete information to the system. Moreover, only incidents with radiological impacts are classified in higher categories. Using this method, a 'near miss' can be classified as simply a Level 2 incident. This study shows that the use of the INES scale is misleading and accentuates the tendency to systematically underestimate the risk potential of nuclear incidents.

The permanent risk of a core meltdown is a strong argument against the use of nuclear power. The lifetime extension of nuclear power plants heightens the risk of a major accident considerably. The question of how to dispose of nuclear waste safely not only remains unanswered, no answer can be imagined. Every country using nuclear power could build a nuclear bomb if it decided to do so. These dangers are no less terrifying given the challenges of climate change.

However, there are not only wrong answers. There are also real solutions to climate change. To be able to reduce greenhouse gas emissions and fight climate change, as well as addressing current energy wastage, we need a new approach for a modern and sustainable energy supply. Energy savings and efficiency and an ambitious expansion of renewable energies are the sensible and sustainable solution, as was demonstrated in the Greens study 'Vision Scenario'.
(http://www.greens-efa.org/cms/topics/dokbin/155/155777.a_vision_scenario_for_climate_and_energy@en.pdf)

I hope that the work of the authors of "Residual Risk" will help increase awareness of the inherent risks of nuclear power. I also hope that we will succeed in once and for all ending the discussion about the lifetime extension of nuclear power plants or the construction of new plants.

My thanks go to the team of authors and to the coordinator of the project, Mycle Schneider. Without the financial support of the Altner-Combecher Stiftung für Ökologie und Frieden and Hatzfeldt Stiftung this project could not have been realised.

Rebecca Harms

9 May 2007
Brussels

Residual Risk

An Account of Events in Nuclear Power Plants Since the Chernobyl Accident 1986

Contents

Contents **2**
1. Introduction **4**
1.1 Purpose and background of the study 4
1.2 Overview of status and trends in the nuclear industry with focus on the European Union 6
1.2.1 Nuclear power reactors worldwide 6
1.2.2 Types of nuclear power reactors 8
1.2.3 Nuclear power reactors in the European Union 9
1.2.4 Design and operational safety 10
2. Definitions: Incidents or Accidents? Events! **12**
3. Overview of the Main Causes and Contributing Factors Leading to Nuclear Events. **13**
3.1 Design Faults 14
3.2 Construction and Manufacturing Problems 16
3.3 Material Defects 17
3.4 Failures of Equipment, Components, and Systems 19
3.5 External Events 20
3.6 Internal Events 23
3.6.1 Loss of Coolant Accident (LOCA) 23
3.6.2 Fires 23
3.6.3 Secondary cooling circuit and other pipe failures 24
3.7 Human Errors and Violations of Rules and Procedures 26
3.8 Deficiencies in Documentation 27
3.9 Malicious Impacts 27
3.9.1 Security Failures Prior to the 11 September 2001 Attacks 29
3.9.2 Security Failures After the 11 September 2001 Attacks 30
4. Systemic Issues **33**
4.1 Recurring Events 33
4.2 Violation of Rules and Procedures 36
4.3 Lack of Systematic Verification and Control 38
4.4 Difficulty of Root Cause Identification and Assessments 39
4.5 Generic Faults 40
4.6 Decline in Design and Fabrication quality 41
5. Classification Systems **44**
5.1 The International Nuclear Event Scale (INES) 44
5.2 The US–NRC Incident Reporting System 45
5.3 The German Incident Reporting System 46
6. Role and Problems of Scale – Public Communication or Technical Rating? **47**

7. Gross Event Numbers as Declared by Authorities 48
7.1 Available INES Numbers 48
7.2 IAEA-NEA IRS Statistics 48
7.3 Country statistics 48
7.3.1 Nuclear Event Statistics in the USA 48
7.3.2 Nuclear Event Statistics in France 49
7.3.3 Nuclear Event Statistics in Germany 53
8. Selected incidents and accidents in the USA and France 54
8.2.1 Selected events in the USA 54
8.2.2 Selected events in France 58
9. Residual Risk Project Selection of Nuclear Events 1986-2006 62
9.1 Definition of selection criteria 62
9.2 Selection of events by type of incident 62
9.2.1 Advanced Material Degradation (before break) 63
9.2.1.1 3 April 1991 Shearon Harris (USA) 63
9.2.1.2 6 March 2002 Davis Besse (USA) 63
9.2.2 Significant Primary Coolant Leaks 66
9.2.2.1 18 June 1988, Tihange-1 (Belgium) 66
9.2.2.2 12 May 1998, Civaux-1 (France) 66
9.2.2.3 9 February 1991 Mihama-2 (Japan) 67
9.2.3 Reactivity Risks 68
9.2.3.1 12 August 2001, Philippsburg (Germany) 68
9.2.3.2 1 March 2005 Kozloduy-5 (Bulgaria) 70
9.2.4 Fuel Degradation (outside reactor core) 73
9.2.4.1 Paks (Hungary) 2003 73
9.2.4 Fires and Explosions 78
9.2.4.1 14 December 2001, Brunsbüttel (Germany) 78
9.2.5 Station Blackout 79
9.2.5.1 18 March 2001 Maanshan (Taiwan) 79
9.2.5.2 25 July 2006, Forsmark, Sweden 81
9.2.6 Generic Issues – Reactor Sump Plugging 82
9.2.6.1 28 July 1992, Barseback-2 (Sweden) 83
9.2.7 Natural Events 84
9.2.7.1 27 December 1999, Blayais-2 (France) 84
9.2.8 Security Events and Malicious Acts 86
9.2.8.1 7 February 1993, Three Mile Island (USA) 86
9.2.8.2 July 2000, Farley (USA) 87
9.2.8.3 29 August 2002, 17 TEPCO Reactors (Japan) 88
10. Summary and Conclusions 92
11 Annexes 101
11.1 IAEA International Nuclear Event Scale (INES) 102
11.2 Chronology of Data Falsification at the Fukushima NPP, Japan 107
11.3 Biographical Notes on the Authors 110

1. Introduction

If our understanding of our past is incomplete or inaccurate then we are not well equipped to make sense of the present. More specifically, if we do not make the effort to learn what the influences were that shaped our past, then we are hopelessly unequipped to detect and respond to similar influences today.

For example, to simply characterize the Three Mile Island accident as a minor mechanical failure which was allowed to escalate into a major accident through serious operator errors is a gross and dangerous distortion of the truth, actively concealing important human errors in nuclear plant design organizations, operating utilities and the regulatory authorities. If we cannot identify these errors in the glare of hindsight, then we have little hope of anticipating them in the future.

David Mosey
Nuclear Safety Engineer, Canada
Author of *Nuclear Accidents*[1]

1.1 Purpose and background of the study

Fifty years ago, on 25 March 1957, the EURATOM Treaty was signed. Article 1 stipulates that *"it shall be the task of the Community to contribute to the raising of the standard of living in the Member States and to the development of relations with the other countries by creating the conditions necessary for the speedy establishment and growth of nuclear industries"*. Half a year later, on 10 October 1957, the fire at a Windscale reactor releases large amounts of radioactivity. For the first time, contaminated milk and vegetables had to be destroyed following an accident at a nuclear power plant. Nevertheless, the accident – like many less significant events that followed – had surprisingly little effect on public opinions and on the strategies of government and industry.

The growth of the nuclear industries continued. It is in March 1979, more than twenty years after the Windscale fire, that the core-melt accident at the US Three Mile Island (TMI) plant shocked the world. Thereafter and in response to TMI, the nuclear industry and plant operators implemented massive upgrading programs to operational reactors, plants under construction and those on the drawing board were revised. Nevertheless, no new nuclear plants were ordered in the United States since TMI, over a hundred projects having been abandoned. In the West, by the mid-1980s the nuclear power industry was in stagnation.

Then in 1986 the Chernobyl disaster in the Ukraine, the worst nuclear power plant accident to date, sending radioactive clouds around the planet that hit collective consciousness as *worst-case scenario*.

What happened since Chernobyl? No major accident, no large radioactive release, no massive evacuations, no widespread areas of radiologically contaminated land. So everything is fine? Has the risk from nuclear power plants been mastered and safety been improved to "acceptable standards"?

These are questions that are at the basis of the present study. The authors quickly realized that there are no comprehensive international statistics on incidents and accidents and

[1] David Mosey, *Reactor Accidents,* Second Edition, Nuclear Engineering International, 2006

even definition and safety significance of nuclear “incidents” are highly controversial. Operators and nuclear safety authorities prefer speaking about “events”.

The International Atomic Energy Agency (IAEA), that maintains an international nuclear event database confidential to its members, did not reply to repeated information requests for this report. In some countries, like France, Germany and the USA, one-line listings of nuclear events reported by nuclear operators to the safety authorities of the respective countries are publicly accessible. However, they are established according to very different criteria that make the statistical comparison entirely meaningless. A simple look at the figures available per country does not give any indication as to whether incidents in one country are more frequent or more serious than in another country. Finally, the absence of information on another country is, of course, no indication that everything is perfect there.

The present analysis is a glance at available information on a narrow number of events in a limited number of countries. The specific knowledge of the participating research teams about their respective countries and regions was essential for the selection of events.

After a brief overview of the status of nuclear power in the world, in Chapter 3 the report provides a presentation of the main causes that can lead to nuclear accidents. Design errors, construction and manufacturing problems can lead to material defects and failures of equipment, components and entire systems. Problems can be triggered by external or internal events. Primary and secondary loss of coolant and fires can lead to serious events. Deficiencies of documentation and operating manuals have played a role in a number of events.

The significance of systemic issues is often underestimated. They are presented in Chapter 4. It is stunning how often the same type of event happens over and over again. Voluntary or involuntary violation of rules and procedures as well as the lack of systematic verification and control can obviously have significant effects on nuclear safety. In many instances identification and assessment of the root causes of a given event turns out extremely difficult. A further problem is the appearance of generic faults that are technical or organizational problems that can be multiplied throughout one specific facility or several plants. Sometimes problems are identified that concern all units of a given reactor series type around the world, which can exceed tens of reactors.

While there are no internationally agreed criteria for the reporting and classification of nuclear incidents and accidents, there is the International Nuclear Event Scale (INES), inspired by the former French event scale, developed by the IAEA and theoretically applied in all nuclear countries (see Annex 1). However, INES has been designed as communication tool rather than as technical rating index. Often operators and safety authorities argue about the appropriate level to be applied to a given event.

Chapters 5 and 6 of the present report present INES as well as the US and German reporting systems. Chapter 7 provides an exemplary overview of event statistics in France, Germany and the USA and Chapter 8 selected events in France and the USA according to differing methodologies. The statistics in these chapters could lead the reader to conclude that there is an incredible number of incidents in France compared to relatively few in Germany, the USA and other countries. This is unlikely to be so. The availability and classification of data is very different from one country to the other. And it is by no means the purpose of the present study to compare the safety performance of countries.

Finally, Chapter 9 provides the reader with the presentation of a selection of 17 events from 9 countries. The authors have extracted exclusively incidents that took place in light water reactors (pressurized and boiling water reactors). The vast majority of nuclear reactors currently operating in the world are light water reactors, 357 of a total of 435 units. There are

264 pressurized water reactors (PWR) and 93 boiling water reactors (BWR). This does, of course, not mean that there are no serious incidents and accidents in other nuclear reactor types and nuclear facilities other than power reactors. Examples include the sodium fire at the Japanese fast breeder reactor Monju in 1995 or the more recent leak at the UK thermal oxide reprocessing plant (THORP) that was discovered in April 2005. Both facilities are still shut down since the respective events took place.

Some examples of specific events are mentioned in this report that make reference to facilities other than power plants. Throughout the report the authors have attempted to illustrate incident patterns with specific examples. But mainly, the report concentrates on the most common reactor technology.

The final selection of incidents reflects the attempt to extract examples for event patterns rather than looking for the most extreme cases. The location attached to each event is sometimes not more than just the first place that a specific problem has been identified. In many cases, similar or even identical events are multiplied throughout a large number of nuclear facilities, sometimes spread out over a period of decades.

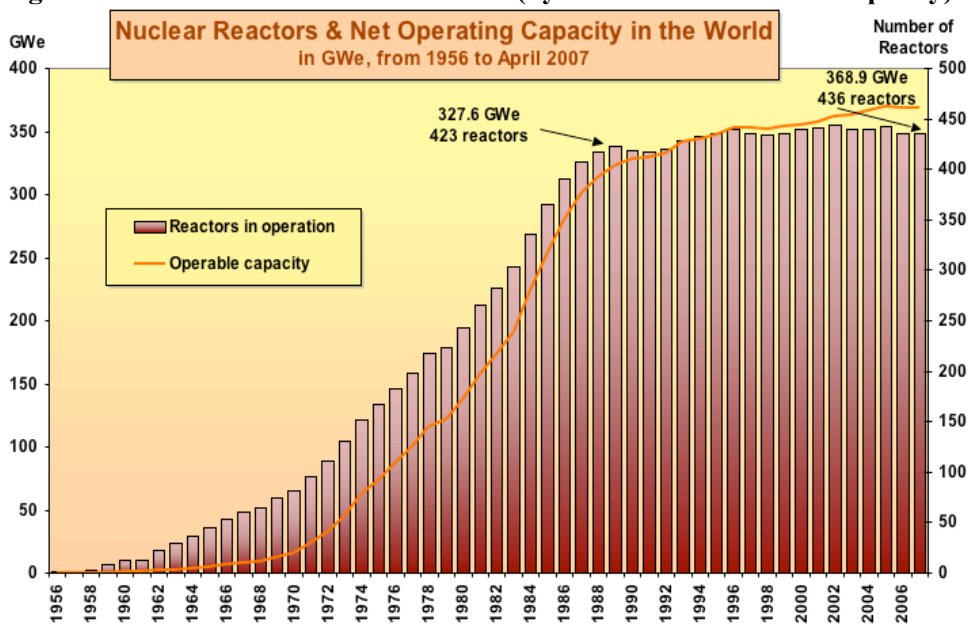
There is no doubt that this event list could have covered events other than those selected. Other experts might have come up with different examples. However, there seems to be a rather broad expert consensus that most of the 17 events constitute particular significant examples for a specific event pattern.

1.2 Overview of status and trends in the nuclear industry with focus on the European Union

1.2.1 Nuclear power reactors worldwide

At the time of Chernobyl accident (1986) there were some 384 nuclear power reactors in operation and more than 50 in construction. The most severe accident in the history of nuclear power in Chernobyl in 1986 slowed the practical application of this technology. This is clearly demonstrated on the following figure, where the number and capacity of operating reactors is shown.

Figure 1: Nuclear Reactors in the World (by number and installed capacity)



Source: IAEA-PRIS 07

The number of operating reactors reached 423 in 1989 and since that time their number has been almost constant. As of April 2007 there are 436 nuclear power reactors in operation worldwide.

The following table shows the relative numbers and age of commercial reactors in operation, under construction and their relative share in electricity and commercial primary energy consumption in different countries.

Table 1: Significance of Nuclear Programs by Number of Operating Reactors by Country

Countries	Nuclear Reactors				Power	Energy
	Operate	Average Age	Under Construc-tion	Planned	Share of Electricity (in 2006)	Share of Com.Primary Energy (in 2005)
USA	103	25	0	2	20%	8%
France	59	20	1	0	78%	38%
Japan	55	20	1	12	25%	10%
Russia	31	23	5	6	17%	5%
Korea RO (South)	20	12	1	7	40%	14%
United Kingdom	19	26	0	0	24%	9%
Canada	18	20	0	2	13%	6%
Germany	17	23	0	0	28%	11%
India	17	17	6	4	3%	1%
Ukraine	15	17	2	0	46%	14%
Sweden	10	26	0	0	50%	33%
China	10	4	5	13	2%	1%
Spain	8	23	0	0	24%	10%
Belgium	7	24	0	0	56%	19%
Czech Republic	6	13	0	0	31%	13%
Taiwan	6	23	2	0	22%	9%
Slovakia	5	17	0	2	57%	21%
Switzerland	5	29	0	0	40%	21%
Hungary	4	19	0	0	33%	10%
Finland	4	25	1	0	27%	19%
Bulgaria	2	19	2	0	38%	20%
Argentina	2	26	1	1	9%	3%
South Africa	2	20	0	1	6%	2%
Mexico	2	13	0	0	5%	2%
Brazil	2	13	0	1	4%	2%
Pakistan	2	19	1	2	2%	1%
Lithuania	1	19	0	0	80%	38%
Slovenia	1	23	0	0	40%	21%
Armenia	1	24	0	0	36%	23%
Romania	1	8	1	0	9%	3%
Netherlands	1	31	0	0	5%	1%
Iran	0	0	1	2	0%	0%
Turkey	0	0	0	1	0%	0%
Korea DPR (North)	0	0	0	1	0%	0%
EU27	145	22	5	2	30%	15%
Total	436	22	30	58	16%	6%

Sources: IAEA-PRIS 2007, BP 2006, WNA 2006, MSC 2007

The net electricity generating capacity of the operating reactors is about 369 GW. Due to the uprating of existing reactors and higher capacity of the new reactors as compared to shut-down units, the installed capacity slightly increased during the last decade. This cannot be directly compared though to the growth rate of competing power generation technologies although the installed capacity developments suggest that nuclear power has not attracted capital investment. For example since 1992, the US utilities alone have built over 270 GW of new natural gas fired power plants, 10 times the total nuclear capacity added through new build and uprating over the same period.[2] And the installed capacity of world wind power has increased from 5 GW in 1995 to over 59 GW in 2005 and is projected to more than double by 2010.

Nuclear power reactors produce about 15% of the total electricity generation worldwide and their relative share is on a downward trend.

At the time of the Chernobyl accident and up to 2001 there were constantly more than 50 reactors under construction. By the middle of April 2007, only 29 units are listed by the IAEA as under construction.[3] It has to be mentioned that for 11 of them construction started between 1975 and 1988. Fast growing economies in Asia (Japan, China, Korea, India and Pakistan) remain the centre of expansion of nuclear industry, accounting for 15 of the 30 reactors under construction and for 25 of the last 35 reactors that have been connected to the grid during recent years.

1.2.2 Types of nuclear power reactors

The most prevalent design is the Light Water Reactor (LWR – essentially, both PWR and BWR types), with 357 units in operation around the world, accounting for 82% of all operating reactors. The individual unit capacity of these reactors is the largest, with a net electrical output of up to 1500 MWe. Within this category the Pressurized Water Reactor (PWR), including the Russian designed WWER, is the most widely used reactor type with 264 units in operation (as of the middle of February 2007).

The other type of LWR is the Boiling Water Reactor (BWR) with 93 units in operation.

Another design deployed is the Pressurized Heavy Water Reactor (PHWR). 42 units of this type are in operation, mainly in Canada.

The Chernobyl reactor, that experienced the accident in April 1986, was of so-called Light Water Graphite Moderated Reactor (LWGR) design, also known as RBMK. The remaining three Chernobyl RMBK units are now closed down and the six RBMK units under construction at the time of the Chernobyl accident, including two at Chernobyl, have been abandoned. 16 power reactors of this type remain in operation – 15 in Russia and 1 in Lithuania.

Gas Cooled, Graphite Moderated Reactors (Magnox and Advanced Gas Cooled Reactors - AGR) were developed in the United Kingdom. 18 units of this type are in operation in the UK, but there are no plans for further development of these reactors.

Fast Breeder Reactors (FBR) were and are still the hope of the nuclear industry for further expansion. However, due to many factors, mainly scientific and technological difficulties, their development practically stopped. A number of units have been abandoned, either prior to commissioning (Kalkar, Germany) or after serious technical difficulties or

[2] http://www.world-nuclear.org/sym/2005/bowman.htm

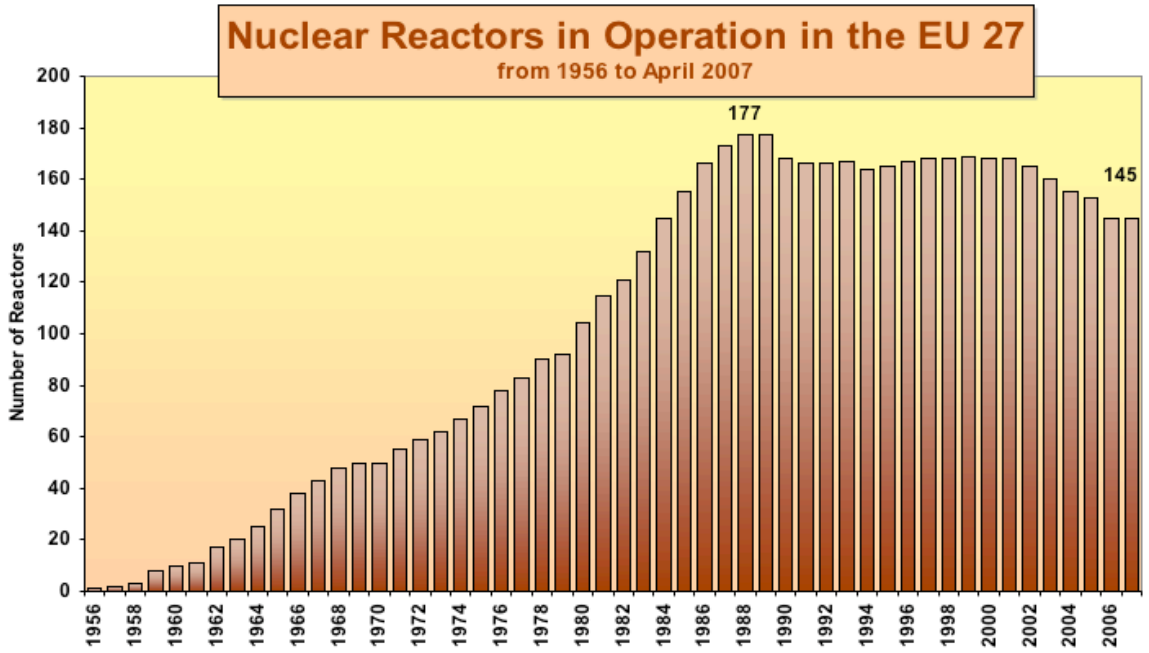
[3] We are indicating 30 units under construction in Table 1 because, contrary to the IAEA, we are taking into account the French Flamanville-3 unit, because groundwork has started and construction has been authorized just prior to the French Presidential elections.

economic decisions (Superphénix, France; Shevchenko, Kazakhstan; PFR, UK). The Monju reactor in Japan has experienced a serious fire in 1995 and has since been shut down. Today there are only two fast breeder reactors in operation, one in Russia, one in France (Phénix in France, has been downgraded to research reactor status) and two are in the construction phase (in Russia and India).

1.2.3 Nuclear power reactors in the European Union

The evolution of the number of operating reactors in EU-27 countries is shown on the following figure.

Figure 2: Nuclear reactors in operation in the European Union 1956 to April 2007



Source: IAEA – PRIS 2007

The Chernobyl accident practically stopped the growth of nuclear power in the then EU-15 and significantly slowed down its development in Central and Eastern European countries. In Western Europe the most recently power reactor to be commissioned was at the end of 1999 (Civaux-2, France). Five nuclear power reactors, which had started construction prior to the break up of the Soviet Union, were commissioned between 1996 and 2002 in three countries in Central and Eastern Europe (Cernavoda-1, Romania, Mochovce-1 and -2, Slovak Republic and Temelin-1 and -2, Czech Republic).

125 power reactors are presently operated in 8 countries in Western Europe (EU-15) and 20 power reactors in seven countries in Central and Eastern Europe. In addition five nuclear power reactors are operated in Switzerland. The total number of operating units in Europe significantly declined during recent years, as first generation reactors have been shut down. Currently there are only two reactors under construction in Western Europe, both being Generation III European Pressurized Water Reactors (EPR) at Olkiluoto-3 in Finland and most recently at Flamanville, France, for which the construction license was issued in March 2007. Three reactors are still in various stages of construction in Central and Eastern European countries (Belene-1 and -2, Bulgaria and Cernavoda-2, Romania), where work started between 1983 and 1987.

There are eight countries for which nuclear power provides 40% or more of total electricity generation; all these countries are in Europe (Belgium, Bulgaria, France, Lithuania, Slovak Republic, Sweden, Switzerland, and Ukraine). Of the sixteen countries that get more than 25% of their electricity from nuclear power plants, thirteen are in Europe. This means that nuclear power is still very important for the electricity supply in Europe and this situation will subsist in the short and medium term.

However, it is in Europe that the decline of the nuclear industry has been the fastest over the past two decades, while the decline in the USA corresponded to the TMI accident of 1979. All of the currently 103 operating units in the USA have been ordered in the decade from 1963 to 1973. Reactor orders that had been registered up to 1978 have all been cancelled. In fact, a total of 138 orders have been cancelled between 1970 and 1994, many in advanced stages of construction[4].

1.2.4 Design and operational safety

Prior to the Three Mile Island Unit 2 accident in 1979, it was quite typical for nuclear safety experts to assert that the likelihood of a severe accident in a commercial power plant was of the order of one in a million per reactor per year of operation (10^{-6}/a), notwithstanding the fact that the pioneering probabilistic safety assessment of its time (WASH-1400) estimated a likelihood far more frequent (one in 17,000 per year, or about 6×10^{-5}/a). The occurrence of the TMI-2 accident after less than 1,000 reactor-years of operating experience with commercial power reactors was a wakeup call for the nuclear industry.

Apposite to the European situation was, however, the Chernobyl accident in 1986 - resulting in a large radioactivity release that spread contamination widely throughout Europe – and which provoked a significant re-examination of nuclear safety. Numerous improvements in human factor aspects of plant operation, procedures, training, and to a lesser extent changes in plant design were carried out at European nuclear plants in the decade that followed the accident.

Over the last decade many LWRs in Europe were backfitted and supposedly upgraded with filtered venting systems, bunkered residual heat removal plant and hydrogen burning or passive auto-catalytic recombiner equipment as a means of avoiding containment failure in severe accidents, and as a means of reducing the release fraction (the amount of released radioactivity) from severe accidents. Some power plants were also equipped with digital instrumentation and control systems.

Significant modernization measures were implemented also at Russian PWRs in Central and Eastern European countries.

In recent years a number of first generation reactors were finally shut down in Germany, UK, Bulgaria, Spain, Sweden and Lithuania (22 units between 2002 and 2006). It is expected that after 2009 there will be no more such reactors operating in Europe.

Four Generation III units are in operation in Japan; all are Advanced Boiling Water Reactors (ABWRs).

After accidents in Three Mile Island and Chernobyl a large number of measures were introduced in order to improve the safety during reactor operation: improvement of operational procedures, implementation of comprehensive quality systems, development of emergency operating procedures, intensive training of personal including simulator training, etc. All these measures were expected to result in significant improvements of operational safety during the following years. However, there is evidence, as can be seen from many of

[4] CEA, *Nuclear Power Plants in the World*, Edition 2001; It is interesting to note that the listing of the cancelled units in the world has disappeared from more recent editions of the same publication.

the examples considered in this report, that despite these measures there was little or no further improvement during recent years and concerns have been expressed in many international forums regarding complacency in the industry.

A number of more recent incidents in the nuclear industry continue to illustrate shortcomings in the design of the systems, safety documentation, and safety culture. A total number of 23 Level 3 (serious incident) and one Level 4 (accident, Tokai Mura, Japan, 1999) events have occurred in nuclear power facilities worldwide since the introduction of the International Nuclear Event Scale (INES) in 1991 (see Annex 11.1).

Even leaders of the nuclear industry have publicly expressed their concerns. Hajimu Maeda, Chairman of the World Association of Nuclear Operators (WANO) warned that "*loss of motivation to learn from others...overconfidence...(and) negligence in cultivating a safety culture due to severe pressure to reduce costs following the deregulation of the power market*." Those troubles, if ignored, "*are like a terrible disease that originates within the organization*" and can, if not detected, lead to "*a major accident*" that will "*destroy the whole organization. We must avoid the pitfalls of self-satisfaction which threaten us*". "*Even a minor accident could be a disaster*," echoed Bruno Lescoeur, executive vice president, generation & trading, of Electricité de France (EDF), *"because it could question the acceptability of nuclear energy in France, and perhaps in the world."* Armen Abagyan of Rosenergoatom said lack of attention to operational events—he cited events in Russia, France, and the U.S.—"*may lead to a new burst of antinuclear opposition and adversely affect both Russian and the world nuclear industry.*"[5]

IAEA Director General Mohamed El Baradei said that an accident or significant safety incident would cripple the nuclear industry. "*We cannot afford another accident*," he added. El Baradei stated that there would still be a lot of work that needs to be done in the area of safety, particularly in the area of applying safety standards and safety culture uniformly across the industry.[6]

[5] Statements made during the biennial general meeting of the World Association of Nuclear Operators (WANO) held in Berlin, on 13-14 October 2003.

[6] Statements made in a video presentation at the American Nuclear Society meeting in New Orleans in November 2003.

2. Definitions: Incidents or Accidents? Events!

The Chernobyl accident caused damage which went much further than anyone could have imagined up to that point. (...) The range of damage suffered seems almost limitless. No precise figures are available, but the costs of the accident over the last two decades are estimated to have risen to the level of hundreds of billions of dollars.

Julia A. Schwartz
Head of Legal Affairs, OECD Nuclear Energy Agency

There seem to be as many terms and definitions as sources for what could be called a nuclear incident. The dictionary defines the term *incident* as "an event or occurrence" and *accident* as *"unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury"*.[7]

On the main basis of (western) design the probabilistic approach identifies all "incidents" that are reasonably foreseeable on a frequency and severity basis so these are "foreseeable incidents" and not random accidents.

The selection of events in this report is not based on the IAEA's INES index. Certain events can be considered of great significance or large potential risk but are not rated beyond a low level on the INES scale, because of the particular criteria definition. The INES scale attempts to translate the severity of a given event only from a point of view of immediate radiological impact but not from the potential risk.

The joint IAEA–OECD Nuclear Energy Agency (NEA) Incident Reporting System (IRS) claims providing information on *"safety-significant events from the global nuclear community"*[8].

The IAEA's INES defines events as "deviations" (Level 0), "anomalies" (Level 1), "incidents" (Level 2) "serious incidents" or "near accidents" (Level 3) and "accidents" (Levels 4 to 7) – see Annex 11.1.

There is also the term "near miss" that the US National Academy of Engineering defines as *"an almost complete progression of events - a progression that, if one other event had occurred, would have resulted in an accident. (...) A near miss can be considered a particularly severe precursor."*[9] However, the near miss criteria are neither applied in the selection of events for the IRS nor in the INES rating.

There is no objective, internationally recognized definition for particularly severe incidents that bear the potential for severe accidents. In many occasions the direct material, environmental and health consequences of an event are strictly zero. However, this does not provide any indication on how close a given situation has come to an event with serious consequences. Sometimes it is only time that makes the difference – if material stress had been prolonged, rupture would have occurred (see e.g. the hole in the vessel head at Davis Besse incident in the US of 2002). Sometimes safety systems would not have been operable in case they had been needed (see e.g. inoperable pressure relief valves at Gravelines in France

[7] Oxford American Dictionaries
[8] IAEA/NEA, *Nuclear Power Plant Operating Experiences – From the IAEA/NEA Incident Reporting System 1999-2002,* December 2003
[9] J.R. Phimister, V.M. Bier, H.C. Kunreuther (eds.), *Accident Precursor Analysis and Management: Reducing Technological Risk Through Diligence*, National Academy of Engineering, Washington, DC USA, 2004, page 198; available at http://www.riskinstitute.org/PERI/PTR/Accident+Precursor+Analysis+a

in 1989, or reactor sump clogging at Barseback in Sweden in 1992 and at many other plants around the world). In many cases an additional event could have turned a benign incident into a severe accident (see loss of off-site power at Maanshan in Taiwan in 2001 and Forsmark in Sweden in 2006).

In this report the reader is provided with the main characteristics of a given event and their interpretation. It is explained why particular events have been selected. While the responsibility for the final selection is with the project team, it is clear that other choices could have been made, even if the choice of a number of cases seems to be based on a broad international consensus amongst experts.

The selection of events in this report is not based on the IAEA's INES. Certain events can be considered of great significance or large potential risk but, because of the particular criteria definition, these have not been rated beyond a low level on the INES scale. The INES scale does not adequately translate the severity of a given event.

3. Overview of the Main Causes and Contributing Factors Leading to Nuclear Events

This section of the report discusses some of the main causes and contributing factors that have lead to events in nuclear facilities in the more than 8,000 reactor-year of operating experience accumulated since the Chernobyl Unit 4 disaster. It is important to realize that questions about "safety culture" underlie many of the events and accidents at nuclear facilities. The IAEA defines the term "safety culture" as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance". The IAEA's International Nuclear Safety Analysis Group (INSAG) reported in 2002: *"Most incidents and accidents in the nuclear industry have occurred because someone has failed to take the relevant precautions or has failed to consider or question in a conservative way decisions that they have made or the steps which were taken to implement them."*[10]

The historical record of such events (insofar as public domain documents is concerned) is incomplete for a number of reasons:

- In many countries, even though reporting systems exist that require nuclear facility operators to report operating experience to the regulatory authority, the resulting reports and reporting system data are often considered to be (commercially) confidential information, or contain proprietary information that cannot be released to the public.
- Event databases such as the database of events reported to IAEA and the NEA of the OECD in the "Incident Reporting System" are often confidential. Not all events are publicly reported, and some INES reports for events, which do attract press attention, are not themselves publicly released, leading to incomplete information in the public domain. This is sometimes true even for events categorized at INES Level 3 (an example is the Kozloduy Unit 5 control rod insertion failure incident in 2006 - the incident itself was widely reported, but no public report appeared in the publicly-accessible area of the IAEA Nuclear Events Web-based System – NEWS - data base). Even though summary level reports for the IAEA/NEA Incident Reporting

[10] See, INSAG-15, "Key Practical Issues in Strengthening Safety Culture", September 2002, page 1

System are periodically published, neither the facilities at which the events take place nor the date of occurrence (other than that it happened within a three-year period covered by the report) are identified. Another difficulty is that the INES Level is often identified and released to the press before any formal and painstaking inquiry into the incident ha concluded and, often, the INES Level is quietly upgraded once the inquiry has concluded.

Examples reported below to illustrate the main causes and contributing factors to events at nuclear facilities are entirely based on publicly available sources.

3.1 Design Faults

The engineering design of hazardous plants, such as nuclear facilities, is carried out in compliance with a complex quality assurance program that covers individual components, assemblies and trains of engineered equipment and plant, and the buildings and services that house and contain the nuclear plant.

Design verification is achieved as a responsibility of the so-called Design Authority who acts to type approve the many thousands of pre-manufactured components, instruments and systems that are bought-into the nuclear plant, and who provides the assemblage of these separately sourced components, etc., and sets out the sophisticated management routines and procedures to oversee the safe operation of the overall the plant.

At stages and when completed, the plant and its systems are scrutinized by an Independent Reviewer and then, dependent in detail on the country of installation and its municipal legislation, the plant design and operating procedures are subject to a regulatory regime or Nuclear Regulator that centers about the nuclear safety of operation and when the plant under internal and external fault events. All of the EU27 states require the plant, both in condition and design status, to be periodically reviewed throughout its operational lifetime.

Underpinning the robustness of the nuclear safety case is a requirement of providing the safety trains and abnormal event management with redundancy and diversity: For example, redundancy is where two pumps are provided instead of one, and diversity is where there is an entirely independent response, such as a bursting membrane as well as a pressure relief valve, to avoid a common-mode or common–cause failure. However, as plants and systems have becoming increasingly more complex, particularly from the lessons learnt from the TMI and Chernobyl incidents, a greater element of passive response has been introduced with the aim that whatever the prevailing abnormal circumstances the plant will settle to a safe and contained state, not being reliant upon active safety systems.

These approaches to achieving nuclear safety require excellence and painstaking detailed checking with formulation of design features that could never be realistically demonstrated other than in a real and severe event (ie such as the reactor core corium melt management system proposed for the EPR). Even so, the overall design and regulatory approaches are strengthened by a presumption that each aspect of the plant function has to be demonstrably safe in that it operates at levels of ‘acceptable risk and tolerable consequences’.

Even with such precautions, however, both detailed design errors and deeper-rooted errors in the design philosophy or approach can and have nevertheless occurred.

For a *detailed design* error to persist and reveal itself in a plant event, not only the original design must be in error, but the design checker within the organization that created the design has to miss the error. In addition, the design review - conducted by personnel or organizations not involved in the original design - also has to miss the error. Thus, it can be seen that all design errors that manifest themselves in plant events are the result of not one but multiple misjudgments or the like.

Errors of *design approach* can and have been deep rooted, remaining hidden until revealed by exceptionally challenging circumstances. For example, the lateral bulkhead design of the SS *Titanic* (which stopped short for forming completely watertight cells throughout the height of the hull) was entirely inadequate because the situation of striking an iceberg so far south in the Atlantic crossing was never foreseen and, if it had been, then the risk would have been assessed and, if unacceptable, the bulkhead design set for an outcome of tolerable consequences. Design approach errors are fundamental, passing by the Design, Reviewing and Regulatory authorities.

The threats and challenges to nuclear plants is not static, with certain of these being unforeseen at the time of the design and commissioning.

Challenges such as the risk of flooding and extreme weather conditions might evolve throughout the service lifetime (and throughout its decommissioning and radioactive waste management periods). Such changes, perhaps brought about by Global Warming, might not be readily defended against and might beyond the original composite of 'acceptable risk and tolerable consequences'. Similarly, threats against nuclear plants might evolve but much more rapidly with events such as the 9/11 terrorist attacks heralding an absolute requirement that such hazardous plants be safeguarded, a feature that was certainly absence in the Generation I and II nuclear power plants, and which is being found to be difficult to incorporate into the present Generation III nuclear plants such as the AP and EPR series PWRs.

Design errors have been identified since 1986 as root or contributing causes in numerous cases, including the following examples:

a) A fire at Unit 2 of the Palo Verde nuclear power plant in the United States on 04 April 1996 was identified as resulting from an electrical grounding design error. The result of the error was simultaneous fires in the main control room and in the safe shutdown equipment room. Damage from the control room fire resulted in loss of one train of control room emergency lighting circuits, some general plant essential lighting, and the loss of plant fire detection and alarm panels. The fire in the safe shutdown equipment room affected equipment that supported post-fire safe shutdown capability in event of a control room fire. Investigation of the fire resulted in the discovery that the same design error had been made on all three units at Palo Verde.[11]

   The Palo Verde incident involved elements of lack of redundancy and diversity.

b) Japan's prototype fast-breeder, sodium (roughly 1,530t) cooled nuclear reactor Monju (280 MWe) was built at a cost of about $5 billion and was designed to burn a combination of plutonium-uranium mixed oxide fuel and to produce more plutonium than it consumes. After a decade of technical delays and costly preparations Monju started operation in April 1994 and was connected to the grid in August 1995. On 8 December 1995, when running at 40% of nominal power, about 750kg of liquid sodium leaked from the secondary cooling system and caused a subsequent fire. The leaked sodium melted parts such as a ventilation duct and a catwalk, and was piled up on the floor, covering some 4,400 sq. m. The floor temperature reached 700 to 750^0C, but it did not melt. The Monju sodium leak was the largest ever from a fast breeder reactor.

[11] See US Nuclear Regulatory Commission Information Notice Nr. 97-01

The cause for the incident was the faulty design of the temperature sensor pocket in the sodium coolant pipes. In the 1995 accident one of these pockets had broken off, which started the leaking of the pipe. Other pockets also were found with signs of cracks. The investigations of the incident discovered questionable operating procedures, inadequate manuals, and sloppy crisis management - all rendering the Monju case a result of failed detailed design and inadequate institutional controls and quality assurance.

For more than 10 years, Monju has been undergoing safety inspections and a modification program. Every year plans to restart Monju in the near future are announced but, to date, the reactor remains shutdown.

c) The 10 April 2003 fuel damage accident at Paks Unit 2 (which occurred during chemical cleaning of 30 fuel assemblies in a tank in the spent fuel pool, outside the reactor) was identified by the IAEA as due in part to eight separate design errors. This event was categorized as INES Level 3. (See 9.2.4.1 for details on the accident.)

d) New control rod drive mechanisms were installed in Kozloduy unit 5 in July 2005 during the annual outage. The unit restarted in beginning of September and was operated on full power. However on 1 March 2006 after a main coolant pump trip it appeared that 22 of total 61 control rods could not be moved with control rod driving mechanisms. The root cause for this incident was design changes of driving mechanisms, which were not properly authorized and tested. The event was classified as INES Level 2. Thus, during eight months the reactor was operated at full power with an insufficient number of operable control rods. (See 9.2.3.2 for details on the event).

The Kozloduy incident included elements of faulty detailed design and institutional failure to conduct type approval quality assurance controls.

3.2 Construction and Manufacturing Problems

Even when the design of a nuclear facility is correct, errors during construction can nonetheless result in an event at the facility. This is particularly the case when the design specifications are not respected during construction, and the as-built system is not verified to conform to the design.

Construction errors have been identified as root or contributing causes in the following exemplary events:

a) At an unnamed Japanese nuclear power plant in the 1999-2002 time period, a crack was discovered on a pipe. Investigation of the event found that a vinyl chloride tape was placed on the piping during plant construction to identify the pipe. During preoperational testing, high temperature water was passed through the piping for a short period. The high temperature decomposed the tape, producing chloride ions. During each subsequent plant start-up, the chloride ions reacted with the pipe metal and moisture, resulting in chloride stress corrosion cracking on the outer surface of the pipe. During periodic inspection, a hydrostatic test was performed, and the cracking propagated to the inner surface, resulting in

a leak.[12] This is an example of where the original design intent was thwarted by a temporary modification.

b) In the 1960s, for the on-site fabrication of the UK's Magnox reactors, separate preformed steel plates forming the 15m diameter primary pressure vessel were temporarily tack welded in place with steel channels located on the outer surface to enable full welding to be completed. Once that the pressure vessel had been tested the mass concrete biological shield was cast to completely enclose the reactor pressure vessel. Under irradiation the pressure vessel shell itself became very radioactive so that only remote monitoring was possible. In the 1990s when concern was expressed about the extent of irradiation and embrittlement of the steel pressure vessel, a spider robot was designed to crawl over the outer surface of each pressure vessel to inspect for crack development of the shell but, much to the surprise of the robot designers, the spider encountered the tack welded channel sections and was unable to proceed further, all at great expense and considerable delays in proving the period safety review.

   Thus incident, occurring at a number of the Magnox nuclear power stations, was simply because the failure to record the continuing presence of the tack weld channel sections on the as-built design.

3.3 Material Defects

Nuclear safety is dependent on the proper performance of the various materials used to construct and maintain structures, systems, and components in nuclear facilities. When incorrect material is used in an environment that is not conducive to the material, component failures can result. Material degradation mechanisms in nuclear power plants include irradiation embrittlement, fatigue, corrosion fatigue, stress corrosion cracking, corrosion, thermal ageing, wear, and erosion.[13]

Material selection in the engineering design process usually assumes a set point failure. For example, for the design of a welded joint it is assumed that a hypothetical defect or flaw exists in the weldment with the size of this flaw is assumed to be just below the limit of non-destruction examination so that the weld would pass through the inspection quality control. The flaw is assumed to develop and propagate under the specified service conditions (embrittlement, thermal cycling, etc) to failure, which is required to be within the design requirement in terms of age, time, number of cycles etc. This cautious approach enables the component design to be matched to a prescribed service or replacement life.

Material defects have been identified as root or contributing causes in numerous events, including the following examples:

a) The Davis-Besse reactor vessel head hole, detected in 2002

[12] NEA-5168, "Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System 1999-2002", page 16

[13] See, IAEA, "Material Degradation and Related Issues at Nuclear Power Plants", Proceedings of a Technical Meeting held in Vienna, Austria, 15-18 February 2005, published September 2006, pages 2-3

In evaluating events involving ostensible materials problems, it is often a matter of judgment whether an event is properly ascribed to "material defects". For example, it is well known in industry that carbon steel is subject to corrosion when exposed to acidic solutions and it is well recognized that LWR primary coolant (which contains boric acid) can corrode carbon steel. When such corrosion occurs, concluding that it is the result of a material defect is misleading – there was nothing wrong with the material per se – rather, a problem can occur when the material is not regularly inspected for corrosion damage and repaired before the corrosion damage results in failure.

Thus, the Davis-Besse reactor vessel head corrosion event but was also due to an inappropriate detailed design of the reactor head penetration sealing to avoid the acid getting in contact with the vessel head material and, in addition to this, a prolonged institutional failure to conduct proper surveillance, combined with a lack of management procedures mandating further investigation of the root cause, such as following through the reason at the discovery of carbon steel corrosion products trapped in the main containment air sampler filters). (See 9.2.1.2 for further details on the event).

b) Reactor Pressure Vessel Shroud Cracking

Boiling water reactor core shroud cracking occurred at a number of nuclear power plants in the 1996-1999 time period, and was identified as one of a handful of problems discussed in the joint IAEA/NEA Incident Reporting System report for this period.[14]

c) Graphite Moderator Degradation – Magnox and AGR Plants, UK

The mainstay of the UK's reactor development program was the graphite moderated, gas cooled reactor design that was applied to the 1st generation Magnox, to the development marquee AGR and planned for but abandoned series of high temperature, graphite moderated reactors. Graphite was chosen as the moderator because of its high neutron moderation characteristic, that it lessened the need uranium fuel enrichment (natural uranium in the Magnox and minimal enrichment for the AGR)), it could be used in a dual role for plutonium breeding, and that, in conjunction with a carbon dioxide primary coolant, higher steam turbine temperatures could be achieved thereby winning considerable gains in overall thermal efficiency of the plant.

However, the speed at which the UK developed its commercial, power generating reactors outstripped the acquisition, mostly by empirical means, of the in-core characteristics and degradation of graphite. This resulted in a number of design and operation difficulties, namely:

i) Early experience in the Magnox reactors indicated that the in-core neutron flux accelerated radiolytic oxidation (weight loss) over that anticipated from the data obtained from the lower pressure research reactor cores. To

[14] Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System 1996-1999", pages 10-11

offset this, a continuous trace of methane was injected into the primary circuit with the desired result but, unbeknown at the time, the methane also accelerated the corrosion of the reactor core support steelwork to the extent that in the early 1970s all of the Magnox reactors had to be significantly derated in output. Even so, the extent of the moderator weight loss in the four remaining operational Magnox reactors, at Oldbury and Wylfa, is now in excess of 20 to 30% of the first commissioned level, so much in fact that slightly enriched fuel is now required to maintain criticality in the cores.

ii) In light of the steelwork corrosion in the Magnox reactors, the follow on AGR internal steelwork was chosen to be corrosion resistant to permit a tolerable level of methane injection. However, the reactor circuit operating conditions, particularly the higher pressure, has accelerated graphite oxidation to the extent that the four AGR reactors at Hunterston and Hinkley Point (2,400MWe in total) have been shut down for the last 6 months while the graphite core residual strength safety case is reviewed.[15]

The Magnox and AGR core difficulties have resulted in considerable financial impact and loss of the nuclear safety margin, particularly for the AGR where sufficient core residual strength is necessary to prevent core collapse in the event of a multiple boiler tube failure. The failure illustrates the risks involved in the rapid development of a reactor series where unproven extrapolation has to be relied upon in material selection.

3.4 Failures of Equipment, Components, and Systems

Nuclear power plants are typically designed using a "single failure criterion", which means that systems are designed such that following an initiating event, a single failure is assumed and then the remaining available equipment is evaluated to ensure that all essential safety functions can still be performed. The single failure criterion has been a fundamental nuclear safety design principle and analysis assumption since the 1960s. There is a difference though from country to country on the decision whether the single failure criterion is applied to active systems only or also to passive system.

Unfortunately, operating experience has consistently shown that a surprisingly large proportion of all equipment failures are so-called "common-cause" or "common-mode" failures - that is, multiple trains of equipment are failing due to a common-cause. Previous common-cause failure data indicates that about 10% of all equipment failures are in fact common-cause failures in which two or more trains of equipment fail.[16] Data compiled by the US Nuclear Regulatory Commission (NRC) in 1999 indicates that common-cause failures account for the following percentages of all failures for the indicated component types:

---

[15] Large J H, *Brief Review of the Documents Relating to the Graphite Moderator Cores at Hinkley Point B and Other Advanced Gas-Cooled Reactors*, R3154 5 July 2006 - http://www.largeassociates.com/3154%20Graphite%20AGR/R3154-Graphite%20FINAL%2028%2006%2006.pdf

[16] See EPRI, *Classification and Analysis of Reactor Operating Experience Involving Dependent Events*, EPRI NP-3967, June 1985, page 5-3; more recent report indicate a similar pattern; see for example, NRC Regulatory Issue Summary 99-003, "Resolution of Generic Issue 145, Actions to Reduce Common-Cause Failures", 13 October 1999

a. Air-operated valves (AOVs), 37.8%.
b. Batteries & battery chargers, 4.8%.
c. Check valves, 30.6%.
d. Circuit breakers, 11.7%.
e. Diesel generators, 9.7%.
f. Heat exchangers, 62%.
g. Motor-operated valves (MOVs), 7.5%.
h. Pumps (auxiliary feedwater, emergency service water, emergency core cooling), 8.0%
i. Relief valves, 11.8%.
j. Safety valves, 13.6%.
k. Strainers, 24.1%.

The NEA has initiated the International Common-cause Data Exchange Project. The most recent reporting of the project (in the Incident Reporting System report for the period from 2002-2005) indicates that despite improvements in maintenance, training, design documentation, updating of safety analysis reports, and many other industry initiatives to improve performance, about eleven percent (11%) of all common-cause failures are complete system failures.

Taken together, this indicates that about 1% of all component failures represent common-cause failures resulting in complete failure of all similar components (10% of all failures are common-cause failures, and 11% of the common-cause failure represent complete system failures). The results vary across different classes of components, but the general average for all components in the program supports the one percent (1%) complete common-cause failure rate. The study also found that most of the failures that lead to complete failures are due to human actions.

3.5 External Events

This section of the report is concerned with potential risks originating with events occurring outside the plant. Such events can result from natural phenomena hazards and from man-made hazards. Exemplary types of external event hazards include (a thorough analysis of external events typically involves the assessment of more than one hundred different events):

- Flooding (due to extreme rainfall, tidal effects, storm surges, seiche, tsunami, dam failure, levee failure, etc.)
- High winds (tornado, hurricane, cyclone, wind-blown debris, tornado missiles)
- Extreme weather (high temperature, low temperature, hail, snow, sleet, icing, humidity, extreme drought, extreme water temperature)
- Aircraft impact (takeoff, landing, air corridor accidents, fire fighting aircraft accidents, military aircraft, hijacking & terrorism)
- Adverse electromagnetic environment (electromagnetic interference, lightning, electromagnetic pulse due to conventional means)
- Pipeline accidents
- Onsite or nearsite transportation accidents (road, sea, river, rail)
- Explosions (blast waves, missiles)
- Gas clouds (toxic, asphyxiates, combustible)
- Liquid releases (flammables, toxic, radioactive, corrosive)
- Near-site accidents at industrial or military facilities

- Biofouling hazards (zebra mussels, asiatic clams, clogging of intake and service water structures)
- Seismic events
- Volcanic hazards (dust, debris, lava flows, mass movements, ground motion, etc.)

For most external events, nuclear facilities are required to withstand prescribed levels of severity referred to as the Design Basis – these include design basis earthquake, design basis wind speed, etc. Some extreme levels and types of external events are categorically excluded from the design, often due to low frequency of occurrence arguments (such as meteorite impact) or lack of event possibilities in the nuclear facility region (such as no volcanoes present in the region where the facility is located).

The Design Basis approach is dependent upon both *a priori* and *post priori* knowledge which is used to forecast the chance or probability that a specific event will occur in the future but utter dependence upon this has several pitfalls: For example, the future occurrence of the event may not be described by the same probability distribution as the past, this might be particularly pertinent to severe weather conditions, flooding, etc., possibly due to climatic change; the forecasting model may not fit the historical data very well, particularly where the chance levels under consideration (~1 in 1,000,000) are very remote; and/or the probability of chance may be corrupted by human intervention such that malicious acts might properly be considered to be inevitable rather than an act of chance.

There are several examples where external events have affected nuclear facilities since 1986, including the following:

a) An external flooding event (due to a storm surge topping local flood protection provisions) occurred on 27 December 1999, affecting the Blayais nuclear power plant in France, causing all four units to be shut down and rendering some safety systems inoperable at Units 1 and 2 (see 9.2.7.1 for details). This event was rated as INES Level 2. As a result of the Blayais flooding, a site-specific reassessment of flooding potential was undertaken for French nuclear facilities. The Belleville, Bugey, and Chooz nuclear power plant sites were found to need new, higher maximum flood design levels.

b) The Indian Ocean tsunami on 26 December 2004 (resulting from a very large undersea earthquake off the coast of Indonesia) caused flooding at the Kalpakkam nuclear site in India. IAEA characterized the resulting wave as a "huge tsunami".[17] Water from the tsunami caused $3.5 million in damage at the site, and caused water level in the operating unit to rise, resulting in tripping of the reactor. Although this specific event was rated as INES Level 0, the event is noted here due to the potential for tsunamis to affect this and other coastal nuclear facility sites around the world.

c) Two external fires (wild fires that started with a controlled burn offsite) affected various facilities at Los Alamos National Laboratory in the United States on two occasions (the so-called "Dome Fire" in 1996, and the so-called "Cerro Grande Fire" in 2000). Such fires can also affect nuclear power plants, as demonstrated by a loss of offsite power resulting from a wild fire near the Diablo Canyon nuclear power plant on 04 April 2001.

[17] IAEA Staff Report, 08 August 2005, http://www.iaea.org/NewsCenter/News/2005/tsunami.html

d) A Fujita Scale 2 tornado passed near the Davis-Besse nuclear power plant in the United States in 1998. Although the wind speed experienced at the plant site was within the design basis, significant damage occurred to the plant electrical switchyard and to non-safety related buildings. Lightning strikes resulted in opening and closing of breakers. A total loss of offsite power occurred, and two of three emergency response communications systems were disabled. The plant computer system also failed due to loss of power. Rain entered the turbine hall owing to large holes in the turbine hall roof caused by storm damage. A pair of tornadoes (one rated at Fujita Scale 4, but at F1 or F2 near the power plant) passed near to the Calvert Cliffs nuclear power station on 28 April 2002.[18] A tornado affected the Quad Cities site in the United States in 1996.[19]

e) Hurricane Andrew struck the Turkey Point nuclear power plant in the United States in 1992, with sustained winds of 233 km per hour and peak gusts at 282 km per hour (a hurricane Intensity Level 4 on a scale of 5). Safety-related structures at the nuclear power plant were designed for a maximum wind speed of 378 km per hour. Owing to the lead-time available before the hurricane reached the site area, drains were plugged to prevent water entering the plant, and operators were stationed in the diesel generator building as a precaution. Although safety related structures did not suffer any damage, offsite power was lost to the site for five days. During this time period, one of the diesel generators had to be shut down due to overheating. Offsite communication was lost and plant access roads were blocked by debris. Helicopters had to be used to bring fuel and consumables to the plant site. Families of plant staff were taken to the plant and fed, to allow operators to work in a "non-emotional" environment. A water tower collapsed causing major damage to the fire protection system piping, the water supply system, electrical services, and instrumentation. Some non-safety-related buildings were destroyed during the storm. In addition, an effluent stack at a fossil-fired unit at the Turkey Point site structurally failed. Over $90 million in damage was caused at the plant site.

f) Offsite power was lost to the Maanshan nuclear power plant in Taiwan during a tropical storm in 2001 (see 9.2.5.1 for details). Similar losses of offsite power due to salt spray effects have affected the Pilgrim nuclear power plant in the United States.

g) So-called "biofouling" incidents continue to occur, resulting in unscheduled plant shutdowns and some impacts on safety systems (particularly service water systems). Electricité de France shut down two Paluel reactors in the summer of 2005 as a precautionary measure when heavy storms resulted in the accumulation of an unusually high amount of seaweed that was interfering with the water intake at the plant.[20]

[18] http://www.somd.com/news/headlines/2002/04/tornado/; http://www.weatherbook.com/laplata.html; http://www.erh.noaa.gov/er/lwx/Historic_Events/apr28-2002/laplata.htm
[19] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/admin-letters/1997/al97003.html
[20] Nuclear Engineering International, 13 July 2005

3.6 Internal Events

This section of the report is concerned with potential risks originating with events occurring inside the plant, but due to causes not associated with the normal operation of plant systems. Such events include fires, rupture of primary system components leading to Loss of Coolant Accident (LOCA), flooding resulting from pipe breaks, and internally generated missiles resulting from turbine failures.

3.6.1 Loss of Coolant Accident (LOCA)

On 20 January 2003 Kozloduy unit 3 was operated at 98 % of rated power. At 04:14 AM the reactor protection system was automatically actuated by a low pressure in the primary system (PI<115 bars) signaling a primary coolant leak. At the same time a safety injection signal was actuated (at PI=105 bars). All safety injections and confinement spray pumps started as designed. At 04:35 the leaking part of the primary system was isolated and the leak was compensated. Soon after this the primary system pressure and the pressurizer level were restored. During the event the safety injection and confinement spray pumps were in operation for about 60 min.

During the revision the leak was found at a pipeline (38 x 4mm) and the estimated leak size was equivalent to a diameter of 22,5 mm. The direct cause of the pipe leak was a mechanical damage due to a long time vibration and friction of a pipe to a part of the structural components. Deficiencies of the surveillance program for pipes in the confinement also contributed. The damaged pipe was not included in the non-destructive testing program and surprisingly the visible mechanical damage was not discovered by visual inspections.

It appeared that at least for several hours the personnel did not check the readings of systems for early detection of leaks from the primary side, which indicates serious degradation of the safety culture. This incident shows that the role of Leak Before Break Concept has to be dramatically re-considered as an important line in the Defense in Depth Concept (several levels of protection). The event was rated at Level 1 on the INES scale only, in spite of the fact that according to INES guidelines the starting assessment for events with real leakage from primary system is to be considered a Level 2 event.

3.6.2 Fires

Most frequently fires in nuclear power plants are detected quickly and manually suppressed before significant damage can be done. In other cases, the automatic fire suppression systems are actuated and these quickly suppress the fires. Such benign outcomes are not always the case and nuclear power plant probabilistic safety studies often identify specific fires as important contributors to core damage frequency. Serious fires have occurred in the past two decades, and can be expected to continue to occur in the future.

There are numerous examples of **turbine failures** since 1986 (most accompanied by a fire due to the combustion of hydrogen leaking from generator cooling systems and/or fire due to leakage and combustion of turbine lubricating oil):

a) In 1989, Unit 1 of the Vandellos nuclear power plant, a now shut down gas-graphite moderated reactor in Spain, suffered a turbine failure and subsequent turbine hall fire. Suppression of the fire took six hours. During the fire, a rubber expansion joint in the turbine hall failed, resulting in seawater flooding of the lower levels of both the

turbine hall and the reactor building (in the latter case, this flooding occurred due to violation of administration controls that left a door open). Considerable equipment failures ensued, including failure of two of four main coolant circulators, two feedwater pumps, the turbine building sump pumps, the control air system, area lighting in many plant buildings, the shutdown heat exchanger, the public address system[21] and the condenser control valves. Smoke entered the control room, and fire suppression systems were automatically actuated in numerous areas despite the lack of fire in those areas. This event was rated as INES Level 3. The resulting damage was so significant that it was decided to permanently close and decommission the plant.

b) In 1991, a turbine hall fire occurred at Unit 2 of the Chernobyl nuclear power plant in Ukraine due to an electrical short circuit resulting from the inadvertent operation of one of the turbines as an asynchronous motor. This resulted in turbine rotor displacement, and release of hydrogen from the generator cooling system and release of lubricating oil from the turbine systems. As a result of the lack of smoke discharge provisions in the turbine hall and insufficient cooling of steel structures, the turbine hall roof collapsed. The collapse resulted in the disabling of three of the five main feedwater pumps and one of three emergency feedwater pumps. Ultimately, both main and emergency feedwater were totally disabled before the fire could be suppressed. Reactor cooling was maintained only by increasing main circulating pump seal cooling flow. The fire was suppressed three and a half hours after it began. According to the Finnish safety authority STUK, *"only some very extraordinary measures to remove residual heat saved the plant unit, with a small margin, from a severe reactor accident."*[22] Ultimately, the decision was taken to permanently close and decommission the unit owing to fire damage.

c) In 1993, a turbine hall fire at the Narora nuclear power plant in India resulted in a prolonged station blackout. The fire burned for more than ten hours before it was suppressed. During the course of the fire, smoke entered the main control room. No control room indications were available due to the loss of electrical power. Emergency control panel indications were also blacked out. The main control room was evacuated. The plant remained shut down for repairs from March 1993 until January 1995. The fire was rated INES Level 3.

d) Turbine hall fires resulting in prolonged shutdowns occurred at the Salem reactor in 1991, and at the Fermi Unit 2 in 1993, both plants in the United States. In both cases, turbine failures were the initial event leading to the fires. The Salem event resulted in generation of turbine ejected debris missiles that impacted numerous plant structures.

3.6.3 Secondary cooling circuit and other pipe failures

Another type of event that has periodically occurred over the period since 1986 involves secondary pipe failures due to erosion corrosion. The most recent example of this type of event took place at the Mihama nuclear power plant in Japan in 2005 when a pipe

[21] The system by which control room operators can communicate with personnel in other areas of the plant by way of announcements.
[22] see http://www.stuk.fi/julkaisut/tr/stuk-yto-tr168.pdf

failed due to erosion corrosion, resulting in the deaths of five workers and injuries to six more workers. It was later revealed that the pipe wall thickness of the failed pipe had not been checked since the plant went into operation in 1976. After the Mihama-3 pipe failure, two additional erosion-corrosion-related pipe failures occurred at the South Ukraine nuclear power plant in Ukraine. On 19 May 2005, a high-pressure heater line ruptured at Unit 2; and on 26 August 2005, a condensate pipe ruptured at the same plant.[23] The lack of surveillance of this piping appears difficult to justify considering the previous operating experience with secondary pipe failures, which included:

a) A feedwater line break at the Surry Unit 2 plant in December 1986 that resulted in four deaths and two serious injuries.[24]

b) Discovery in 1987 of significant erosion-corrosion of safety-related feedwater piping at the Trojan nuclear power plant in the United States, resulting in the replacement of the affected piping.[25]

c) Failure of an extraction line at Arkansas Nuclear One Unit 2 in April 1989 due to erosion-corrosion.[26]

d) Failure of an extraction line at the Fort Calhoun nuclear power plant in the United States due to flow-accelerated corrosion.[27]

e) Failure of a moisture separator drain line at Millstone Unit 3 in the United States in December 1990, causing failure of adjacent line due to pipe whip damage, resulting from erosion-corrosion.[28]

f) Failure of feedwater regulating valve bypass lines at the San Onofre Unit 2 plant in the United States in July 1990 due to erosion-corrosion.[29]

g) Failure of a low-pressure heater drain pipe at Surry Unit 1 in the United States in March 1990 due to erosion-corrosion.[30]

h) Failure of the main feedwater piping at Loviisa Unit 1 in Finland in May 1990 due to erosion-corrosion.[31] On 25 February 1993, a feedwater pipe ruptured at the adjacent Unit 2 reactor.[32]

---

[23] IAEA, "Material Degradation and Related Issues at Nuclear Power Plants", Proceedings of a Technical Meeting held in Vienna, Austria, 15-18 February 2005, published September 2006, page 15
[24] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1986/in86106.html, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1986/in86106s1.html
[25] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1989/gl89008.html, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1987/in87036.html
[26] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1989/in89053.html
[27] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1997/in97084.html
[28] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1991/in91018.html
[29] ibidem
[30] ibidem
[31] ibidem
[32] IAEA, "Material Degradation and Related Issues at Nuclear Power Plants", Proceedings of a Technical Meeting held in Vienna, Austria, 15-18 February 2005, published September 2006, pages 40-42

i) Failure of a moisture separator re-heater line at Millstone Unit 2 in the United States in November 1991 due to erosion-corrosion. [33]

j) Failure of a condensate line at Sequoyah Unit 1 in the United States in November 1994 due to erosion-corrosion.[34]

Corrosion affected piping in other systems as well as in secondary steam-related systems. Essential service water systems can be affected by several types of corrosion. On 25 August 2004, a circumferential break occurred in one train of a two-train essential service water system at the Vandellos Unit 2 reactor in Spain. This break left only a single train of equipment supplying essential cooling to safety-related equipment such as the diesel generators, the residual heat removal system, and others. After repairs, the other train of essential service water was checked and it too had to be repaired.[35]

3.7 Human Errors and Violations of Rules and Procedures

Humans make mistakes. For this reason, in technologies with potentially high consequences in case of an untoward or unplanned for event, actions undertaken by humans should be checked by other persons to provide additional insurance of correct execution. Even this does not ensure perfection, because the failure of the "checker" to identify and correct the mistake made by the person in the first instance results in the mistake continuing to exist.

Unfortunately, the likelihood of human errors is not so small as to make such combinations of errors very unlikely. It is thus not at all surprising that human errors are among the causes of events in nuclear facilities. Deliberate violations of procedures - whatever the motivation (goodwill or ill advised) – also not surprisingly results in events in nuclear facilities.

Human errors and violations of procedures have been identified as root or contributing causes in the following examples of events:

a) At Unit 1 of the Kozloduy nuclear power plant, during an outage in May 1998, a spill of chemical cleaning fluid resulted in the contamination of the water tank used for three emergency core cooling and confinement spray systems. Plant management decided – contrary to safety requirements – to drain the emergency water tank. This left the emergency core cooling system and spray system without a water supply for 24 hours, contrary to license requirements. This event was categorized as INES Level 2 due to a serious reduction in defence-in-depth and the adverse safety culture of the plant executives and personnel.[36] Note that this event occurred at a pressurized water reactor that does not have a containment.

b) Japan: Data Falsification in TEPCO reactors. Staggered by a series of scandals, all 17 boiling water reactors operated by Tokyo Electric Power Co. were shut down between September 2002 and April 2003 for extensive safety checks after revelations erupted in late August 2002 that TEPCO personnel had systematically concealed findings on core internal inspections from regulators. (see 9.2.8.3 for more details).

[33] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1991/in91018s1.html
[34] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1995/in95011.html
[35] IAEA, "Material Degradation and Related Issues at Nuclear Power Plants", Proceedings of a Technical Meeting held in Vienna, Austria, 15-18 February 2005, published September 2006, pages 49-52
[36] See Committee on the Use of Atomic Energy for Peaceful Purposes (Bulgaria), 1998 Annual Report, page 10

In all three cases above, human errors were deliberate violations of requirements – not unfortunate mistakes.

3.8 Deficiencies in Documentation

Deficiencies in documentation is another of the factors causing events in nuclear facilities, where it is often a matter of judgment to decide whether a given event was caused by human error or documentation deficiencies. For example, if a procedure is changed, but the persons executing the procedure are not properly trained in the change, is the event that results due to a deficiency in documentation (i.e., the documentation does not describe what is actually practiced in the field) or is it a deficiency in training (i.e., the procedure was not executed correctly because the persons performing the procedure were not trained properly in its use)? Nonetheless, it is clear that documentation deficiencies can be a root or contributing cause to nuclear events.

> Example: In 2001 a shortfall of the specified filling level of the flooding tanks during the start up of the Philippsburg-2 plant in Germany was detected late because of wrong data interpretation (see 9.2.3.1 for further details).

3.9 Malicious Impacts

Note: The following section will focus only on the situation in the US. This shall not preclude any judgment about the quality of the respective security arrangements in the US or any other countries.[37,]

The potential for sabotage attacks at nuclear power plants poses a unique risk and deserves special consideration. All nuclear power plants, no matter how low their probability of severe accidents, are vulnerable to catastrophic meltdown and large radiological release in the event of a well-planned sabotage attack. Therefore, every nuclear plant should have a highly effective security organization that is prepared at all times to immediately and successfully respond to a range of external and internal threats.

However, dangerous security weaknesses at nuclear plants are all too common. While there has not been a documented case of sabotage at a nuclear power plant resulting in a radiological release, numerous incidents over the last twenty years have revealed serious security vulnerabilities that could have been exploited in the event of an attack. These vulnerabilities should be considered comparable to vital safety systems that are non-functional. A broken security system would be unable to prevent a successful attack, just like a broken safety system would be unable to prevent a serious accident. However, security vulnerabilities are distinct because intentionally caused events are of a different character than randomly occurring accidents. An insider who is aware of a security vulnerability can provide the information to external attackers, therefore increasing the likelihood of a successful attack.

---

[37] Publicly available case-specific studies and papers include:

• Large J H. Marignac Y, Submission to the International Atomic Energy Agency - Convention on the Physical Protection of Nuclear Material (CPPNM) – IAEA InfCirc/274 & InfCirc/225/Rev.4 - *IAEA Requirements on Design Basis Threat Assessment - Non Compliance of Eurofab LTA shipment from US to France on UK Vessel: Security and Physical Protection Issues*, IAEA 20 September 2004;

• Large J H & Schneider M, *Vulnerabilities of Nuclear Plants to Terrorism*, Oxford Research Group Seminar, Rhodes House, Oxford, December 2002

But no such correlation exists between a broken safety system and the random occurrence of an accident initiator.

A key factor in assessing the effectiveness of security programs at nuclear power plants are performance tests. These range from tests of the intruder detection systems to full-scale "force-on-force" exercises involving simulated attacks by mock adversary teams with paramilitary equipment and training.

In this section, we discuss several security-related incidents that have occurred at U.S. nuclear plants since the Chernobyl accident that are notable for the severity of the weaknesses that they revealed. Typically, after events like these, the U.S. Nuclear Regulatory Commission (NRC) will take steps to address the vulnerabilities that were exposed. However, even after the revamping of the NRC's security programs in the aftermath of the 11 September 2001 attacks, incidents of concern continue to occur, often brought to the attention of the public through whistleblowers, indicating that the systemic problems in security are not being addressed.

Compiling information about security problems at nuclear plants is a far harder task than compiling information about safety problems. In the United States, most information about nuclear plant security is classified as "safeguards information" and is only disseminated to individuals with proper authorization and who are determined to have a "need to know" the information. However, prior to the 11 September 2001 attacks in the United States, a substantial amount of security-related information was available to the public. After 11 September 2001, the NRC, along with all other government agencies, took steps to greatly reduce the amount of information available to the public that was deemed useful to terrorists. Much of the information provided in this section comes from the archives of the Union of Concerned Scientists. Although some of the documents referenced below are no longer readily available to the public through the NRC website or other easily accessible sources, none of these documents are considered "safeguards information" and hence are not restricted from distribution.

The events discussed are examples of four categories of security event: (1) specific threats against nuclear plants that were neutralized before occurring; (2) actual breaches of security; (3) gross failures of preparedness of the security force as revealed through performance tests; and (4) general decline of the "security culture" that would severely impair security response in the event of an incident.

a) Potential sabotage against the Palo Verde nuclear plant and Diablo Canyon nuclear plants in 1989. On 30 May 1989, a number of members of the environmental activist organization Earth First!, including the founder, Dave Foreman, were arrested by the U.S. Federal Bureau of Investigation for plotting to cut the transmission lines carrying power to the Palo Verde nuclear plant near Phoenix, Arizona and the Diablo Canyon nuclear plant near San Luis Obispo, California. The plot was not far advanced at the time of the arrests, and questions remain regarding whether the conspirators were entrapped by an undercover FBI agent who had infiltrated the group. As a result, the security significance of this event is unclear.

b) Unauthorized forced entry and site area emergency at Three Mile Island Unit 1 on 7 February 1993[38]. (see 9.2.8.1 for details)

3.9.1 Security Failures Prior to the 11 September 2001 Attacks[39]

Between 1991 and 2001, the NRC conducted a program known as the Operational Safeguards Response Evaluation (OSRE). This program consisted of performance exercises designed to evaluate whether nuclear power plant security forces could effectively defend against an adversary team with a defined set of characteristics: number, weaponry, equipment and tactics. This set of characteristics is known as the design basis threat (DBT). Although the details of the design basis threat are classified as "safeguards information" by the NRC, it is well-known that no more than three external attackers were used in these exercises. In these wargame-type exercises, a mock adversary force would carry out a series of four attack scenarios, with the objective of simulating the destruction of enough plant equipment to cause a core meltdown (known as a target set). The NRC would then evaluate the performance of the nuclear plant security force in preventing the adversary team from achieving its goal.

In the course of the ten-year program, the NRC conducted 81 OSRE exercises. All operating U.S. nuclear plants had at least one OSRE, and several had two. According to NRC data, in 37 of the exercises, or about 46%, the mock adversary force was able to simulate causing a meltdown in at least one of the four scenarios tested. This means that if a real terrorist assault had occurred during this time, by a group of adversaries with capabilities at or below the design basis threat, there was a substantial chance that the attack would have been successful in causing a catastrophic core melt.

Special attention should be paid to the last 11 OSREs conducted prior to the 11 September 2001 terrorist attacks, when the program was terminated. Those tests can be regarded as a measure of the level of preparedness of U.S. nuclear power plants against terrorism just before 11 September 2001 and provide a rough sense of the likelihood that a terrorist ground attack at a U.S. nuclear plant would have been successful had al Qaeda chosen such a target and mode of attack. These OSREs were also distinct because they were graded by NRC under a revised procedure for determining the significance of the failures. NRC data reveals that the OSRE failure rate in this period, judged by the loss of at least one target set, was seven out of eleven, or 64%; a failure rate higher than the average over the entire decade.[40] Thus it appears that the overall level of security at U.S. nuclear plants declined over the course of the OSRE program.

This period was also characterized by an unusually high level of public disclosure of nuclear plant security information by the NRC, and fairly detailed public inspection reports of the OSRE exercises taking place at that time. This transparent era came to an abrupt end after 11 September 2001, when the NRC, along with other U.S. government agencies, severely restricted the amount of security-related information available to the public.

---

[38] U.S. Nuclear Regulatory Commission, *"Unauthorized forced entry into the protected area at Three Mile Island Unit 1 on February 7, 1993"* NUREG-1485, 1 April 1993.

[39] Edwin S. Lyman and David Lochbaum, *"Protecting Vital Targets: Nuclear Power Plants,"* in *Homeland Security: Protecting America's Targets (Vol. III: Critical Infrastructure)* (James J.F. Forest, ed.), Praeger Security International, Westport, Connecticut, 2006, p. 157-173.

[40] U.S. Nuclear Regulatory Commission, *"Physical Security Significance Determination Process,"* Powerpoint presentation at NRC public meeting, 30 August 2001, slide no. 17.

Below are three excerpts from OSRE inspection reports of that period that reflect some of the problems that nuclear plant security forces were experiencing. The severity of these problems provides a stark indication of the lax security that was present at many nuclear plants on the eve of 11 September 2001.

a) Farley Nuclear Plant, Columbia, Alabama, July 2000.[41] During the July 2000 OSRE, the security force at Farley could not prevent the mock adversary team from simulating the destruction of entire target sets in two out of four exercises (and therefore simulating a meltdown); and simulating the destruction of "significant plant equipment" in a third exercise.

Part of the reason for this poor performance was the "failure to adequately perform multiple portions of the response strategy." Adversaries were not detected in time to allow security officers to defend pieces of vital safety equipment; responders could not leave defensive positions without making themselves vulnerable to the adversary; and some security officers were outside of the protected area and took too long to respond after the attack.

b) Oyster Creek Generating Station, Forked River, New Jersey, May 2001. During the May 2001 OSRE, the security force at Oyster Creek failed to protect a target set from destruction from the mock adversary team in one out of four exercises. However, NRC determined the failure to be the result of a flaw in the protective strategy for a two-target target set, as well as performance errors by the responders. The strategy at issue required the plant armed responders to leave one of the two targets completely undefended and concentrate forces to defend the other target. However, the security officers protecting the second target were vulnerable to being killed by the adversaries, and this is exactly what happened during the exercise. The adversaries were therefore able to destroy both targets and cause core damage.

c) Vermont Yankee Generating Station, Brattleboro, Vermont, August 2001.[42] The August 23, 2001 OSRE at Vermont Yankee was the last one conducted by the NRC before the program was terminated after the 11 September 2001 attacks. Of the 11 OSREs preceding the 11 September 2001 attacks, this was the worst, the only one assigned a "yellow" finding by NRC, indicating the failure had "substantial safety significance" and resulted from a "broad programmatic problem." However, because the inspection report was not filed before the NRC revamped its policy on release of security information after 11 September 2001, specific details about what warranted such a harsh finding never became publicly available.

3.9.2 Security Failures After the 11 September 2001 Attacks

The 11 September 2001 attacks made it clear to U.S. officials that they had to take seriously the threat of catastrophic terrorism against critical infrastructure facilities. The NRC pledged to increase the level of security at U.S. commercial nuclear facilities. Yet at the same time, it greatly reduced the amount of security-related information available to the public, so

[41] U.S. Nuclear Regulatory Commission, *"Farley Nuclear Plant – NRC Inspection Report 50-348/01-07 AND 50-364/01-07,"* letter to Mr. D.N. Morey, Vice President, Southern Nuclear Operating Company, 21 June 2001.
[42] U.S. Nuclear Regulatory Commission, *"Vermont Yankee Generating Station – NRC Inspection Report 50-271/01-010,"* letter to Mr. Michael A. Balduzzi, Senior Vice President and Chief Operating Officer, Vermont Yankee Nuclear Power Corporation, 28 November 2001.

that it became more difficult for the public to assess whether the steps the NRC was taking were appropriate and whether nuclear plant operators were complying with them. Thus no official information was released of the type described above, such as specific force-on-force test results.

After several years in which the NRC's security information policy was in flux, it decided on an approach in which it would issue an annual summary report of security findings, with few details about the nature of the violations and no discussion of the specific plants involved. It would also issue redacted cover letters of security inspection reports, which would simply mention whether or not a security concern was found.

The NRC issued its first summary report on 30 June 2006, covering the period from 29 October 2004 to 31 December 2005.[43] In that period, the NRC conducted 111 "baseline" security inspections and 23 force-on-force tests. 104 violations were found during the baseline inspections, of which 99 were judged to be of "very low safety significance." (It is not clear from this data how many inspections found at least one violation, since it is possible that more than one could be found in a single inspection.)

Three violations were found during the force-on-force tests, all of which were judged to be of "very low safety significance" and did not result in any fines or other enforcement actions. On the surface, this would appear to be an improvement over the pre-11 September 2001 performance. However, so little is publicly known about the exercises compared to the period before 11 September 2001 --- NRC even keeps secret the procedure for determining the safety significance of a security violation --- that the relationship between the two sets of data is not clear.

Despite the NRC's attempts to keep a tight lid on security information, problems continue to emerge, usually revealed by whistleblowers concerned that nuclear plant managers and the NRC are not taking their concerns seriously. Security allegations that came to light at several nuclear plants in 2005 and 2006 are troubling indications that the security culture at the NRC and within the industry has not undergone the radical shift needed to be able to cope with the emerging threat after the 11 September 2001 attacks.

In December 2005, the nuclear power watchdog groups NC WARN and Union of Concerned Scientists disclosed a number of security allegations that had been brought to their attention by security personnel at the Shearon Harris nuclear plant in New Hill, North Carolina. In response to the NC WARN-UCS letter, the NRC sent an inspection team to the site to investigate the allegations. None of these issues had previously been noticed by NRC inspectors.

The allegations included broken security doors leading to vital areas that management refused to fix despite repeated complaints from security officers; widespread cheating on the security certification exams administered to security officers by the state of North Carolina; and the issuance of merchandise "gift cards" in lieu of overtime payments in order to keep excessive overtime hours off the books. All three of these allegations were substantiated, although the NRC claimed the last one was due to a misunderstanding. In any event, the NRC

[43] U.S. Nuclear Regulatory Commission, "Annual Status Report on the Results of the Security Inspection Program Conducted by the United States Nuclear Regulatory Commission," attachment to letter to James Inhofe, Chairman, Committee on Environment and Public Works, U.S. Senate, 30 June 2006.

claimed that these events were of "very low safety significance."[44] This mischaracterization provides a window into the NRC's questionable perception of the dangers posed by such chronic and severe security violations.

The NRC only conducts one force-on-force test for regulatory compliance purposes every three years at each nuclear power plant, using the allegedly independent Composite Adversary Force. In between, the licensee conducts training drills, which the NRC may observe. In these drills, the licensee typically uses an adversary force composed of the site's own security officers.

Whistleblower complaints brought to light in August 2006 by the Union of Concerned Scientists at the South Texas Project nuclear plant near Bay City, Texas, also resulted in a special security inspection by the NRC. These included an allegation that during a force-on-force security drill being observed by both the NRC and the Federal Bureau of Investigation (FBI), the mock adversary team was instructed by management to intentionally lose the exercise. The NRC substantiated the concern of the employee who reported it, but claimed that it was a misunderstanding of the management's intention.[45]

Another troubling incident involved the discovery of a hole drilled into a stainless steel pipe connected to the pressurizer at the Turkey Point Unit 3 nuclear reactor in Florida, which led the NRC to dispatch an "Augmented Inspection Team" to investigate, a sign of the potential serious nature of what could have been an intentional attempt to sabotage the plant. Further details on this situation are not available.[46]

In summary, despite all the public attention on the risks of nuclear power plant attacks since 11 September 2001, the NRC and the US nuclear industry do not appear to have responded with the appropriate level of vigilance, and nuclear plants remain vulnerable to the rapidly evolving terrorist threat.

[44] U.S. Nuclear Regulatory Commission, *"NRC Staff Responds to Security Concerns at Harris Nuclear Plant Near Raleigh*, press release, 22 March 2006, http://www.nrc.gov/reading-rm/doc-collections/news/2006/06-005ii.html.

[45] U.S. Nuclear Regulatory Commission, Letter to Edward Markey, U.S. House of Representatives, 22 December 2006.http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2006/markey-12-22-2006.pdf

[46] U.S. Nuclear Regulatory Commission, *"NRC Sends Augmented Inspection Team to Review Equipment Damage at Florida Nuclear Power Plant",* press release, 31 March 2006, http://www.nrc.gov/reading-rm/doc-collections/news/2006/06-011ii.html.

4. Systemic Issues

4.1 Recurring Events

The term "events" is widely used in the nuclear lexicon as a synonym for "failures, incidents and accidents".

In public discussions the argument is often stressed, that an important component of nuclear safety is the lessons learned from failures, incidents and accidents that have occurred in the past. Therefore analysis and evaluation of operational events have been performed by nuclear regulators on their respective national level as one of the most vital nuclear safety activities for decades. An international exchange system of operational experience also exists, the Incident Reporting System (IRS, see chapter 5.2), which is based on national information of the respective regulators on a selection of incidents considered significant.

Nuclear operators maintain other exchange systems on experiences with events, on the utility level, but also within "Owners Groups" operating reactors from the same supplier. WANO also operates a worldwide event reporting system.

A widely held opinion is that gross failures and damaging events from the past could not happen again in future and can be excluded because of the learning processes provided through the existing exchange systems. If that was true, the analysis of events and failures over time should show that certain types of events, which happened long ago, would not recur. To implement experience feedback, "corrective actions" have been developed after each event. The expert language term "corrective actions" means a defined bundle of tools to prevent the specific type of event happening again. Depending on the event, the tools can consist of e.g. general information to the operators, changes in operating management regime, enhancing the information base of the operation staff by better displays of the actual status of the plant, technical changes in the safety system and/or other parts of the plant. Given the implementation of those corrective actions, previously identified or experienced events should not happen again.

However, event analysts learn by their practical experience that some of the actual events recall similar events from earlier times. The OECD NEA published a first investigation on that issue in 1999[47]. The result was not in accordance with widespread belief, but fits with the experience of event analysts until now. Four types of recurring events were identified:

1. Loss of residual heat removal while at mid-loop (Pressurized Water Reactor).
2. Failure of valves to operate.
3. Service water degradations due to biofouling.
4. Boiling water reactor (BWR) power oscillations.

The NEA Report points out: *"The history of loss of RHR [Residual Heat Removal][48] at midloop conditions was reviewed. There were over 20 such events in the time period 1980-1996, i.e. more than one per year. The events were widely publicized and there were numerous communications by the regulatory bodies. Even so, this scenario continued to occur even though the corrective actions were well known.*

[47] OECD-NEA, *Recurring Events,* CSNI, September 1999

[48] Residual heat removal is the evacuation of heat that is still generated by the nuclear fuel when the reactor has been shut down.

Another recurring event identified was instability in boiling water reactors. A usual design criterion for boiling water reactors is that either the reactor remains stable by design, or else instabilities are detected and corrected. However, over the period 1982-1995 about ten instances of BWR instability were detected. These instabilities were quite large, e.g. with neutron power oscillating between 40 and 90% power. In spite of this, experts generally agreed that the risk attendant to BWR instability is quite low. Corrective actions for these oscillations or instabilities were not well defined and, in some cases, utilities were somewhat surprised when inadvertent instability was experienced.

A third example of recurring events was reduction or interruption of service water due to build-up of marine life, including clams, barnacles, shrimps, and mollusks. Seven such cases were noted over the period 1980-1997. Service water plays an important role in transporting energy from key systems to the ultimate heat sink."[49]

The investigations of the now identified effect of "recurring events" were continued. A second NEA report, using a broader background of experience with events and failures, identified nine classes of recurring events, which include the formerly identified types[50]:

1. Loss of RHR at mid-loop.
2. BWR instability.
3. PWR vessel head corrosion.
4. Hydrogen detonation in BWR piping.
5. Steam Generator Tube Rupture.
6. Multiple valve failures in ECCS.
7. Service water system biofouling.
8. System level failures due to human factors considerations.
9. Strainer clogging.

The NEA experts continued with an attempt to identify reasons for the persisting situation[51]:

"It was seen that the history for some recurring events is, at least, up to 20 years. This raises questions as to why the corrective actions had not been implemented in a timely manner. Several possibilities exist:

- *The operating organisation failed to take timely action, or was not aware of the events, or thought it was not applicable.*
- *The regulatory authority was not aware of the events, or had not imposed the licensee to take timely corrective actions.*
- *Work on the appropriate corrective action was in progress, but not fully implemented.*
- *The event was considered to be of lesser importance and risk than other plant modifications, and thus was not being pursued as rapidly as needed.*
- *Overall, the operating experience feedback programme was not fully effective.*

[49] CSNI Technical Opinion Papers No. 3, *Recurring Events*, OECD 2003, NEA No. 4388
[50] quoted in CSNI Technical Opinion Papers No. 3, *Recurring Events*, OECD 2003, NEA No. 4388
[51] ibidem

- *The root cause of the event had not been correctly identified, and thus the corrective actions were not responsive.*
- *The contributing factors or causes were not appropriately taken into account in identifying the corrective actions.*
- *What was thought to be a solution was, in fact, not one or the problem was generic, and what was a fix for one aspect did not cover all aspects.*

It is likely that all of these possibilities play a role in delaying action."

The NEA concludes with*: "Recurring events are important to safety in that they can indicate deficiencies in the plant safety culture, gaps in the national operating experience feed back systems, loss of continuity in skilled and knowledgeable operations and engineering staff, or lack of attention to design and operational factors such as plant ageing."*

The knowledge and experience from "lessons learned" up to now does not really impact in practice on the operation of nuclear power plants. A report published by the NEA in 2006[52] deals with that ongoing debate. It provides a number of quite alarming statements:

"Now, however, questions are being raised about whether the lessons from operating experience are being used commensurate with their importance to safety. For example, recent concerns have been voiced that:

- *lessons may be learned but they are subsequently forgotten over time;*
- *often nothing is done in response to information learned about others' experiences;*
- *there is a tendency to consider foreign operating experience as not relevant to one's own situation; and*
- *more generally, operating experience reporting is not meaningful if it is not used to promote operational safety."*

The NEA continues:

"The fundamental logic supporting the need for a vigorous operating experience programme is that serious accidents are almost always preceded by less serious precursor events and that by taking actions to prevent recurrence of similar events, one is thereby reducing the probability of serious accidents."

and

"Nuclear power plants are highly complex installations, with several redundant and diverse mechanical, electrical and control systems. There are dozens of such systems and thousands of individual components in a typical plant. Experience over the years has shown that all plants experience individual component and system failures from time to time, almost always with no safety consequences. Many of these operating events at nuclear power plants include contributions from human and organisational factors. If no steps are taken to correct the root causes of these failures, they will recur and, accompanied by other failures or perhaps human errors, will lead to a more serious event or accident."

[52] Regulatory Challenges in Using Nuclear Operating Experience, OECD 2006, NEA No. 6159

Also in 2006 the third Edition of the NEA's "Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System" was published[53], which covers the years 2002-2005. In its conclusion the report states inter alia:

> *"About 200 events have been reported by the participating countries during that period…*
>
> *Almost all of the events reported during that period have already occurred earlier in one form or another. It shows that despite the existing exchange mechanisms in place at both national and international levels, corrective measures, which are generally well-known, may not reach all end-users, or are not always rigorously or timely applied.*
>
> *Recently, some top regulators expressed their concerns with respect to the international effort devoted to operational experience. They notably noticed that:*
>
> - *A worldwide observation is that operating experience feedback (OEF) needs to be much improved in the international arena.*
> - *There is a tendency to consider that foreign OEF is not relevant.*
> - *The global effort in the area of event reporting does not appear to be functioning as it should.*
> - *The focus of existing networks (IRS, etc.) should move from event reporting towards a synthesis of the given information and to combining it with other available knowledge on the respective topic, e.g. insights from risk studies and other research."*

The widespread belief that nuclear safety will be actually enhanced because of a lessons-learned process turns out ill-conceived as illustrated by the above-cited reports. It is an open question whether the actual discussions within the nuclear expert community can lead to an improvement of nuclear safety in the reality of nuclear power plant operation. The discussion runs in high ranking international expert circles. Nevertheless, their analyses are based on a broad overview on real nuclear events. On the other hand, nuclear safety itself is mainly influenced by day-by-day behavior of people who are very close to nuclear installations, people like the operating shift managers, maintenance workers, designers of system details in case of system changes, etc. There is a big distance between these different groups of people with all their different attitudes and thinking. Therefore it is unclear whether tools can be found, to interact in a way that a real enhancement in safety is accessible.

It seems rather that the actual discussion on "recurring events" has identified a field of strong limitations for the implementation of an enhancement of nuclear safety, which could not be surmounted in real life.

4.2 Violation of Rules and Procedures

The enormous risk potential of nuclear power plants requires a comprehensive set of safety measures. The proper functioning of complex safety systems depends on the interaction of many technical and administrative conditions. The technical design has to meet the requirements of the possible operative range. Additional provisions are necessary to retain the

[53] Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System, OECD 2006, NEA No. 6150

operating conditions within the permitted limits. Thus the safety of the plant has to be ensured as well by a complex set of regulations applying to safety related processes covering technical, management, personal and organizational aspects. Binding procedures are implemented as a requirement for the action of the staff. The compliance with rules and regulations is important to safety in all phases of planning and operation of the plant.

When important effects are disregarded during the design phase, the capability and the behavior of the plant are not verified for all event sequences and conditions. Incorrect or insufficient design assumptions may cause the malfunction or total loss of functions later. Inadequate operation and maintenance of equipment can cause a degradation of properties that may affect safety related functions. Insufficient inspection and testing can allow for failures going undetected for a long time. Poor surveillance of major operating parameters can allow for systems to run beyond their design basis with the risk of damage or ineffectiveness of these systems. Incomplete documentation can lead to misinterpretations.

Due to such circumstances a wide range of possible failures may affect safety and cause malfunction or total loss of functions required to cope with accidents. The violation of rules and regulations can impact on safety as much as technical failures can.

The malfunctioning of a cooling pump, for example, might be caused by technical failures but also by design characteristics inappropriate for specific operational conditions (e.g. capacity, medium, loads). It might also be caused by an insufficient amount (pressure, temperature, composition) of coolant but also by lacking supply of required utilities like electricity, control, lubricant. The malfunctioning might also be the effect of personal failures or ineffective regulations.

Rules and procedures can be disregarded consciously or inadvertently. Weaknesses in staff education and training, incomplete technical knowledge, missing awareness of the safety related context just as inappropriate ergonomic constitution of regulations will influence their implementation adversely. There are many reasons that render plausible the violation of rules and regulations; the compliance with regulations is laborious and time-consuming. Procedures become more complicated and deviate from usual day-by-day practice. Regulation is often perceived by staff as unnecessary additional paperwork and largely exaggerated control procedures.

The violation of rules and procedures is not automatically apparent. Control measures to check staff behavior and the efficiency of rules and procedures cannot cover all possibilities of violation and certain can be bypassed. In many cases the resulting effects do not appear in close temporal or technical context: Insufficient maintenance may induce a malfunction only after years. Design errors may induce damage only under unusual or rare conditions (e.g. specific loads, specific operational states, specific events). From there a large number of unreported cases may be expected. However, the compliance with rules and procedures is assumed in safety analysis in general. Special functions of safety related equipment are checked within the regular proceedings under test conditions. Other functions depending mainly on the application of rules and procedures cannot be checked totally this way.

All in all the potential and the safety significance of possible consequences of this systemic issue are supposed to be very high.

a) In 2001 a shortfall of the specified filling level of the flooding tanks during the start up of the Philippsburg-2 plant in Germany was detected late because of wrong data interpretation. Subsequent investigations revealed that significant deviations from requirements during start-up and violations from related instructions seemed to be common probably for several years and took place in a similar way in other German nuclear plants too. (see 9.2.3.1 for further details)

4.3 Lack of Systematic Verification and Control

One of the key safety principles for design and operation of nuclear power plants is to ensure an exceptionally high level of quality. This is related to the design of the technical properties of equipment but also to the performance of all measures and tasks necessary for its safe operation. To meet the intended high quality level an appropriate system of verification and control has to be established complementarily. A comprehensive set of quality assurance measures has to be developed in a systematic way and implemented into the operational routines.

Testing and inspection procedure prior to initial operation shall make sure that the design and as-built states are in compliance with planning and approval. Periodical tests during operation shall verify the orderly status and function of components. This is mainly aimed at potential degradations of safety related properties due to operational conditions. Moreover there are features that are tested only once. For these it is assumed, sometimes wrongly, that the features are in a constant state as built or designed. Also, the performance of safety related tasks (e.g. inspection, maintenance, repair, technical changes) is accompanied by a set of administrative control measures and regulatory hold points, e.g. permission, surveillance, final inspection.

Even though the quality assurance regime is comprehensive it is possible for the system of verification and control to be incomplete. Mistakes during planning, execution and documentation of test routines or misinterpretation of test results have been reported. This may be a consequence of the incomplete reliability of human performance. Another reported fact is that failures were built in as a result of test routines, e.g. due to inadequate handling of equipment. In addition as a systemic weakness the test routine cannot exactly anticipate and simulate all real conditions, loads and attitudes. Another problem may be the quality assurance of the performance of verification and controlling itself. This means the thorough and safety-conscious design and implementation of related administrative routines is necessary.

Failures built-in during construction, changes and/or plant misassembly may remain undetected for a long time, if the affected function is not covered by frequent routine tests. And, of course, there are a number of extreme functions that cannot be routinely non-destructively tested (ie primary containment, certain location internal crack propagation, etc). When the affected function is only required in the case of accidents the normal operation may give no indication of a malfunction. Lack of safety awareness in a given context may cause the insufficient design and performance of test routines and lead to relevant properties and possible deviations are not being rechecked systematically. In some cases, when the equipment has no active safety function (e.g. buildings, structures) usually the dimensioning and the as-is state is not verified again after initial approval. Such failures can often only be detected by chance or when upgrades are performed. Even after more than twenty years lifetime failures built in during construction have been identified. Due to this there is no exact information about the possible number of latent failures. The potential consequences are not analyzed, because they cannot be analyzed.

All in all, the existing system of planning, construction/performance and quality assurance is no guarantee for the faultless state of the plant. This means there is always a latent residual risk.

The effectiveness of safety systems to cope with a fault sequence is only demonstrated when the actual operating conditions are in compliance with design assumptions. Latent failures due to insufficient verification and control were not accounted for in the fault analysis. They may cause a variation of event sequences the safety systems are not designed for.

Past examples of lack of system and verification control include the following:

> The German Biblis nuclear power plant is situated in a region exposed to earthquake risk. After the initial operation of the plant the maximum possible earthquake loads at the site were verified according to state of the art. As a result of reinvestigation characteristic parameters for the design of buildings and mounting parts were updated. The dimensioning of the mounting of safety related components was recalculated regarding the updated design assumptions. Several thousand heavy-duty dowels were mounted for the fixation of piping and other components.
>
> The justification of the changes was checked by several instances. Finally the installation of the dowels was approved. Later it was discovered that dowels were assembled incorrectly. Subsequent investigation showed that most of the dowels were affected and should be replaced. The total number of affected dowels was about 15,000. They have been mounted in a way, fixing piping and other components, not corresponding to the standard necessary to withstand certain design basis accidents (DBA) like earthquakes. This means, that the affected plant in reality was not able to cope adequately with design basis accidents.
>
> The provided system of verification and controlling was ineffective and not suitable to ensure a sufficient quality level. The interface between the different test procedures and instances were obviously not adjusted as well as they should have been.
>
> There are reasons that make plausible the ineffectiveness of the provided measures: The work is performed under difficult conditions. In an existing plant the location of mountings may be difficult to access and exposure to intolerable working conditions like dirt, high temperature or radiation may be involved. In addition, tasks during outage are usually carried out under time pressure.
>
> Eventually the common-mode failure was discovered by chance and not as a result of systematic control. Possibly the failure could have remained undiscovered. In case of an earthquake, safety related components (e.g. piping, vessel) might have collapsed and been severely damaged. The function of the different safety systems might have been affected resulting in uncontrollable plant states. The plant is not designed to cope with such type and degree of damage.

4.4 Difficulty of Root Cause Identification and Assessments

The complicated technical configuration and the multitude of functional interrelations facilitate highly complex fault event trees that might affect the safety of a nuclear power plant and indeed any nuclear facility. A combination of initial events and subsequent failures may cause a loss of required systems leading to dangerous situations, which have to be avoided. There are many intersections that facilitate a great number of different event courses. Just as well a great number of influencing variables has to be regarded: different operational modes, malfunctions, malpractices, internal and external loads. The worst case to be covered might be the result of the most adverse combination of contributing factors. This includes the

identification of relevant root causes possibly initiating serious consequences as the event tree unfolds.

In view of the enormous risk potential, the consideration of the most probable sequences seems to be inadequate to guarantee the required extraordinary safety level. However, it is documented that some design features are limited by a insufficient level of assumptions. Scenarios that really happened have been insufficiently or non comprehensively integrated into the definition of the design basis. This might have been due to the fact that some hazard scenarios are difficult to reliably forecast and describe.

For example the probability and the magnitude of impact of specific external events like earthquakes or flooding can only be determined with a high degree of uncertainty. Other external influences caused by disturbances of the grid or loss of essential infrastructure might have been considered only partially. But they become more and more important because of an increasing change of external conditions, in particular the increase in frequency and magnitude of extreme weather events due to climate change. As a result loads generated by scenarios that were supposed to be extreme have been excluded from the design basis but in reality plants may now have to cope with such events.

a) The unusual storms on 27 December of 1999 led to off-site power loss and the partial flooding of the Blayais nuclear power plant site with 900 MW_e reactors. (see 9.2.7.1 for details)

b) On 25 July 2006 a short circuit in an outdoor switching station of the grid near the Swedish Forsmark nuclear power plant caused the emergency shutdown of the reactor (scram) and, in a complex scenario, led to a number of subsequent failures at the plant. (see 9.2.5.2 for details)

4.5 Generic Faults

The capability of a nuclear power plants to cope with accidents is determined by design assumptions. The safety systems are configured to prevent and, in the case of occurrence, to control a generic set of fault conditions or sequences. Typical event sequences that might result in critical plant states have to be considered. The event spectrum should cover the range of probable failures such as the range of adverse loads and required functions.

The plant's behavior and possible event sequences are analyzed to determine the requirements to be met by the design, e.g. functionality, capacity and efficiency of installations but also preconditions like procedures, tests, tools and qualified staff.

For reasons of practicability and in view of the application of calculation programs a number of settings have to be defined. Complex interrelations are simplified to make real event situations transferable to a model. Circumstances important for the course and the control of the events have to be defined, e.g. initial conditions, system parameters, system availability, special phenomena have to be considered and the possible coincidence of different independent failures. The assumptions are not only derived from a scientific context but also postulated by engineering judgment. So the quality of design is limited by knowledge and experience. Hence the assumptions have to be verified even over the period of operation. Over the years experience feedback has been used to enhance the design characteristics and to achieve a better standardization in the range of safety concepts.

The simplification of complex information and situations is necessary but holds the risk that facts highly relevant for safety might be misinterpreted due to incomplete knowledge or uncertainties.

The control of accidents is only demonstrated for a course of events as defined in the design. If generic issues remain unconsidered even in the case of a design basis accident the plant may run into uncontrollable states. The standardization of design contains the risk of multiplying such errors throughout a number of facilities. Examples include the following:

> In July 1992 a leaking pilot valve in the Swedish boiling water reactor in Barseback caused a safety valve for the reactor vessel to open. Insulating material was washed into the suppression pool and affected the emergency core cooling system (see 9.2.6.1 for details).

The phenomena that became obvious in Barseback are transferable to other reactors in Sweden and elsewhere. By the end of 2003, it had become clear that all 34 French 900 MW reactors were facing the same problem. This is an example of generic weakness of safety analysis, which may concern a large number of facilities. The French nuclear reactors have the highest degree of standardization in the world, which is a significant advantage when it comes to experience feedback, but they are also particularly prone to generic faults.[54]

4.6 Decline in Design and Fabrication quality

The high quality of nuclear equipment components and systems is a precondition to assure high levels of safety. However, during recent years concerns have been frequently expressed among experts regarding the quality of nuclear design and manufacturing. A non-comprehensive list of examples includes the following:

> **Delivery by Atomstroyexport, Russia to Tianwan-1, China, of steam generators with damaged tubes.**
>
> Licensing and commissioning of Tianwan-1 (WWER, 1000 MW, grid connection in May 2006) was delayed by a regulatory investigation and ensuing repairs of steam generator tubing. Four steam generators were delivered in 2004 by the Russian nuclear industry under the project's turnkey contract. Non-destructive tests after trial operation of the unit without fuel showed that as many as 2,000 tubes have different cracks and defects. After thorough investigation more than 700 tubes were plugged before start-up. There is some evidence that the steam generator tubes might have suffered damage during sea transportation. The start-up of the unit was delayed by more than two years.
>
> **Design, fabrication and supply by AREVA NP to the Paks nuclear power plant, Hungary, of a fuel cleaning system with insufficient safety features.**
>
> A chemical system designed to clean 30 partially burned fuel assemblies from magnetic deposits outside of the reactor, was developed, manufactured and delivered by AREVA NP (then Framatome ANP) to the Paks nuclear power plant unit 2 (WWER-441 MW) in 2003 with design shortcomings and without full scope safety analysis. These design safety deficiencies finally caused insufficient cooling of 30 fuel

[54] Numerous generic faults have been detected in French nuclear power plants over the years. In the latest one, revealed by the French nuclear safety authority on 26 February 2007 and concerning all 58 French pressurized water reactors, it was found out that during periodical tests of key safety devices the error margins of the given test had not been taken into account. In other words, a number of tests would have registered as failed if the error margin had been counted in. This generic fault was given a level 1 INES rating.

assemblies, which were heavily damaged. The event was classified as Level 3 (accident) on the INES scale.

Design, fabrication and supply by Westinghouse to the Temelin nuclear power plant, Czech Republic, of fuel assemblies, that are bending and twisting, causing problems with control rod insertion.

By the middle of 3rd fuel cycle of Temelin unit 1 (WWER, 931 MW) there were 11 control rods (neutron absorbers) that could not be entirely inserted and at the end of the fuel cycle their number had increased to 30. In the beginning of the 4th fuel cycle (October 2005 – June 2006) there were two control rods that could not be inserted properly and at the end of the cycle their number had increased to 51. The results of the last drop test of control rods performed on 2 June 2006 demonstrated a step change in further deterioration of fuel assemblies - two neutron absorbers came to a halt above the bottom of the reactor core and the unit was shutdown about four months before the planned outage. Despite improvements to the design, in the beginning of September 2006 Temelin unit 1 started the next fuel cycle, presenting again seven control rods unable to reach full insertion. Similar problems are experienced in Temelin unit 2.

Design, fabrication and delivery by Atomstroyexport, Russia to Kozloduy unit 5, Bulgaria, of a set of control rod drive mechanisms, not properly tested after implementing design changes.

New control rod drive mechanisms were installed in Kozloduy unit 5 (WWER, 953 MW) in July 2005 during the annual outage. The unit restarted in the beginning of September 2005 and was operated at full power. However, on 1 March 2006 after a main coolant pump trip triggered the shut down of the reactor, it appeared, that three control rods remained in the upper end position. The follow-up tests identified that 22 of a total of 61 control rods could not be moved with control rod drive mechanisms. The total number of control rods unable to scram (to drop due to gravity only) remains unknown. Presumably their number was between 22 and 55. Thus, for eight months the reactor was operated at full power with an insufficient number of operable control rods.

The post incident investigation showed that the fixating electromagnets were made of improper metal and the phenomenon “detention” took place. After several months of operation this resulted in fixation and inoperability of drive mechanisms. Control rod drive mechanisms of this faulty design were delivered and installed to Tianwan unit 1 (China) and Kalinin 3 (Russia).

Significant lack of safety culture and repeated delays in the construction of Olkiluoto-3, Finland

Construction of Olkiluoto-3 (PWR, 1600 MW) is being undertaken by AREVA NP under a turnkey contract. Construction started in the beginning of 2005 and according to the original schedule the unit would have to be commissioned on 30 April 2009.

Pouring of the reactor building base slab was delayed by questions about the strength of the concrete used, according to Finnish safety authorities STUK and main

contractor AREVA NP. In the summer of 2006, STUK released a harsh report on the OL3 project[55]. It noted in particular:

> *"Detailed design (e.g. dimensioning calculations for determination of required concrete strengths and reinforcement as well as final site drawings) had not been carried out, and the time and the amount of work added for accomplishing the design had clearly been under-estimated. An additional problem was caused by the fact that the plant vendor was not familiar with the Finnish practices. (...)*
> *The case studies seem to indicate that TVO's [the utility that ordered OL3] supervision activities have not reached their goal to institute a high-level safety and quality culture in the supply chain and the construction organisation. Although an abundance of technical non-conformancies have been identified in the manufacturing of different equipment, components, and in construction as well, and these have been recorded in non-conformance reports, the observations made during the investigation show that the plant vendor and its subcontractors have not essentially improved their working practices or attitudes toward safety."*

On the specific issue of training in safety culture STUK notes significant omissions by the project management:

> *"The so-called safety culture training to all those participating in the plant delivery, as stipulated in IAEA regulations and in discussions between STUK and TVO, has in practice not been provided in most cases. One expert of TVO's quality organisation stated in the interview that, as far as he knew, this training had not been provided in any organisation. It has not been defined what the content of the training should be and who should be responsible for its provision."*

On the attitude of AREVA NC as the vendor, the Finnish safety authorities note:

> *"At this stage of construction there has already been many harmful changes in the vendor's site personnel and even the Site Manager has retired and [has been] replaced. This has made overall management, as well as detection and handling of problems difficult. (...) The incompetence in the constructor role becomes obvious in the preparations for concreting of the base slab. (...) The consortium has a habit of employing new people for problem solving, which seems to have resulted in even more confusion about responsibilities."*

Manufacturing of the reactor pressure vessel and steam generators, carried out in Japan, is also behind the original schedule, those delays were connected with the qualification of welders for the manufacturing work. The delay in construction of the reactor is currently estimated at about a year and a half. The unit shall now start commercial operation at the turn of the year 2010-2011. AREVA's loss is estimated at € 700 million at least. AREVA's 2006 operating income was hit hard by delays in construction of Olkiluoto-3. The group's operating income was down almost 65 % in first-half 2006 compared to first-half 2005.

[55] STUK, "Management of Safety Requirements in Subcontracting During the Olkiluoto-3 Nuclear Power Plant Construction Phase", Investigation Report 1/06, translation dated 1 September 2006; for full report see http://www.stuk.fi/stuk/tiedotteet/en_GB/news_419/_files/75831959610724155/default/STUK Investigation report 1_06.pdf

5. Classification Systems

5.1 The International Nuclear Event Scale (INES)

The International Nuclear Event Scale (INES) was introduced in 1990 by the IAEA and the OECD's Nuclear Energy Agency (NEA). On its website the IAEA has referenced INES – User's manual under the headline "Public Information Management". The foreword to the manual explains the background of the INES scale: *"Its primary purpose is to facilitate communication and understanding between the nuclear community, the media and the public on the safety significance of events occurring at nuclear installations."*[56]

The underlying objective developed for the INES scale is the differentiation between events that involve some radiation release or that have some kind of radiological effect (see Annex 1 for a detailed presentation of the scale). No event without radiological impact could go beyond Level 3. However, even the definition of Level 3 leaves a small number of events that would fit into the classification because either there is still some radiological effect or it is labeled "near accident – no safety layers remaining".

While, besides the application of the highest level for the Chernobyl accident, any of the event classifications suggested by the IAEA in its INES user manual could be debated, the most difficult classification concerns events that do not lead to immediate radiological consequences but do represent a significant degradation of the safety situation or the safety culture at a given site.

The INES manual notes: *"Each country has different arrangements for reporting minor events to the public, and it is difficult to ensure precise international consistency in rating events at the boundary between Level 0 and Level 1. Although information will be available generally on events at Level 2 and above on the scale, the statistically small number of such events, which also varies from year to year, makes it difficult to provide meaningful international comparisons."*

A key objective of the INES scale by nuclear operators and nuclear safety authorities is to supply decision makers and the public rapidly, that is within hours of an event, with a meaningful evaluation of the severity of the event. However, often it is complex to analyze and understand the potential implications of an event in a nuclear facility and the INES rating does not provide any information that would assist emergency planning decisions to be taken (most likely it would be issued too late anyway). It is even more difficult to attempt to fit an event into the scheme elaborated under the INES scale. The INES manual counts 102 pages and, in case of a significant event, operators and officials usually have other short-term priorities than making sure that the rating fits the manual. In many cases, the original INES rating is corrected much later upwards. It remains a serious question whether the short-term reassuring effect does not have two negative side effects: in the case of a serious accident, decision makers and the public might delay taking appropriate counter measures and it might seriously undermine public confidence in communication by the nuclear operators and safety authorities.

[56] see http://www.world-nuclear-news.org/pdf/INES/INES-2001-E.pdf

5.2 The US–NRC Incident Reporting System

The United States Nuclear Regulatory Commission (NRC) classifies the significance of nuclear plant events using four primary methods: (1) abnormal occurrences reported annually to the US Congress, (2) emergency conditions declared to trigger appropriate responses from local, state, and federal authorities, (3) accident sequence precursors evaluated to assess adequacy of safety margin, and (4) events reported to the International Atomic Energy Agency using the International Nuclear Event Scale (INES). These methods examine nuclear plant events independently using different criteria. Consequently, some events get reported under only one method while other events are reported by two or more methods.

A federal law passed in 1974 requires the NRC report abnormal occurrences to the Congress. The law defined "abnormal occurrences" as events determined by the NRC to be significant from a public health perspective. The NRC developed criteria to shape its determinations. The criteria guide the NRC in reporting events involving (a) moderate exposure to, or release of, radioactive material, (b) major degradation of essential safety equipment, or (c) major deficiencies in design, construction, operation, or management controls of nuclear power reactors. In its reports to Congress on events at nuclear power plants satisfying the criteria to be deemed "abnormal occurrences," the NRC often also informs the Congress about other items of interest; issues not satisfying any of the "abnormal occurrence" criteria but still considered important. For the purposes of this study, only those events NRC reported to Congress as abnormal occurrences have been used.

Federal regulations enacted in 1980 following the reactor meltdown at the Three Mile Island nuclear plant in Pennsylvania require emergency plans to be developed. These requirements include a four-tiered emergency classification system. The lowest level emergency – called a Notification of Unusual Event – is triggered when conditions indicate a potential degradation in the level of safety at the plant. When an actual degradation or potentially substantial degradation in safety levels is identified, an Alert is declared. When an actual or likely major failure of plant functions needed for public protection has occurred, a Site Area Emergency is declared. When actual or imminent reactor core damage with the potential for loss of containment integrity occurs, a General Emergency is declared. As the emergency classification level increases, more local, state, and federal entities get engaged in emergency response activities. For the purposes of this study, only events classified at the Site Area Emergency or General Emergency level have been used.

In the mid-1970s prior to the Three Mile Island accident, the NRC initiated its accident sequence precursor (ASP) program. The objective of the ASP program was to characterize the risk of nuclear plant events, determine if events have generic implications, and provide feedback to the nuclear industry on lessons learned from operating experience. The NRC selects events estimated to have a risk of reactor core damage greater than 1×10^{-6} (one in a million chance) per reactor year for further analysis. The NRC evaluates specific plant design features and operating procedures to derive the final risk value for the events. For this study, only events determined by NRC to have a final risk of greater than or equal to 1×10^{-4} (one in a 10,000 chance) have been used.

The International Nuclear Event Scale was developed in 1989. The NRC has responsibility for assessing events occurring at US nuclear power reactors and submitting reports as appropriate to IAEA.

Significant nuclear plant events can populate one or more of these reporting categories. For example, the March 2002 discovery of degradation to the reactor vessel head at the Davis-Besse nuclear plant in Ohio resulted in NRC reporting it as an abnormal occurrence to the Congress, reporting it to IAEA, and evaluating it under the ASP program. But because the damage was discovered during a refueling outage when the head was not even attached to the reactor vessel, no emergency of any level was declared. Conversely, the February 1993 intrusion by an unauthorized person within the Three Mile Island nuclear plant in Pennsylvania caused a Site Area Emergency to be declared, but the event was not reported to Congress as an abnormal occurrence and the NRC did not evaluate it under their ASP program.

While events may get reported via two or more of these four processes, this study counted an event only once. The following hierarchy was applied: (1) abnormal occurrence reports, (2) emergency classification declarations, (3) INES reports, and (4) ASP program reports. Thus, an event appears in this study as an ASP report only when it was not also reported via all three of the other processes.

5.3 The German Incident Reporting System

Events occurring in German nuclear power plants are reported to the regulatory authority according to a defined reporting system. From 1985 onwards the reporting system was defined in "Criteria for particular events in nuclear power plants"[57], released by the Federal Ministry of the Interior, which was superseded by the "Regulation on the nuclear safety delegate and on the reporting of incidents and other events"[58] of October 1992.
Relevant for the classification of reportable events is the significance for safety issues and the degree of urgency to inform the regulatory authority. There is an obligation to report in cases that more particularly fall under the following categories:

- disposal and release of radioactive materials,
- contaminations and carryover,
- damage, failure or malfunction of the safety system or other safety-related systems or components,
- damages and leakages to the piping system and vessels,
- criticality events,
- crash of loads,
- handling and transport events,
- external events,
- fire, explosion or flooding,
- events that take place before the license for initial commissioning of the plant is granted.

.

[57] „*Meldekriterien für besondere Vorkommnisse in Kernkraftwerken*"
[58] *Verordnung über den kerntechnischen Sicherheitsbeauftragten und über die Meldung von Störfällen und sonstigen Ereignissen (Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung –AtSMV)*

The classification of the events has to be conducted according to the actual evaluation at the time of detection. In an Annex to the Regulation a number of criteria for the classification of reportable events is indicated.

The report categories for reportable events are defined as:

- Category S ("Sofortmeldung", immediate reporting): Events, which have to be reported to the regulatory authority immediately, so that inspections or measures can be initiated at very short notice. These are events, which show some kind of acute safety-related deficiencies.
- Category E ("Eilmeldung", urgent reporting): Events that have to be reported to the regulatory authority within 24 hours. Due to safety issues the cause has to be identified and resolved within a reasonable timeframe. Normally these are potential (not immediate) safety-related significant events.
- Category N ("Normalmeldung", normal reporting): Events that have to be reported to the regulatory authority within five working days. Usually these events have low impact on safety issues within the approved plant status routine. These events are notified in order to identify weak spots in advance.
- Category V ("Vor Inbetriebnahme", prior to commissioning): The regulatory authority has to be informed not later than 10 working days after these events in view of safe operation later on.

The report to the regulatory authority is transmitted by phone (categories S and E) as well as by written document (all categories).

6. Role and Problems of Scale – Public Communication or Technical Rating?

The concept of simple categories that translate complex technical events into a degree of severity clearly stems from the operators' and safety authorities' legitimate desire and civic obligation to communicate quickly after an event in an intelligible manner to decision makers and to the public. Unfortunately, particularly over 15 years of practice with the INES scale reveals two major problems:

• The public has a tendency to consider the rating as a technically precise evaluation of the severity of a given event. In other words, the media and even environmental NGOs will not pay much attention to an event that has been given a Level 0 or a Level 1 rating. In fact, even Level 2 events can go completely unheard of. On the other hand, there are events that get a low rating because they do not have any immediate impact but constituted a significant potential risk (see chapter 8).

• Especially operators, sometimes also safety authorities, tend to underrate events because they have a clear interest to present the operational result of their plants free from any high incident/accident rating. In numerous cases the ratings are therefore revised in later stages of the analysis. Of course, sometimes these revisions also take place because the complete extent or potential consequences of an event had not been understood in the immediate aftermath.

7. Gross Event Numbers as Declared by Authorities

7.1 Available INES Numbers

The IAEA database containing the incidents that have been reported by member states with their respective INES rating is not publicly available and the IAEA has not responded to several explicit information requests. A small number of the most recent events in nuclear facilities (less than 20 from previous months) is available online with short descriptions at the IAEA's website (see http://www-news.iaea.org/news/topics/default.asp) but the selection and publication criteria remain unclear.

7.2 IAEA-NEA IRS Statistics

The Incident Reporting System (IRS) has been set up in 1980 and is now managed jointly by the OECD's NEA and the IAEA. All countries operating nuclear power reactors except for Taiwan and Italy are members of the system.

According to the latest overview available[59], about 80 reports are received per year on a voluntary basis from operators of currently 435 operating reactors. The number of reports has been decreasing steadily. The IRS management has only speculated about the reasons (decline of reportable events, lack of resources in some member states) In total some 3,000 events have been covered in the system between 1980 and 2002. There is no clear definition, which events should be reported. *"Events reported to the IRS are those of Safety significance for the international community in terms of causes and lessons learned."*[60]

While the exchange of information on nuclear events that is otherwise not publicly available should be of mutual interest to operators and safety authorities, the statistics of the IRS system are simply meaningless. The French example illustrates the situation: The operator EDF identifies annually between 10,000 and 12,000 events relative to safety, radiation protection, environment and transport of which 700 to 800 are declared as "significant events" or "incidents" of which about 10 are reported to the IRS.[61]

7.3 Country statistics

7.3.1 Nuclear Event Statistics in the USA

Since the Chernobyl accident, the NRC has reported 48 events involving nuclear power reactors to the US Congress as abnormal events, events at 3 nuclear power reactors involved the declaration of a Site Area Emergency, 18 events were reported by the NRC to the IAEA under the International Nuclear Event Scale, and 49 other events had a risk of 1 x 10^{-4} (one in 10,000) per reactor per year of operation or greater per the NRC's accident sequence precursor (ASP) program. While events may have been reported to Congress and also to IAEA, there is no duplication in the tallies. If an event was counted as an abnormal occurrence report and was also reported to IAEA, it was not counted in the IAEA total to

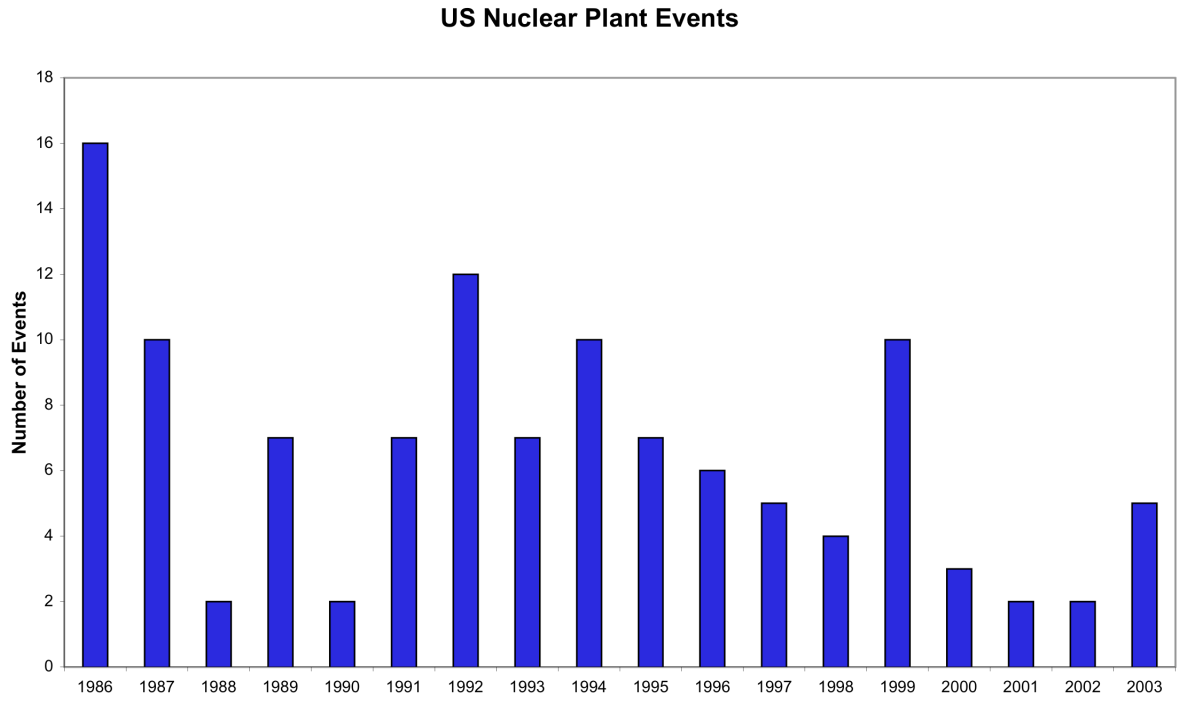
[59] IAEA/NEA, *Nuclear Power Plant Operating Experiences – From the IAEA/NEA Incident Reporting System 1999-2002,* December 2003
[60] ibidem
[61] Martial Jorel, Directeur de la sûreté nucléaire, IRSN, personal communication, e-mail 19 February 2007

avoid double-counting a single event. In fact, a total of 22 events were rated on the INES scale: of which 6 below scale, 7 Level 0, 3 Level 1, 5 Level 2 and 1 Level 3.

There have been 118 events meeting the above criteria at US nuclear power reactors since the Chernobyl accident.

Figure 3 plots the number of events per year. The results for the past three years reflect work in progress – the NRC is currently reviewing 50 events that occurred over this period under their ASP program and it is likely that one or more will be found to have a risk of 1×10^{-4} or greater when the NRC finishes its work later this year or early next year. Any such events would be in addition to the single event for 2006 shown in the graph.

Figure 3: Incidents Subject to "Abnormal Occurrence" Report in the US 1986-2003



7.3.2 Nuclear Event Statistics in France

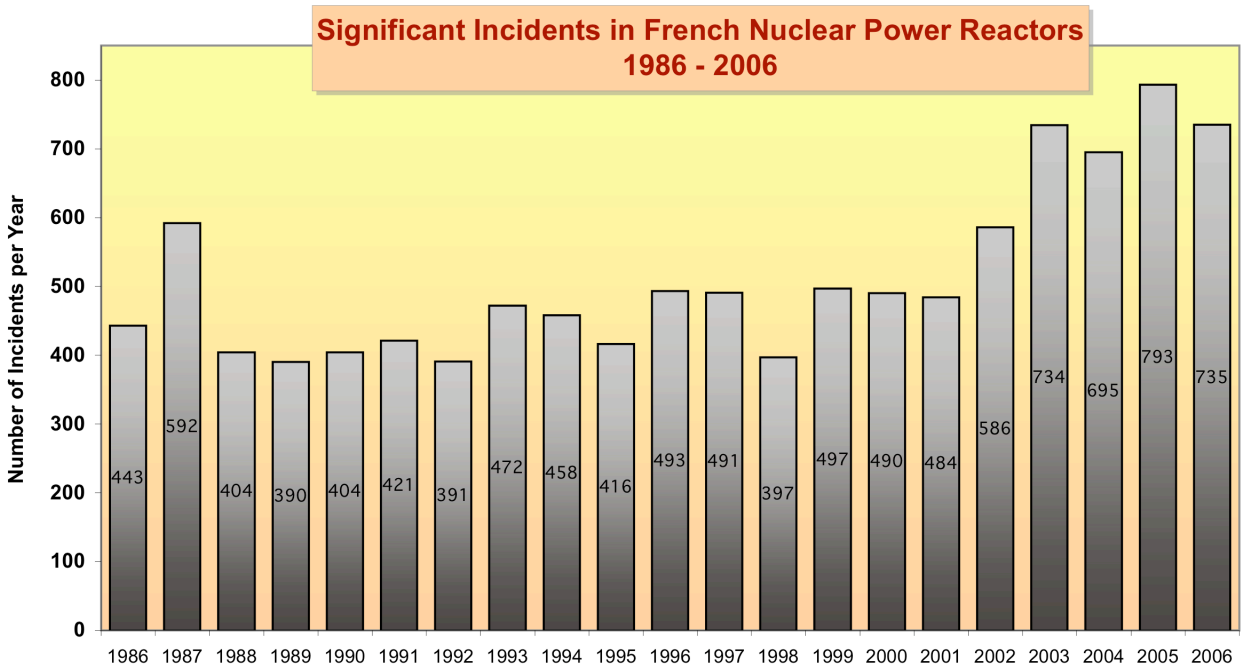
With 58 pressurized water reactors and one fast breeder reactor, France operates the largest number of nuclear power reactors in the EU, second only to the US in the world, and generates about 45% of the nuclear electricity in the EU. France also operates over 200 other nuclear facilities, from research reactors to fuel chain facilities like uranium conversion and enrichment plants, fuel fabrication and reprocessing plants as well as a number of radioactive waste storage and disposal sites.

As indicated in the previous chapter, the utility EDF declares a very large number of events every year, 10,000 to 12,000 of which 700 to 800 are considered "significant events" or "incidents".[62] The Institute for Radiation Protection and Nuclear Safety (IRSN) "examines all of these events in regular internal meetings" in order to apply a hierarchy. Certain events

[62] unless specified otherwise, the following data and quotes are from Martial Jorel, op.cit.

are considered "precursors" that put into jeopardy several lines of defense and, "under different circumstances could have led to serious consequences for safety, or even a major accident". The conditional probability for this type of event leading to damage of the core is higher than one in a million (10^{-6}) per reactor per year. Other events, considered "outstanding" (marquant), are characterized by unusual aspects, for example a new scenario, unexpected causes or potential significant consequences for safety. The evaluation of these events shall contribute to draw lessons for the prevention of operational risks. Every three months, a meeting between the operator EDF, the nuclear safety authorities (ASN) and IRSN provides the basis for the classification of the events.

Figure 4: Total number of significant incidents in French Nuclear Power Plants 1986-2006



Source: IRSN 2007

Annually the classification of these events leads to the analysis of approximately:

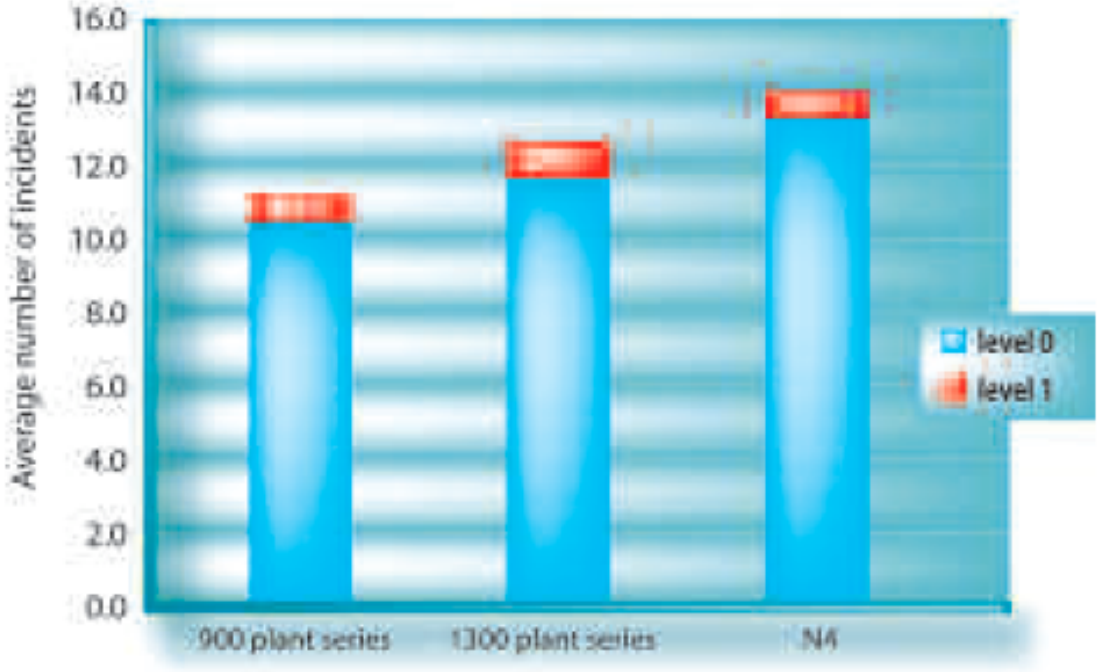
- 200 outstanding events (244 in 2006);
- 100 events retained in the framework of national lessons learned feedback;
- 20 precursor events;
- 2 to 3 in depth analysis.

It remains unclear, which of these events get what INES Level attribution according to which criteria. In its annual report 2005 the nuclear safety authority has provided the distribution of events by type of reactor.

It is remarkable that the average number of incidents increases from around 10 per 900 MW reactor per year to almost 12 per 1300 MW reactor per year and more than 13 per 1500 MW (N4) reactor per year. In other words, the more recent plants – by technology and

by operational age – encounter more incidents than the older ones. While neither operator nor safety authorities indicate specific reasons for this, age alone is certainly not an appropriate nuclear safety indicator.

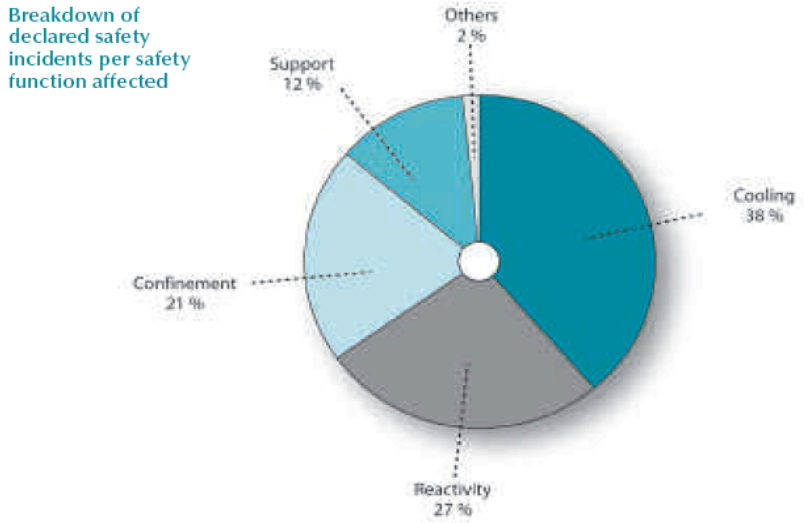
Figure 5: Number of significant events in 2005 per unit according to the reactor series



Source: ASN, Annual Report 2005

While 59% of the incidents reported from French nuclear power plants in 2005 occurred during operation over one third (37%) occurred while the reactor was shut down. Close to three quarters (73.7%) of the incidents concerned safety issues, 22.2% radiation protection and 4.1% environmental issues. A further breakdown of safety function related issues shows that 38% affected cooling, 27% control of reactivity, 21% the confinement of radioactivity and 12% various support functions (see figure 6). The latter share being on the rise over previous years.

Figure 6: Nuclear Incidents in France in 2005 by affected safety function



Source: ASN, Annual Report 2005

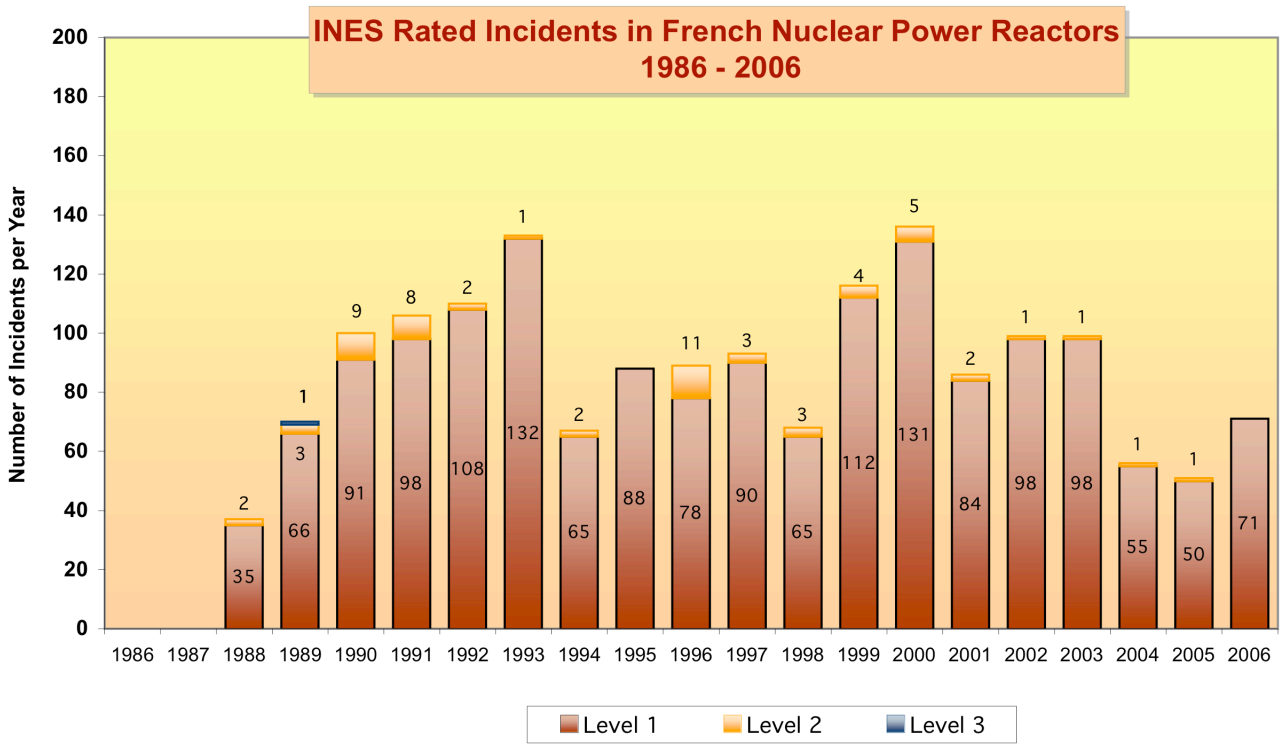
Between 1986 and 2006 a total of 10,786 significant events in French nuclear power plants were declared, of which 1,615 were rated INES Level 1 and 59 Level 2. Only one event has been given a Level 3 rating, an event that took place at the Gravelines nuclear power plant. In August 1989 it was found that the plant had been operated for about one year with a severely degraded primary circuit overpressure protection system.

It is difficult to judge the evolution of safety related incidents over time. Reporting practices, operator practices, safety authorities attitude and the technical environment changes constantly. However, certain trends can be extracted from available statistics (see following table and graphs).

After a period of relative stabilization, the total number of reported incidents from nuclear power plants doubled between 1998 and 2005. At the same time the number of incidents rated on the INES scale has gone from a peak of 131 Level 1 incidents in 2000 to 50 in 2005 before re-increasing to 71 in 2006.

The number of Level 2 events has sharply decreased from a peak of 11 in 1996 to about one per year over the last few years with none in 2006, the first time since 1995. However, it is remarkable that the peak of Level 2 events happened just the year after a zero run.

Figure 7: Annual numbers of significant events in French nuclear power reactors 1986-2006 by rating on the International Nuclear Event Scale (INES)



Source: IRSN 2007

7.3.3 Nuclear Event Statistics in Germany

In Germany there are about 120-140 reportable events in nuclear power plants each year. For the most part these events are reported as Category N ("Normalmeldung"). Only 2% to 3% of the reportable events are classified as urgent or to be reported immediately (Category E or S). In the period from 1991 to the third quarter of 2006 only three reports of Category S were issued.

For the number of reported events a declining trend can be identified for the period of 1991 to 2000 (1991: 250 reported events).

The most of the events are reported because:

- at least one of the safety devices, the safety system or one redundancy of the safety system is not available or
- there are existing safety-related deviations from the specified status of the safety system.

Furthermore there are:

- numerous indications of systematic faults of the safety system or safety-related systems or parts of the plant or
- Reductions of the wall-thickness below the reference value at equipment of the safety, main steam or feedwater systems.

These events are reported as category N.

Most of the urgent reports (category E) have been issued because:

- safety devices are just available in the number necessary by design to control an accident, without providing redundancy,
- of malfunctions of safety valves, blow-off valves or pressure relief valves or
- of fractures or cracks with leakage that necessitate a plant shutdown.

Classification according to INES

Due to the reports to the International Atomic Energy Agency events occurring in German nuclear power plants are also classified using the INES. Most of the events (more than 2,200 events since 1991) are classified as INES 0, because they are considered deviations where operational limits and conditions were not exceeded and which are properly managed in accordance with adequate procedures. These events are without safety significance. Only about 2-3%, which means 72 events from 1991 on, are classified INES 1 or higher.

INES Level 1 events

Most of the events have been classified as INES 1 because they are considered deviations from the authorized regime for the safe operation of the nuclear power plant. This may be due to equipment failure, human error or procedural inadequacies. Among these events are for example:

a) Pipe rupture due to a hydrogen explosion in the spray system in the Brunsbüttel nuclear power plant, 2001 (see 9.2.4.1 for more details) and

b) Design error of emergency power supply control and control of emergency cooling and residual heat-removal system (partial failure of the residual heat removal system as well as possible failure of the core flooding and refilling systems) also in the Brunsbüttel nuclear power plant, 2002.

INES Level 2 events

In German nuclear power plants three events were given an INES Level 2 since 1991:

a) During two of these events, the emergency and heat-removal system was affected. This concerns two consecutive events, which both occurred at the Philippsburg-2 plant in 2001. A shortfall of the specified filling level of the flooding tanks during the start up of the plant was detected late because of false data interpretation. The effectiveness of core cooling was however assured with the lower filling level.
The proper refilling of boric acid did not take place because of the incorrect position of a manually operated valve which in turn lead to the failure of three safety systems that would have been essential in case of a critical plant state. It took the operators 15 days to detect the under-boration and four days more to resolve it. Additional analysis showed, however, that sub-criticality remained guaranteed on the long-run even in failure mode condition.

b) In 1998 lack of verification at the Unterweser plant led to the unavailability of three main steam safety valve stations after the plant had been in standby mode**.** The safety of the plant was not endangered because of three redundant installations.

Human errors contributed to all three INES Level 2 events (erroneous data interpretation, undetected incorrect position of a valve or omission to verify) to some degree, which have not been in accordance with the requirements of system engineering. According to the incident reports, there was no acute state of danger for the safety of the plant.

8. Selected incidents and accidents in the USA and France

8.2.1 Selected events in the USA

The seven events at US nuclear power reactors for which the NRC calculated core damage risk values of 1 x 10^{-3} per reactor year or greater are summarized in this section. The 1 x 10^{-3} (or 1 in 1,000 years or a 0.1% probability per year) cut-off may seem a low risk, but consider the proper context. If the entire fleet of 103 reactors operating in the US had an average risk of 1 x 10^{-3}, about 4 reactor meltdowns would be projected to occur over their 40-year licensed lifetimes.

a) On 3 April 1991 workers at the Shearon Harris pressurized water reactor in New Hill, North Carolina discovered damaged piping and valves within the alternate minimum flow system provided for the pumps in the emergency core cooling system. Most of these pumps are in standby mode during normal operation and start when needed to supply makeup water for cooling the reactor core. Because some of these emergency pumps deliver water at low pressure, they cannot supply water to the reactor vessel until pressure drops low enough. The alternate minimum flow system at Shearon Harris provided a place for the pump output to go until pressure dropped low

enough for the water to be sent to the reactor vessel. The piping and valve damage was serious because had an accident occurred, water needed to cool the reactor core would have instead poured out onto the floor through the ends of broken components. The NRC calculated the severe core damage risk from this event to be 6 x 10^{-3} or 0.6% per reactor year. The event was not rated on the INES scale.

b). On 6 March 2002, workers discovered significant corrosion in the carbon steel reactor vessel head at the Davis-Besse pressurized water reactor in Oak Harbor, Ohio (see 9.2.1.2 for details). The NRC calculated the severe core damage risk from this event to be 6 x 10^{-3} or 0.6% per reactor year and rated it INES Level 3.

c) On 13 June 1986, control room operators at the Catawba Unit 1 pressurized water reactor in Clover, South Carolina received indications of a reactor coolant system leak exceeding 1 gallon per minute. The normal makeup pumps could provide sufficient water to the reactor coolant system to compensate for this leakage. Five hours after the initial indication, the leak rate jumped to nearly 130 gallons per minute. This leak rate exceeded the makeup capacity of the pumps. As the water level in the pressurizer dropped due to more water leaving the reactor coolant system than was being added, the operators manually shut down the reactor. The operators also took steps to reduce the leak rate and measures to recover the pressurizer water level.
It was later determined that a weld on the letdown or bleed system piping had cracked to cause the initial leak. The letdown system allows a continuous flow of about 45 gallons per minute of reactor cooling water to go to a system that purifies it and adjusts its chemical parameters as necessary. Five hours later, the nameplate—a metal label identifying the manufacturer and operating parameters—vibrated loose from a power transformer and fell onto an electrical circuit board. The nameplate caused an electrical short that, among other things, caused the flow control valve in the letdown piping to fully open. The higher flow rate through the letdown piping caused the crack to propagate.
The NRC calculated the severe core damage risk from this event to be 3 x 10^{-3} or 0.3% per reactor year. The event was not rated on the INES scale.

d) On 17 September 1994, operators at the Wolf Creek pressurized water reactor in Burlington, Kansas made mistakes as they opened and closed valves. The reactor had been shut down 28 hours earlier for refueling. The residual heat removal system was being used to remove the large amount of decay heat still being produced by the irradiated fuel in the shut down reactor core. The erroneous valve line-up allowed nearly 9,200 gallons (35 m^3) of reactor cooling water to flow to the refueling water storage tank. The inadvertent drainage of reactor coolant water was stopped after about one minute by an operator who closed a valve.
The NRC investigated the event and concluded that, had operator intervention not occurred, the reactor core cooling by the residual heat removal system would have failed in about 3 ½ minutes. The NRC reported that restoration of reactor core cooling would have been complicated because the water in the piping for the cooling pumps would have been replaced by steam in further 2½ minutes. The operators would have had to vent the piping and refill it with water before restarting the pumps needed to restore reactor core cooling. The NRC estimated that the water level inside the reactor vessel would have dropped below the reactor core in about 30 minutes had the operators been unable to restore cooling water flow. The NRC calculated the severe

core damage risk from this event to be 3 x 10^{-3} or 0.3% per reactor year and rated it Level 2 on the INES scale.

e) On 6 February 1996, the Catawba Unit 2 pressurized water reactor in Clover, South Carolina automatically shut down from 100 percent power after main transformer problems disconnected the reactor from the electrical grid. The loss of offsite power signaled both of the emergency diesel generators to start and provide electricity to vital equipment needed to cool the reactor core. One of the emergency diesel generators started and powered its assigned equipment, but the second diesel generator failed due to a faulty capacitor in its battery charger. Workers repaired this diesel generator and connected it to its loads about 3 hours into the event. Workers repaired the transformer and reconnected the reactor to its electrical grid about 37 hours into the event.
The loss of offsite power deprived the reactor of all the equipment normally used to cool the reactor core. The initial failure of one emergency diesel generator deprived the reactor of half of the emergency equipment used to cool the reactor core during accidents. The NRC calculated the severe core damage risk from this event to be 2.1 x 10^{-3} or 0.21% per reactor year and rated it Level 1 on the INES scale.

f) On 27 December 1986, the control room operators at the Turkey Point Unit 3 pressurized water reactor in Florida City, Florida manually shut down the reactor after a malfunction in the turbine control system caused an unplanned, undesired rapid power increase. The condition should have caused an automatic shut down of the reactor, but there was a failure in the reactor protection circuit that forced the operators to respond. Shortly after the reactor shut down, the pressure in the reactor coolant system increased. A power-operated relief valve opened to limit the pressure increase by discharging some water from the system. The power-operated relief valve successfully curbed the pressure rise, but it failed to re-close when pressure dropped. Reactor cooling water poured out through the stuck open power-operated relief valve, as it had done during the March 1979 reactor meltdown at Three Mile Island. Unlike at Three Mile Island, the operators at Turkey Point Unit 3 recognized the problem and promptly closed a second valve downstream of the stuck open valve to terminate the loss of coolant accident. The combination of the reactor's failure to automatically shut down when conditions warranted it and an equipment failure causing a loss of coolant accident were key factors in the NRC calculating the severe core damage risk from this event to be 1 x 10^{-3} or 0.1% per reactor year. The event was not rated on the INES scale.

g) On 20 March 1990, the Alvin W. Vogtle Unit 1 pressurized water reactor was in the 25th day of a refueling outage. The reactor coolant system was drained for mid-loop operation. In this configuration, the upper portions of the reactor vessel and the steam generators were emptied of water to allow inspections and maintenance on components such as the steam generators and pressurizer. The reactor core in the lower portion of the reactor vessel remained covered with water. A single residual heat removal pump circulated water through the reactor core to remove decay heat, maintaining the water temperature at approximately 90ºF. One of the two main power transformers and one of the two emergency diesel generators were out of service for maintenance. The containment equipment hatch was open.
A truck in the plant's electrical switchyard backed into a support column for a transmission line providing power to the in-service transformer. A phase-to-ground

electrical fault de-energized the transformer and disconnected the reactor from its electrical grid.
The only available emergency diesel generator automatically started on the loss of offsite power, but it shut down about 80 seconds later due to sensor problems in its control circuit. The operators declared a Site Area Emergency when ac power had not been restored 15 minutes into the event.
About 18 minutes into the event, operators manually restarted the available emergency diesel generator, but it shut down about 70 seconds later. About 36 minutes into the event, operators manually restarted the available emergency diesel generator in emergency mode, which bypassed most of the protective trips for the diesel generator. They connected the emergency diesel generator to its electrical bus and restarted the residual heat removal pump to re-established reactor core cooling. In the 41 minutes it took to restore reactor cooling, the reactor water temperature increased from 90ºF to 136ºF.
Workers closed the containment equipment hatch about 80 minutes into the event. Their efforts were slowed by lack of procedural guidance.
The interruption of reactor core cooling coupled with delay in re-establishing containment integrity represented a risky situation because things could have led to a reactor meltdown without a barrier against release of radioactivity to the environment. The NRC calculated the severe core damage risk from this event to be 1×10^{-3} or 0.1% per reactor year. The event was not rated on the INES scale.

These events reflect a range of reactor safety challenges. Three events involved an actual loss of reactor coolant inventory while two others involved the potential for loss of reactor coolant inventory. Loss of reactor coolant inventory events have two high risk components. First, they involve reductions in the amount of water available to cool the reactor core and prevent damage from overheating. Second, they involve a breach in at least one of the barriers between lethal radioactive materials and the environment. Loss of reactor coolant inventory events pose an increased risk of core meltdown coupled with decreased likelihood of containing radioactive releases. Two events involved a loss of offsite power with impairment of the onsite backup power supplies that complicated reactor core cooling capabilities. Loss of power events have high risk because electricity is needed to power and control equipment used to cool the reactor core and provide containment integrity. Four events occurred or were discovered while the reactors were shut down while three occurred while the reactor was operating, illustrating the fact that reactor cooling must be provided at all times and not just when the reactor operates. All events occurred at pressurized water reactors, even though this type of reactor comprises about two-thirds of the US reactor fleet.

If there is a common thread among these events, it is complication of the initial cause by pre-existing or undetected equipment problems. Nuclear power plant safety relies on a defense-in-depth concept seeking to put many barriers between a problem and harm to the public. This concept is embodied in multiple backups intended to cope with a pump or valve failure with a fully redundant pump or valve that performs the necessary safety function. These high-risk events demonstrate the vulnerability when nuclear power reactors operate with pre-existing and undetected impairments – it takes fewer steps to reach nuclear disaster.

8.2.2 Selected events in France

The French nuclear safety authorities ASN have provided the authors with a database containing a list of about 10,800 events declared by EDF between 1986 and 2006. ASN had also been requested to provide the present project with a selection of maximum 20 events n nuclear power plants that ASN considers as the "most significant" ones. ASN responded that "the incidents considered by ASN as the most significant are the events that have been subject to a rating on the INES scale superior or equal to [Level] 2".[63]

The French IRSN, the French nuclear safety authorities' Technical Support Organization (TSO), has provided the authors, also on request, with a list of events that took place between 1986 and 2006 considered the most significant by the organization. IRSN has selected 18 events in French nuclear power plants and 18 events in nuclear reactors outside France.[64]

The INES rating of the 18 events that took place in France since 1986 selected by IRSN as the most significant was as follows:

- 1 x INES Level 3
- 9 x INES Level 2
- 7 x INES Level 1
- 1 x unrated

Considering the fact that over the period there were 59 events that were given an INES Level 2 rating, it is remarkable that seven of the 18 selected by IRSN as the most significant events were given a lower rating.

The IRSN selection is additional evidence of the limited technical meaning of the INES rating. It is all the more surprising that the French safety authorities, that had received the information transmitted by IRSN to the authors a full week prior to its own response, simply point to INES Level 2 and 3 events.

IRSN has chosen the events according to "a number of technical elements principally based on the contribution in terms of experience feedback for the safety of the installations". The selected incidents also "illustrate the main safety problems and the specific risk for each type of nuclear installation". The selection therefore "does not correspond to a simple sorting according to a single criterion, as for example the rating on the INES scale". IRSN comments further on the INES scale by stating that "it should be recalled that this scale is aimed at providing the public with synthetic data on the severity of the incident, while the analysis carried out by IRSN aims at providing technical elements contributing to the decisions to be taken in order to increase the safety level of the facilities."

The list provided by IRSN attempts to collect, beyond any concern of hierarchy, incidents with different real or potential consequences and of a different degree of real or potential severity. The selection has been made with help of computerized databases that

[63] Marc Stoltz, Director for the Environment and Emergency Situations, ASN, personal communication, e-mail dated 23 February 2007

[64] The request was asking for a maximum of 20 events each in France and outside France.

”ease the comparison of technical data, the identification of recurring events and the elaboration of statistical elements”.

The IRSN selection covers the following events[65] in French nuclear power plants (by chronological order):

• 12 January 1987, Chinon-B3, not rated on INES scale
The particularly cold conditions during the winter 1986-87 led to the freezing of several materials and systems significant for the safety of the unit, in particular at the level of feed water intake from the Loire river.

• 16 August 1989, Gravelines-1, INES Level 3
The mounting of an inappropriate type of screws onto pressure relief valves on the primary circuit would have rendered the overpressure protection system inefficient. The valves would have opened and closed significantly later than under design basis conditions. The operators did not agree to the Level 3 rating and initiated, in vain, a procedure to get it downgraded to Level 2.

• 30 October 1990, Cruas-4, INES Level 1
The explosion of a 6.6 kV commutator caused a fire that entailed the loss of one of the two electrical safety circuits. The destruction of the commutator was caused by the degradation of elastic washers due to the exposure to heat. Subsequently, the second line was found to be affected in the same way.

• 23 September 1991, Bugey-3, INES Level 2
A leak was identified during the decennial primary circuit pressure test on the support of the control rod drive mechanisms that was going through the reactor vessel head.

• 29 January 1994, Bugey-5, INES Level 2
The reactor was shut down and the primary coolant level was decreased to working level in order to carry out some maintenance operations. The water flow level at the primary pumps and the motor intensity fluctuated for eight hours without any operator intervention. The technical specifications explicitly require close supervision of these parameters under these operational conditions because fluctuation can indicate the degradation of the primary pumps leading to their potential loss and thus the risk of core degradation. The safety authorities identified “significant malfunctioning”: the manual was erroneous, the operators had not received any specific training for this “particularly delicate” operation, the situation has been considered falsely as “normal and safe”, the visit of the safety engineer in the control room did not lead to any corrective action.[66] The event had originally been given an INES 1 rating.

[65] The following short description of the incidents also draws on other sources, in particular on the bulletin of the French nuclear safety authorities.
[66] Bulletin Sûreté Nucléaire, n°97, 3/1994

• **12 May 1998, Civaux-1**, INES Level 2
While the unit was shut down, a 25 cm diameter pipe cracked open due to thermal fatigue and a large leak (30 m3 per hour) occurred in the primary cooling circuit. It took 10 hours to isolate the leak. An 18 cm long crack was on a weld was identified. The unit, which is one of the four most modern French reactors (N4, 1500 MW), had been operating only for six months. (see 9.2.2.2 for details)

• **10 June 1999, Tricastin, then identified on all 58 EDF units**, INES Level 1
Polyamide cages, non-qualified for accidental situations, instead of metal cages have been built onto ball bearings of coolant safety injection pumps. First identified at the Tricastin site, the problem turned out to be spread over all of EDF's nuclear power plants.

• **11 March 1999, Tricastin-1,** INES Level 1
Following a series of organizational and human errors, a technician has penetrated into a protected, highly radioactive area of the reactor (red zone) and has received a dose of about 340 mSv (17 times the current legal limit for worker exposure).

• **27 December 1999, Blayais-2**, INES Level 2
The unusual storms at the end of 1999 led to the flooding of the Blayais nuclear power plant site. Certain key safety equipments of the plant were flooded, for example the safety injection pumps and the containment spray system of units 1 and 2. The electrical system was also affected. For the first time, the national level of the internal emergency plan (PUI) was triggered. The IAEA's Operational Safety Review Team (OSART) report on Blayais notes "The plant's communication department has had a hard task after the 1999's flood to recover the lost credibility, but now the situation is considered to be good again."[67] (see 9.2.7.1 for further details)

• **2 April 2001, Dampierre-4**, INES Level 2
Following human and organizational errors, the correct core loading scheme has not been implemented. The situation could have led to a criticality risk.

• **21 January 2002, Flamanville-2**, INES Level 2
The installation of inappropriate condensers due to an inappropriate procedure led to the simultaneous loss of several control-command boards and systems while the unit was operating as well as to the destruction of two safety significant pumps during the shut down sequence.

• **24 December 2003, all 900 MW reactors (34 units)**, INES Level 2
The misconception of the reactor sump filters induced the potential risk of debris blocking the cooling function in case of the need for recirculation under post-accident conditions. The problem has been subsequently identified not only in all of the French 900 MW reactors but also in many other plants around the world.

[67] IAEA, *Report of the Operational Safety Review Team (OSART) Mission to the Blayais Nuclear Power Plant*, 2 - 18 May 2005, IAEA-NSNI/OSART/05/131

• 24 January 2004, Fessenheim-1, INES Level 1
Following the erroneous operation of an auxiliary circuit valve, ion exchange resins[68] have been introduced into the primary cooling circuit. Their presence could have threatened the integrity of the primary pump joints as well as the proper functioning of the control rods. Both elements are essential to control and shut down the reactor.

• 22 March 2004, all 58 EDF reactors, INES Level 2
An insulation default at an electrical switchboard, experienced on unit 2 of the Penly nuclear power plant, was triggered by a steam leak close to electrical equipment that was to be qualified to resist accidental conditions. The non-conformity of the cabling has been subsequently identified on all of the French nuclear power plants and led to large-scale verification and remediation operations.

• 16 May 2005, Cattenom-2, INES Level 1
The sub-standard of the secondary coolant pump power supply cabling led to a fire in the electricity funnel. As a consequence one of the two safety circuits had to be disconnected. The operator EDF triggered its local (Level 1) internal emergency plan (PUI) The technical emergency center (CTC) has been activated for a few hours. The nuclear safety authorities issued a nine-line press release. Details of the event have never been published.

• 7 April 2005, Gravelines-3, INES Level 1
During the year 2006 the operator has noticed the presence of provisional pieces of equipment on both of the reactor protection control command lines. These pieces were applied during the previous reactor outage and had been left there by mistake. Under accidental conditions certain automatic sequences would not have taken place in a normal way.

• 30 September 2005, Nogent-1, INES Level 1
A certain number of material failures added to a human error during the restart of the reactor led to the hot water and steam penetrating the four rooms containing the control command boards of the reactor protection system. Under normal conditions these rooms are independent from each other and should never be put in danger simultaneously. In the case of an accident, this incident could have made it difficult for the operator to bring back the reactor into safe state. EDF has activated its internal emergency plan and the nuclear safety authority ASN activated its national emergency organization for a few hours. ASN issued a 10-line press release.

• 21 December 2005[69], Chinon-B (four units), INES Level 1
An ill-conceived surveillance of the tertiary cooling water intake canal led to its significant silting up. The collapse of the sand hill could have led to the heat sink loss of all four reactors.

[68] Synthetic material used to selectively remove dissolved contaminants such as heavy metals or radionuclides from water by replacing or exchanging them with other constituents.
[69] As dated by IRSN, the safety authorities technical support organization. According to a database transmitted by ASN have dated the incident on 30 December 2005 and notes it as declared by EDF on 4 January 2006; Marc Stoltz, database transmitted by e-mail to the project coordinator, personal communication, 23 February 2007

9. Residual Risk Project Selection of Nuclear Events 1986-2006

9.1 Definition of selection criteria

Hundreds of significant events take place in every major nuclear country every year, several thousand worldwide. There is no internationally agreed methodology for an established reporting threshold and type classification of these events. In fact, even official organizations in a given country often do not agree about the classification of events. The IAEA INES has been developed for public communication purposes and as such has served operators and nuclear safety authorities usefully. It is therefore not surprising that operators frequently underrate incidents, at least in the short term, and even attempt to negotiate with safety authorities to lower a given rating.

However, INES is not an appropriate tool for the technical evaluation of the risk level entailed by a specific event or its potential significance for nuclear safety.

In the absence of a recognized uniform evaluation tool, the authors have questioned nuclear safety authorities and technical support organizations and have studied published listings and event evaluation reports from the past 20 years.

The authors of the present study neither wish to present a ranking of nuclear incidents nor claim to have identified *the* most significant events.

The following selection of events is based to some extent on the evaluation that has been provided by national organizations in France (on request), on accident probability calculations in the case of the USA (severe core damage probability) and on the appreciation of the experts involved in the project. In most of the cases there is a consensus as to the particular significance of the incidents.

The IAEA did not respond to repeated information requests.

9.2 Selection of events by type of incident

Rather than attempting to provide a world overview, an ambition that would have gone far beyond the scope of the project, the authors chose to select a number of events that seem typical or particularly severe for a given family of events. Many times the significance of a given incident is considerably amplified by the fact that it reveals a generic problem for a number of plants and, indeed, sometimes for an entire series of reactors (>10), and sometimes for an entire reactor type (>100).

The availability and paucity of information also played a significant role for the selection. The fact that events from certain countries are discussed while most of the 31 nuclear countries are not represented is no indication of the frequency or absence of events. The core of the report provides numerous other examples that could equally have been selected as exemplary. However, there are countless events that are insufficiently documented or not documented at all. And, no doubt, there are many incidents that the international public has never heard of.[70]

[70] In the United Kingdom, for example, incident reporting has become extremely restrictive in the few years following the 9/11 terrorist attacks with the Nuclear Security Regulations 2003 rendering it an offence for any person to provide information on nuclear sites and/or activities that could assist at the planning and/or implementation of a malicious act.

The events are presented by event family rather than by country or date. However, there are numerous events that would qualify for several event categories. The dates either indicate the point of discovery of an event or the beginning of an incident or the first time that a generic problem has been identified.

9.2.1 Advanced Material Degradation (before break)

There are many material degradation mechanisms (see chapter 3) that can lead either to severe damage of safety relevant systems or render them inoperable. The following two examples illustrate how close – literally millimeters – to severe accident conditions nuclear power plants have come in the past 20 years.

9.2.1.1 3 April 1991 Shearon Harris (USA)

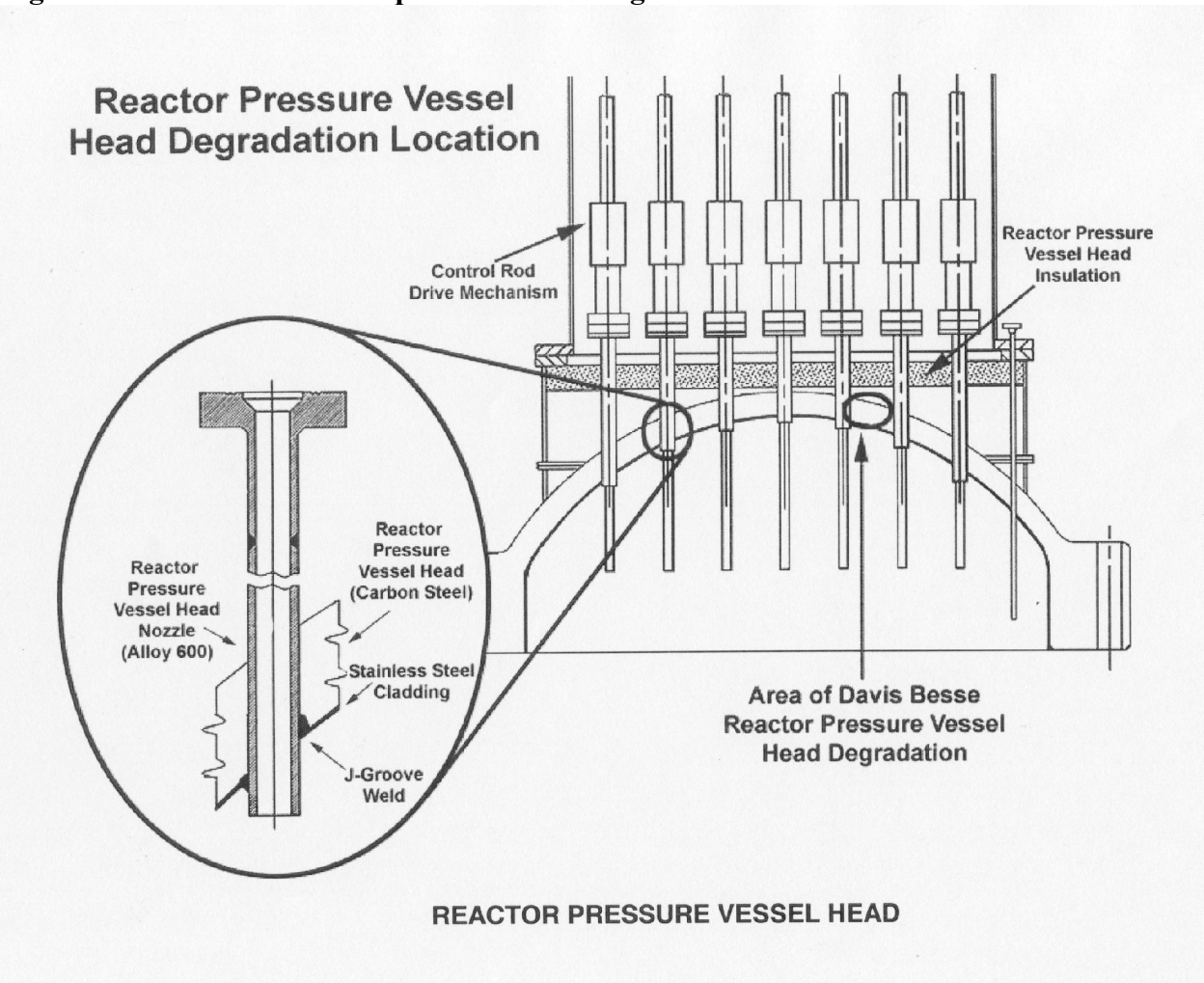
On 3 April 1991, workers at the Shearon Harris pressurized water reactor in New Hill, North Carolina discovered damaged piping and valves within the alternate minimum flow system provided for the pumps in the emergency core cooling system. Most of these pumps are in standby mode during normal operation and start when needed to supply makeup water for cooling the reactor core. Because some of these emergency pumps deliver water at low pressure, they cannot supply water to the reactor vessel until pressure drops low enough. The alternate minimum flow system at Shearon Harris provided a place for output of the pumps until pressure dropped low enough for the water to be sent to the reactor vessel. The piping and valve damage was serious because, had an accident occurred, water needed to cool the reactor core would have instead poured out onto the floor through the ends of broken components. The NRC calculated the severe core damage risk from this event to be 6×10^{-3} or 0.6% per reactor year, an accident probability as high as in the case of the Davis-Besse incident (see hereafter).

9.2.1.2 6 March 2002 Davis Besse (USA)

On 6 March 2002, workers discovered significant corrosion in the carbon steel reactor vessel head at the Davis-Besse pressurized water reactor in Oak Harbor, Ohio. The head is bolted onto the reactor pressure vessel containing the reactor core during operation. There are sixty-nine holes in the head that allow control rods inside the reactor vessel to be connected to their external motors. There are stainless steel tubes, called control rod drive mechanism nozzles, through each hole and welded to the stainless steel inner liner of the head. It is believed that one of these tubes developed a crack around 1991. By 1996, the crack extended all the way through the metal wall of the control rod drive mechanism nozzle and began leaking borated reactor coolant water. The leak rate was small, less than 1 gallon per minute, but it persisted for nearly 6 years.

Rust-laced boric acid "river" flowing through inspection ports on the reactor head and down onto the reactor flange during the refueling outage in 2000.

Figure 8: Davis Besse reactor pressure vessel degradation



When the leaked water evaporated, it left behind dry boric acid crystals. Boric acid is very corrosive to carbon steel. It began eating through the carbon steel head. By 2002, there was a pineapple-sized hole in the head. The boric acid had completely eaten through the 150mm thick carbon steel wall to expose the stainless steel liner. The liner was applied to the inner surface of the carbon steel reactor vessel and head for protection against the corrosive borated water. The liner was not intended to be pressure-retaining, but for years it was the only barrier preventing a loss of coolant accident. As boric acid widened the hole, the stress loading of the liner increased. A government study estimated that the hole would have widened to the point where the liner ruptured in another 2 to 11 months of operation by Davis-Besse. Because Davis-Besse ran 18 months between refueling outages, had the damage been missed during the 2002 outage, it seems likely that a loss of coolant accident would have occurred.

Many warning signs had been overlooked since the leak began in 1996. During refueling outages in 1998 and 2000, workers discovered boric acid blanketing large portions of the reactor head. Nearly a decade earlier, the company had committed to the NRC to completely clean up all boric acid spills to check if there was corroded metal underneath. Workers attempted to remove the boric acid from the head, but management did not extend the outage duration to allow them to finish the work. During 1999, small rust flakes blowing up into the air from the widening hole clogged the filters on monitors inside the containment that continuously sampled the air for radioactivity. Management sent workers into

containment to replace the filters. During the refueling outage in 2000, workers removed bucket after bucket of boric acid crystals and rust flakes from the air conditioning coils inside containment. The company's management explained to the NRC in August 2002 that it overlooked these, and many other warning signs, because it placed generating revenue ahead of assuring safety.

Had the 5mm stainless steel liner ruptured, a hole with a diameter of approximately 250mm would have created a medium-sized loss of coolant accident. While Davis-Besse was equipped with emergency systems to mitigate such an accident, these backup systems were also found to be impaired. The worst problem involved the containment sump used during the second phase of accident mitigation. In the first phase, emergency pumps transfer water from a large storage tank adjacent to the containment building into the reactor vessel to compensate for the cooling water pouring out the 250mm diameter breach. The water pouring out of the reactor drains to the bottom of the containment building where it collects in a concrete pit called the containment sump. Before the storage tank empties in about 30 to 45 minutes, the operators realign the emergency pumps to take water from the containment sump and send it to the reactor vessel. Workers found that the debris created by water jetting out through the hole (e.g., insulation and coatings scoured off piping and components) in addition to pre-existing debris inside containment (e.g., paint applied to the inner surface of the containment dome

The large hole in the reactor vessel head around the vessel head nozzle.

was peeling and falling to the floor during routine plant operation) would be transported by the flowing water to the containment sump where it would clog the protective screens and deprive the emergency pumps of the water they needed. Before Davis-Besse restarted in March 2004, workers enlarged the containment sump screens by a factor of 25 and upgraded insulation and coatings so as to reduce potential debris sources.

The NRC calculated the severe core damage risk from this event to be 6×10^{-3} or 0.6% per reactor year and rated it INES Level 3.

9.2.2 Significant Primary Coolant Leaks

A loss of coolant accident in a nuclear power plant is always highly significant to the safe state of the facility since the failure to evacuate the heat from the reactor core can threaten the integrity of the nuclear fuel. There are hundreds of kilometers of tubes in a nuclear power plant and the thousands of steam generator tubes represent the largest part of the primary circuit boundary. That is where heat from the primary circuit is transferred to the secondary circuit. Steam leaving the generators drive the turbines that produce the electricity. Leaks can appear in any of the operational or backup safety systems.

9.2.2.1 18 June 1988, Tihange-1 (Belgium)

Tihange 1 is an 870 MWe pressurized-water reactor located at Tihange, Belgium. On 18 June 1988, while the reactor was operating, a sudden leak occurred in a short, unisolable section of emergency core cooling system (ECCS) piping. The operator noted increases in radioactivity and moisture within the containment and a decrease of water level in the volume control tank. The leak rate was in the order of 1,300 liters per hour, and the source of leakage was a crack extending through the wall of the piping.

The crack, which was in the base metal of the elbow wall and not in the weld or heat-affected zone, 90mm long on the inside surface of the elbow and 45mm long on the outside surface. A crack indication also existed in the spool connecting the elbow to the nozzle in a hot leg. That indication was in the heat-affected zone at the weld connecting the spool to the elbow. The indication is circumferential, extends 100mm on the inner surface of the spool. Circumferential cracks are considered much more dangerous than longitudinal crack because they have a higher risk of not leaking before they break (which makes early detection more difficult). Two smaller crack indications exist in the vicinity of the weld connecting the elbow to the check valve. The origin of the defects is identified as thermal fatigue (material stress due to thermal shocks from alternate exposure to heat and cold).

The risk of a pipe rupture in the emergency core cooling system is considerable in the case of the activation of the emergency safety injection system – large quantities of cooling water are injected in case of a loss of coolant accident – in an already degraded safety situation.

A much smaller similar leak had been detected at a similar location at the US Farley-2 plant in December 1987, but it had developed slowly and not abruptly as in the Tihange case. Subsequently, the phenomenon has been identified at the French Dampierre plant (in 1992 at unit 2 and in 1996 at unit 1) and later all 34 of EDF's 900 MW reactors were found subject to the problem. The safety authorities have in a first step only asked the operator to increase maintenance and monitoring activities on the affected plants. In the summer of 2001 the experimental modification of the circuits has been authorized in two units (Fessenheim-1 and Dampierre-2). It is only at the end of 2003 that the identical modification has been authorized for the other 32 units. The current status of that program is not known. However, between the identification of the problem and the licensing of an engineered solution over 15 years went by.

9.2.2.2 12 May 1998, Civaux-1 (France)

The Civaux-1 reactor was shut down for five days, when during start-up tests, on 12 May 1998 at 19h45 a 250mm diameter pipe of the main residual heat removal system cracked open and a large leak (30,000 liters per hour) occurred in the primary cooling circuit. The reactor core needs to be cooled permanently, even when it is shut down, in order to evacuate the significant amount of residual heat of the fuel. By 3:00 hours in the morning on

13 May 1998 stand-by teams from the nuclear safety authorities and its technical backup as well as additional staff from the operator EDF and the builder Framatome are activated.

It took nine hours to isolate the leak and a stable situation is reached at 5h40. It was first decided to cool the core via the steam generators, but because of the relatively low burn-up – and therefore relatively low heat output - of the fuel, the attempt fails. The unit, which is one of the four most modern French reactors (N4, 1500 MW_e), the last but one reactor to have been commissioned in France and had been operating only for six months at 50% power level maximum prior to the event. Then, the safety authorities give permission to continue cooling with the remaining line of the shutdown cooling system with modified physical parameters (low pressure, two phase flow). This state is reached on Sunday 17 May 1998 and the permanent activation status of the standby teams is lifted, after five days, in the morning of Monday 18 May 1998.

An 180mm long crack on a weld was identified and 300 m^3 of primary coolant were leaked into the reactor building. The origin of the crack was accelerated thermal fatigue because a cold leg was mounted much too close to hot water piping. Repeated thermal shock initiated the crack within a few months of operation.

In June and July 1998 the fuel was unloaded at Civaux-1 but also on the two other then operating French 1500 MW_e reactors at Chooz and similar crack indications were identified there as well.

EDF later admits that the second level of the internal emergency plan (PUI, national level) had been reached during the night of 12-13 May 1998. Apparently in agreement with the safety authorities, it was not activated. The reason is unclear. However, it should be noted that the head of the safety authorities had scheduled a large press conference in the morning of 13 May 1998 in order to release his report to the Prime Minister on the contaminated spent fuel shipment affair that had raised considerable media attention since its original revelation in France by Libération on 6 May 1998. In fact, certainly in part due to the “competing” media event, hardly anything has been published in France on the Civaux incident.

EDF suggested rating this event Level 1 on the INES scale. The safety authorities immediately decided on Level 2.

The technical problems with the N4 reactors had significant impact on their electricity generation for the year.

9.2.2.3 9 February 1991 Mihama-2 (Japan)

A steam generator tube rupture occurred at Mihama Unit 2 on 9 February 1991. This is the first such incident in Japan where the emergency core cooling system was actuated. Mihama-2 is a 470 MWe pressurized water reactor. The primary coolant flows through several thousand tubes making up the bundles in each steam generator (two in this case) where the heat is transferred to secondary water, which leaves the reactor containment in the form of steam to run the turbines and generate power.

At 12h24 on 9 February 1991, Mihama-2 plant personnel received an "attention" signal from the steam generator. At 13h20 sampling analysis indicated a radioactivity concentration only slightly higher than normal in one of the steam generators, which would signal a small primary leak. At 13h45 hours, plant personnel manually started a third charging pump because of decreased pressure and water level in the pressurizer. At 13:48 hours, personnel began to manually reduce reactor power. At 13:50 hours the reactor shut down

automatically because of "low pressurizer water level" and the emergency coolant safety injection was activated. Leakage from the primary to the secondary circuit was essentially terminated at 14h48 hours.

The utility investigated the rupture and found that it was a complete circumferential tube failure. The utility found that the failure mechanism was high cycle fatigue caused by vibration. By design, all tubes in specific locations in the steam generator are supposed to be supported by anti-vibration bars. However, the subject tube was not found to be supported appropriately because of a reported "incorrect insertion" of the adjacent anti-vibration bars.[71]

The Mihama incident triggered the adoption of an audit system by the utility TEPCO under which non-nuclear power sections of the company would audit nuclear power stations. However, the Nuclear and Industrial Safety Agency (NISA) has been highly critical of the scheme: "An audit team of five employees, who are with the Audit and Operational Development Department, merely conducts a nuclear power audit at each plant site twice a year for three days each. Since the initiation of the audit system, the auditing program has not been reassessed at all. In addition, the audit team informs the power station of the items it has decided to audit before actually carrying out the audit. Thus, the value of the system is suspect. Moreover, because the audit team includes members who are not engaged in nuclear-related work and because such an audit requires high expertise, the thoroughness of the audit is open to question."[72]

9.2.3 Reactivity Risks

The basic principle of a nuclear reactor is controlled nuclear fission. There are various means to control the nuclear chain reaction, in particular the insertion of control rods into the core and the injection of borated water. Both means aim to slow down the nuclear reaction by introducing neutron absorbing substances (e.g. boron) and/or physical neutron "breaks". Any disturbance of the system has potential far reaching consequences, especially in case of an accident that needs fast and efficient control of the nuclear reaction.

9.2.3.1 12 August 2001, Philippsburg (Germany)

In August 2001 in the German Philippsburg nuclear power plant a deviation from the specified boron concentration – a neutron absorber needed to slow down or stop the nuclear reaction – in several flooding storage tanks during restart of the plant was reported to the authorities. Later the report was completed by the fact that also the liquid level had not reached the required value fixed in the operational instructions for the start-up and was only implemented with a delay.

Subsequent investigations revealed that significant deviations from requirements during start-up and violations from related instructions seemed to be common probably for several years and took place in a similar way in other German nuclear plants. The over all extent of the violations was not clearly comprehensible from the available documentation.

---

[71] US-NRC, Information Notice No. 91-43, 5 July 1991

[72] NISA, *Interim Report on the Falsified Self-imposed Inspection Records at Nuclear Power Stations,* Nuclear and Industrial Safety Agency, 1 October 2002,

The flooding tanks are used for the storage of large quantities of boron-treated water. A special boron concentration has to be adjusted in the coolant to control the reactivity in the reactor core. The water quantity is dimensioned to ensure a sufficient heat transfer from the reactor core at any time and to compensate for the potential loss of coolant in the primary circuit. Temporary other coolant inventories, especially the content of the primary circuit, can be depleted into the storage tanks due to performance of particular maintenance or test activities. The water management has to ensure a sufficient amount and a sufficient boron concentration in the coolant to control all possible events at any time. The emergency cooling will only work effectively if it is operated according to design basis conditions.

Due to the violation of rules and regulations the available amount of conditioned cooling water was repeatedly insufficient during the start-up sequence. During these occasions the efficiency of the emergency cooling system and the capability of the plant to cope with possible accidents were limited. Possible accidents during start up could have led to uncontrollable states of the plant.

The deviation from specified values was accepted. Administrative control measures to ensure the orderly performance of procedures were ineffective or missing.

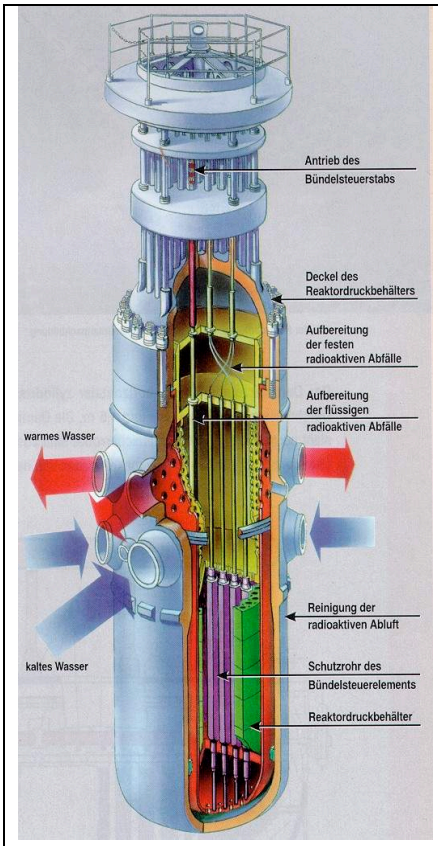
The findings of the comprehensive assessment gave reasons to start an extensive discussion on the importance of safety management in nuclear power plants. It was estimated that the continuous and systematic violation of rules and regulations in general holds the potential for severe consequences in many safety related contexts. The safety authority requested the systematic implementation and enhancement of safety management. The discussion how to control the effectiveness of safety management and to ensure the required standard of safety performance is not yet completed. Different approaches were presented and have to be verified in view of practicability and efficiency by future experience.

There are many other incidents that demonstrate the incompleteness of administrative measures to ensure safety.

9.2.3.2 1 March 2005 Kozloduy-5 (Bulgaria)

The Bulgarian Kozloduy nuclear power plant is state owned. Six units were constructed at the site, all of them of the Russian WWER design. The units were connected to the grid in 1974, 1975, 1980, 1982, 1987 and 1991 accordingly. Units 1-4 are WWER-440 Model 230 and units 5-6 are WWER-1000 Model 320. Units 1&2 were shutdown in 2002 and Units 3&4 were shutdown in 2006 as part of the Bulgarian EU accession agreement.

Introduction



During the annual repair and refueling period July – August 2005 all driving mechanisms of Cluster Control Rod Assemblies (CCRAs) of unit 5 were replaced, as a part of the modernization program. This program was partially financed under a EURATOM loan. The new driving mechanisms were designed and manufactured by the Russian company Gidropress. Some new materials were introduced in their design, trying to increase their operational life up to 30 years. These machines were tested in one of the Russian WWER-1000 plants, but they were installed only for the control rod assemblies in bank No 10. During reactor operation this bank of control rod assemblies controls the reactor power and is almost permanently in motion. No driving mechanism was tested in banks 1-9, which stay in their top position, waiting for a scram signal (to drop down and thus shut down the reactor).
It is unclear whether design changes as well tests were authorized by the Russian Nuclear Safety Authority. It is still even unclear weather the manufacturer of this equipment was licensed by the Russian Nuclear Authority.

Development and causes of the incident

On 1 March 2006 Kozloduy unit 5 was operated at full power. At 06:08 AM due to electrical failure, one of the four main circulation pumps tripped. Following this initiating event, to enable rapid power reduction the system automatically reduced the power to 67% of

nominal capacity. In the process of power reduction the operators identified that three control rod assemblies remained in upper end position.

The follow-up movement tests of remaining control rod assemblies identified that in total 22 out of 61 could not be moved with driving mechanisms. The number of control rod assemblies, unable to scram (to drop due to the gravity only) remains unknown. Presumably their number was between 22 and 55. Multiple attempts have been made to set in motion the drives remaining in upper position and as a result only eight of them recovered their design characteristics.

At 12:45, more than six and one-half hours after detecting the failure, the reactor was shut down with the use of the boron system - feeding the primary circuit with highly borated water that absorbs neutrons and slows down the nuclear reaction. Then the reactor was cooled-down and actions were taken to clarify the case. Three of the driving mechanisms (that remained in upper end position) were dismantled and investigated. As a result of the visual inspections, measurements and experiments, it was identified that the direct cause of lack of movement was "detention" in the foreheads of the movable and immovable poles of the fixing electromagnet. Once driving mechanisms are set in motion, the "detention" phenomenon is no more observed and the rods perform as designed.

The general designer has proposed short-term corrective measures, mainly including periodical operability testing of the control rod assemblies of banks 1-9. The Bulgarian Nuclear Safety Authority (BNSA) accepted the proposed corrective measures and provided regulatory agreement for restarting unit 5 without any specific requirements or remarks.
In respect to the incident at unit 5, all control rod assemblies at unit 6 were tested in motion with driving mechanisms. Reportedly control rod assemblies perform as designed.

After testing of all driving mechanisms and replacement of some of them the reactor was restarted on 10 March 2006.

As a result of this incident the planned change of driving mechanisms to unit 6 in 2006 was canceled.

Severity of the incident

Control rod insertion failures are considered very serious and lead to a severely degraded state of safety in case an accident-initiating event occurs. The WWER-1000 scram system is designed to put the reactor in safe shutdown if one control rod assembly at the most is jammed in the upper position.

Operation of Kozloduy unit 5 at full power during eight months with tens of inoperable control rods is an unprecedented example in the history of nuclear power. This mode could be defined as Anticipated Transient Without Scram waiting to happen. In case of steam line break, or other initiating events, leading to fast cooling down of reactor and increase of reactivity, the ineffective scram system could not prevent severe damage of reactor core.

The INES manual defines events 2 and 3 as follows:

- Level 2 - Incidents with significant failure in safety provisions but with sufficient defense in depth remaining to cope with additional failures.
- Level 3 - Incidents in which a further failure of safety systems could lead to accident conditions, or a situation in which safety systems would be unable to prevent an accident if certain initiators were to occur.

According to these definitions the incident at Kozloduy unit 5 should clearly have been classified as Level 2 or 3. However, it took the Bulgarian authorities a long time to admit the seriousness of the incident as is illustrated by the following chronology of events.

An "information incident"

On 2 March 2006, when Kozloduy unit 5 was already shut down, Bulgarian media were informed that there was a need of "planned repair" and affirmed the reason as "necessity of system checks and additional repair work". There was no word about multiple failures in the reactor scram system.

On 10 March 2006 the Bulgarian society was informed that the "planned repair" was completed successfully and that the unit restarted operation. Bulgarian Minister of Economics and Power Mr. Ovcharov stated that now no problems in providing electricity to consumers could be expected.

On 14 March 2006 for the first time the Bulgarian nuclear safety authorities (BNSA) on their web-site made a statement about the failures in the reactor scram system. According to the safety authorities: "The root causes of the event have to be identified and adequate corrective measures for cause elimination shall be established until the unit's shut-down". It also stated: "According to the preliminary report of the nuclear power plant "Kozloduy" the event rating is evaluated as **"0" Level** of the International Nuclear Event Scale".[73]

On 24 April 2006 the German "Tagesspiegel" published an article in which an independent expert stated that the severity of the incident is higher, presumably INES Level 2 or 3. In response the Chairman of BNSA confirmed that the event would be INES **Level 0**[74] and "the BNSA Deputy Director stated that there was **no serious failure** in the emergency protection system of Kozloduy Unit 5".[75]

On 25 April 2006 for the first time BNSA informed the International Atomic Energy Agency about the incident. However the report says: "In the preliminary event report sent to the BNSA, the Kozloduy nuclear power plant rated the event as INES **Level 1**. The final INES rating will be determined by the BNSA after completing all ongoing analyses and published in NEWS".[76]

On 25 April 2006 Bulgarian Minister Mr. Ovcharov declared to the media "nothing happened on 1 March at Kozloduy nuclear power plant, and the Bulgarian society was informed about the incident in unit 5. (…) According to Ovcharov there was nothing different from normal activities that the nuclear power plant and BNSA have to perform. Ovcharov added that on 12 March BNSA has delivered comprehensive information about the event."[77]

On 02 May 2006, during a press conference, for the first time the Kozloduy management stated that there were safety shortcomings in the design of driving mechanisms and improper activities of the personal.

On 08 May 2006, during a press conference in its headquarters, BNSA announced its decision to increase the risk level of the incident that took place at the Kozloduy nuclear power plant unit 5 at 1 March 2006. According to the statement of the Chairman the final assessment is INES Level 2.[78]

The main lesson learned from this incident is that there are tremendous shortcomings in safety culture at corporate and governmental level in Bulgaria.

---

[73] cf. http://www.bnsa.bas.bg/news/060314_bg.html
[74] http://www.mediapool.bg/show/?storyid=116655
[75] Bulgarian Press Agency (BTA), Sofia, April 24 2006
[76] http://www-news.iaea.org/news/topics
[77] http://www.mediapool.bg/show/?storyid=116685
[78] http://www.bnsa.bas.bg/news/060508_bg.html

9.2.4 Fuel Degradation (outside reactor core)

9.2.4.1 Paks (Hungary) 2003

Four units are operated at the Hungarian Paks nuclear power plant, all of them WWER-440 V-213. The units were connected to the grid in 1982, 1984, 1986 and 1987. The thermal power of each unit is 1,375 MW and the total electrical power capacity of the Paks nuclear power plant is 1,755 MW. [79]

Introduction

The Paks nuclear power plant management scheduled 24 steam generator decontamination operations between 1996 and 2001 at units 1-3. The last step, passivation, was not carried out carefully and became the fundamental cause of magnetic deposits generation. They formed a significantly thick layer on fuel assemblies and reduced cooling water flow and heat transfer. Due to the increased and asymmetrical outlet coolant temperature the power of the units had to be decreased step by step and at least part of the fuel assemblies had to be replaced. Such anomaly was found in unit 2 in 1998 and resulted in its shutdown and the replacement of the entire core. In 2000 new deposits were detected in unit 3, which had to be shut down in February 2003 and the full core was replaced. When the unit was restarted core asymmetry was detected and the unit has been operating at reduced power. In 2000-2001 differential pressure measurements revealed the limitation of the cooling capacity of the fuel assemblies between 10-65 %. Chemical cleaning of the fuel assemblies has become indispensable in order to make use of the remaining fuel capacity that represented still an additional 2-3 fuel cycles. In other words, without cleaning a significant economic loss would have to be accepted.[80]

Chemical cleaning technology during 2000-2001

In 2000 and 2001 the Paks nuclear power plant contracted Siemens GmbH for the cleaning of 170 “cold” fuel assemblies (stored in the fuel pool for more than one year and with low remaining decay heat) in a 7-assembly cleaning container. The specially designed cleaning tank was installed under 10 meters of borated water in a service shaft of the spent fuel pool. 170 fuel assemblies were cleaned during approximately 10 weeks without any damage and were used in the subsequent refueling of Paks units.[81]

[79] See Third National Report of Republic of Hungary to the CNS, 2004
[80] See Report of the IAEA Expert Mission to Paks NPP, 16-25.06.2003
[81] See Fuel assemblies chemical cleaning, Report of Paks NPP and Framatome ANP, 2002

Chemical cleaning technology during 2002-2003

Decisions influenced by time pressure. In 2002 the Paks management decided to upgrade the cleaning process and equipment in order to solve the fuel cleaning problem during annual maintenance. In November 2002 the nuclear power plant commissioned Framatome ANP (the legal successor of Siemens KWU, now AREVA NP) for the designing and manufacturing of the new cleaning system, which was to be installed and ready for use by March 2003. This decision resulted in a very aggressive schedule for design, fabrication, installation, testing and operation of it. In December 2002 Framatome ANP presented preliminary design, which was not agreed with the Russian manufacturer of the fuel and with the Russian scientific manager of WWER-440. The Paks nuclear power plant submitted a license application to Hungarian Atomic Energy Agency (HAEA) on 18 December 2002 and on 24 January 2003 HAEA provided a license for the ex-core fuel cleaning, with only one comment on the safety analysis.

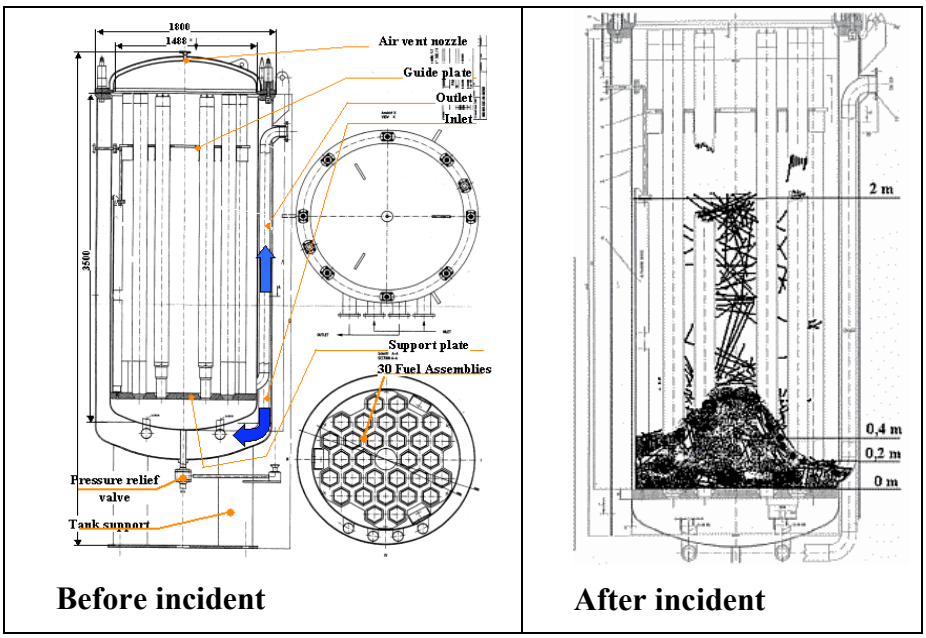
Loss of simplicity and passive safety features

The first most important requirement was to increase the number of fuel assemblies that could be cleaned simultaneously. This resulted in the design of a big vessel, housing 30 assemblies (about 3,550 kg of partially used fuel) and the cleaning technology for it. Measurements of differential pressure of each fuel assembly appeared to be not possible and no measurement of temperatures or other parameters within the tank were provided. Thus there were no means to monitor cooling of each individual fuel assembly. The second requirement was to clean the assemblies during annual maintenance, in a very short time period after the reactor shutdown. Both of these requirements resulted in a big increase of the heat generated in a relatively small closed space. Thus, the simplicity and passive safety features of the initial cleaning facility were lost.

Safety deficiencies in the design of the new cleaning system

- Location of a pressure relief valve at the bottom instead at the top of the tank, which led to malfunctioning of the cooling function;
- Inadequate sizing of the submersible pump, whose redundancy and back-up system was also inadequate. The low-capacity pump had to operate for several hours after completion of the cleaning which was clearly beyond its design specifications;
- The tank design did not assure precise positioning of the bottom end of the fuel assemblies in the cleaning tank;
- Only one fuel guide plate in the cleaning tank was utilized, which cannot assure proper alignment of the fuel assemblies. The possible bypass flows around the fuel assemblies – thus not fulfilling its cooling function – were not fully taken into account;
- Instrumentation, trend recording and alarms provided to detect off normal conditions were inadequate**.**

Figure 9: Paks Fuel Cleaning Tank Before and After the Incident



Incomplete safety analysis

A number of significant aspects of this cleaning project were unique and unproven. It was to be the first time that a large number of assemblies with significant decay heat were being cleaned. However, the safety analysis performed for the fuel cleaning provided only a simple analysis of the cooling conditions of the fuel. Even that analysis identified that in the event of loss of cooling during cleaning, boiling in the tank could occur within only 9,2 minutes. The approach proposed by Framatome ANP to respond to a loss of cooling was to stop the cleaning operation and to open the cover of the tank in order to flood the fuel. However the emergency lifting of the lid was not analyzed and there were no practical exercises. There was no analysis provided for the effects on the fuel assembly cooling if it was not properly installed in the tank, or of blockage of a fuel channel during the cleaning process. The safety analysis submitted with the license application also did not address the possibility of serious fuel cladding failure and the radiological releases expected from a single fuel element failure or multiple fuel failure. The lack of this information during the event contributed to an initial misdiagnosis of the incident.[82]

Improper management of cleaning and lack of safety culture

Cleaning operations were not integrated within the organization of maintenance operations. The responsibility was turned to Framatome ANP with strong over-reliance on a prominent company. Paks nuclear power plant operators did not monitor the cleaning equipment or process indications. The cleaning procedures were not developed, reviewed and approved by operating personnel. The operational and safety parameters and limits for the cleaning operation were not defined. No emergency procedures were developed and activities of the personnel after the incident were not effective, improper and even leading to more negative consequences. There was an accumulation of defaults in the safety culture.

[82] See IAEA Expert Mission op.cit.

Nuclear Safety Authority approach

The Hungarian safety authority (HAEA) clearly underestimated the safety significance of the proposed unproven design for the new cleaning system and did not use a conservative approach in its safety assessments. HAEA considered only a modification of a component, rather than the installation of a new system. The engineering design did not address the single fault criteria for safety systems. In addition operational limits for cooling, and fuel failure were not developed. The fault conditions and indications related to inadequate cooling of the fuel were not properly addressed. Time pressure combined with confidence generated by previous successful operations, contributed to a very weak assessment of a new design and operation.

Development and causes of the incident

The Unit 2 of Paks nuclear power plant finished its 19th fuel cycle, the reactor was shutdown and the annual maintenance started at 28 March 2003. The fuel assemblies were fully unloaded and stored in the storage pool. It was planned to clean 60 "cold" fuel assemblies and 210 "hot" assemblies. On 10 April 2003 the cleaning program for the 4th charge of hot assemblies was accomplished by 16:40. The lid of the container was not lifted due to the engagement of the crane in other operations. The cooling of the fuel assemblies inside the cleaning container was accomplishing in Mode B with the use of submersible pump.

Early signs of developing incident

At 19:20 the pressurizer level had increased by approximately 70 mm in about 20 minutes. This level change was also detected in the water level measurement of the cooling pool. The only possible reason for this could be draining of the cleaning tank and drying of the hot assemblies that could lead to their damage. However, nobody paid attention to these important indications.

At 21:53 unexpectedly higher dose rate and noble gas release were detected in the chemical system and the dosimetry systems of the exhaust stack showed a sudden increase in released noble gas activity. The radiation monitors in the reactor hall indicated alarm level. The dose rate near the cleaning equipment increased drastically and the reactor hall area was evacuated.

The cleaning tank lid was unlocked at 02:15 PM on 11 April and immediately a staggering activity increase ($3{,}1 \times 10^7$ MBq/10 min noble gas release) was observed. At the same time, the water level in the storage pool lowered by approximately 70 mm.

At 04:20 the lifting cable broke, the lid removing operation was interrupted and the damaged cover remained in a partially lifted position.

At 07:45 release of iodine isotopes to the atmosphere accumulates to 142,6 GBq.

At 24:00 the daily noble gas release is 160 TBq.

The event was rated INES Level 2.

In the evening of 16th April 2003, after several attempts, the container lid was finally removed and video inspection showed that all 30 fuel assemblies inside the container had been severely damaged. The event was re-rated to INES Level 3.[83]

[83] See footnotes IAEA Expert Mission op.cit. and Bulletins and official statements of Paks NPP and press releases of Hungarian Atomic Energy Agency from May and April 2003

Radiation conditions, doses and releases to the environment

Radioactivity releases into the atmosphere. Radioactive isotopes with an activity of 410 TBq (noble gases), 360 GBq (iodine-131 equivalent), and 2,5 GBq (long-lived aerosols) were released into the atmosphere in the first two weeks. One half of the noble gases, predominantly Xe-133 and Kr-85m, and most (95 %) of the activity of the iodine, was released in the first day. A release of this nature would be expected to cause a temporary increase in the environmental gamma dose rate within a few km of the release point in the downwind direction of the wind. The nine monitoring stations measuring gamma-dose-rates and located within the 1,5 km vicinity of the Paks nuclear power plant have not shown any increase. In the first hours of the incident the environmental impacts of the noble gas plume were detected by the telemetric environmental monitoring station A1 located 2,000 m north of the stack (downwind direction) - increase up to 260 nSv/h.

The level of environmental effect can be illustrated by the comparison with previous years and with emissions from other European nuclear power plants.

Table 2: Radioactive emissions from Paks in comparison with French nuclear power plants

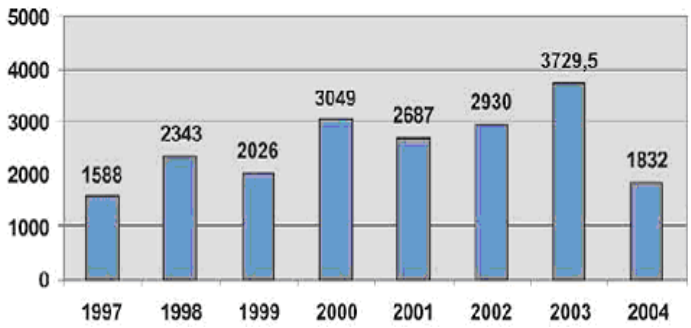
Emissions	Noble gases, [TBq]	I-131 + Aerosols, [GBq]
Paks average annual, 1999-2001	53	< 2
Paks 10.04 - 23.04.2003	410	363
Paks total 2003	517	412
Total emissions from 58 French reactors	109[84]	2

Sources: National Reports under the IAEA Convention on Nuclear Safety and Report of the IAEA Expert Mission to Paks NPP, 16-25.06.2003

The radioactive noble gas emissions following the Paks event correspond to roughly four times the cumulated annual emissions of all 58 French pressurized water reactors and 180 times of their cumulated radioactive iodine and aerosol releases.

Doses to the personnel and to the public. The Paks personnel collective dose for 2003 was the highest during last years and twice as high as in 2004, as shown in the following figure.

Figure 10: Collective dose in the vicinity of the Paks nuclear power plant (in man-mSv)[72]



[84] including noble gases and tritium gas

The calculation results show that the 2003 contributory dose from the airborne and liquid discharges to the group of population within 3 km distance from the plant site was 113 nSv for adults and 185 nSv for children. These doses were higher than the values calculated for the previous years due to the huge emissions from the incident to the environment.[85]

Restart of operation. Unit 2 was restarted in August 2004 and shut down on 8 December 2004 for refueling and major maintenance. In 2004 a new refueling procedure was specially developed to bypass the service pool and the unit was returned to service in March 2005. [86]

Clean-up operations. Due to their complexity clean-up operations started only about 3.5 years after the incident. On 29 January 2007 Paks nuclear power plant reported that the whole amount of damaged fuel was removed from the cleaning tank.[87]

The main lesson learned: Spent nuclear fuel represents a high risk potential not only when it is in the reactor core; providing sufficient cooling to spent fuel after unloading from the reactor core is a safety measure of highest priority, especially under conditions not envisaged in the original design; underestimation of these risks leads to incidents with very serious consequences. A number of findings and lessons learned are not new and most of them are typical for incidents in nuclear facilities.

9.2.4 Fires and Explosions

Fires and explosions are part of the most dangerous events in a nuclear power plant because they can affect several safety relevant systems at the same time. They can also lead to different level problems including physical destruction of parts, excessive heat, impenetrable smoke and missiles.

9.2.4.1 14 December 2001, Brunsbüttel (Germany)

During power operation in December 2001 in the German Brunsbüttel boiling water reactor several unusual signals lit up in the main control room. The signals were interpreted as a steam leakage in the area of the pressure vessel head spray line. The head spray line is used for cooling the inner surface of the reactor pressure vessel head and the flange area upon plant shutdown and only has operational functions.

The leakage and the increase of containment pressure were stopped by manually closing the drainage valve. The operator drew the conclusion that a small flange leakage had happened. The operator decided to bring the plant back to full power the same day.

Following this initial event, additional investigations were performed because records of temperature measurements indicated an accumulation of fluid and gas in different parts of the spray system. Theoretical analyses in view of possible radiolysis reactions were initiated. To clarify the remaining questions an on-site inspection of the containment was arranged. The operator decided to shut down the plant in February 2002, two months after the initial event. During the inspection a high degree of damage to the spray system piping was discovered. Some parts of the 5.6 mm diameter pipes were ruptured. An approximately 2.7 m long piping section had burst and was completely destroyed. Some sections of the piping were missing.

[85] See Radiation protection status in 2003, http://www.npp.hu/kornyezet/radprot_a_2003.htm
[86] See Nucleonics Week 3 February 2005
[87] See Information Report, Institute of Isotopes, Chemical Research Centre, Hungarian Academy of Sciences

A retrospective review revealed that the records of the temperature measurement had been conspicuous since restart of the plant in 2001. Indications of an excessive accumulation of hydrogen gas were identified. It was determined that a hydrogen explosion had taken place.

Prior to this event the possibility of severe explosions caused by radiolysis gas during normal operation was nearly excluded, although the principle of radiolysis gas reactions had been explored. Protective measures for this type of event were not developed the same way as for other phenomena.

The review of the event demonstrated the need for systematic investigation of potential radiolysis gas accumulation. It was realized that systems that were considered of primarily operational function without direct safety significance were not investigated with the same depth as identified primary safety systems. The Brunsbüttel event demonstrated that even on the primarily operational level there can be a considerable contribution to risk.

Experts recommended a graded proceeding to cope with the risk of radiolysis gas reactions. This covers complementary measures to avoid, to detect and to control the consequences of a radiolysis gas accumulation.

Fortunately the degree of damage in Brunsbüttel did not affect any safety devices or functions. This was not the consequence of an elaborated safety concept but due to fortunate circumstances. A higher degree of damage in case of an extended accumulation of hydrogen gas is easily imaginable.

The Brunsbüttel event is an example of a significant weakness in the safety concept. The design did not meet all probable event sequences. Well-known phenomena holding a high risk potential were insufficiently taken into account. This might be also a hint to potential vacancies and risks that are hidden in the nuclear power plant design and that have gone undetected or remained unexpected so far.

9.2.5 Station Blackout

A nuclear power plant generates electricity. But in order to do so safely, the permanent supply of electricity to the power plant is indispensable. Most of the safety devices like pumps, motors, lights, control-command functions etc. need power to operate. A station blackout, the total cut-off of all power supply is considered a high-risk operating condition for each nuclear facility. Therefore every nuclear power plant has several external and internal power sources.

9.2.5.1 18 March 2001 Maanshan (Taiwan)

In March 2001 the Taiwanese nuclear power plant in Maanshan, two 950 MW_e pressurized water reactors, was affected by a total loss of external and internal power supply. The plant is situated near the sea. Salt deposit on insulators due to foggy weather caused instability of the 345 kV high voltage grid.

On 17 March 2001 at 3h23 both units of the plant were shut down automatically and kept in hot standby. On 18 March 2001 at 0h41 the plant looses all four trains of 345 kV of offsite power. A breaker opens the connection to the 161 kV external supply. In the following minutes it is attempted to reconnect the 345 kV grid. Finally during a switch to the 345 kV grid a short circuit in a 4 kV power switch of one redundancy of the emergency power line occurred and caused a cable fire. The CO2 extinguishing system is actuated. The shift to the 161 kV grid was provided to run automatically but the power breaker was affected by the cable fire nearby, before the CO2 extinguishing system was actuated.

Two emergency diesels of unit 1 were unable to provide power to both essential buses. The plant enters alert condition. Heavy smoke is coming out of the control building below the control room. At 0h56 the firemen rush to the smoking part of the plant but lack adequate lighting and ventilation equipment. The operator manually connects the first emergency diesel generator to the essential bus but it provides power only for 40 seconds and then fails. At 1h06 the staff attempts to restore the second emergency diesel generator but the building is full of smoke and there is no sufficient lighting available. At 1h41 the operator calls the local fire department to request additional lighting and ventilation equipment to assist expelling the smoke.

At 2h19 the operator gives an emergency call to the Atomic Energy Council (AEC), which sets up an emergency control centre and calls 17 AEC staff from their homes. Finally at 2h54 the so-called swing emergency diesel generator, which can provide power to either one of the units, is successfully connected to unit 1. The plant is connected to an external power supply (161 kV) only at 22h12 and the diesel is disconnected.

It turned out that the operator should have declared the event much earlier, as soon as the station blackout situation occurred. The breaker fault at the 4 kV essential bus is considered as the main cause of the event. The breaker and the switchgear got totally destroyed by the fire (see figure 11).

The Atomic Energy Council stated later in an enquiry report: *"This incident was viewed as the most notable event over the 22-year history of nuclear electricity generation in Taiwan."*[88]

[88] Atomic Energy Council, *The Station Blackout Incident of the Maanshan NPP unit 1,* Taiwan, 18 April 2001

Figure 11: Breaker Damage at Maanshan During Station Blackout

Normal Breaker

Damaged Breaker

Normal breaker arrangement at a switchgear

Damaged breaker arrangement at a switchgear

9.2.5.2 25 July 2006, Forsmark, Sweden

In 2006 a short circuit in an outdoor switching station of the grid nearby the Swedish Forsmark nuclear power plant caused the emergency shutdown (scram) of unit 1 and, in a complex scenario, led to a number of subsequent failures at the plant. Due to a design error, the disconnection of the plant from the grid and the switch to house load operation – the power plant uses its own power to operate essential auxiliaries – did not function as planned.

In the following course of events an inappropriate converter adjustment led to the failure of the attempt to connect safety related equipment to the emergency power supply. The start up of two of the four emergency diesel generators was aborted, which lead to a partial blackout even in the main control room. The failures in the electrical power supply system were followed by various malfunctions. Due to the lacking indication of important parameters for a period of time the exact state of the plant and the consequences of potential actions to perform were unclear. The shift team decided nevertheless to try to reconnect the plant to the grid, which was performed successfully.

The Forsmark incident revealed a weakness in the plant's safety concept. As a root cause for the unexpected extent of the event, the insufficient separation of safety levels has been identified. A disturbance originating in the external grid was not blocked at the grid connection level. The disturbance could pass several safety barriers and affected safety related equipment of different redundancies. The equipment was not designed for such electrical transients. The potential of external disturbances as a root cause for serious events was obviously underestimated in the design.

An elementary conclusion of the incident was, that an important principle of the safety concept, that no single individual malfunction can affect several different safety systems, was not maintained.

The Forsmark incident provoked subsequent investigations by Swedish and foreign authorities (e.g. Germany, Switzerland) to verify the transferability of the event sequence. The most important contributing factors were identified as follows:

- The electrical selectivity of protective adjustments was insufficient.
- The start up of the emergency power diesel generators was not independent of the orderly functioning of the AC/DC-converter.
- The communication between the operator of the plant and the operator of the grid was poor. Sufficient measures to avoid unacceptable consequences caused by potential disturbances coming up from work in the external grid were not agreed.
- Weakness in the shift management of the plant facilitated that a failure remained undetected and led to delayed disconnection from the grid.

These findings were seen as indications of weakness of the plant's safety management in general. Accordingly subsequent to the review of the technical dimension of the incident further safety related issues were brought into discussion.

A possible contributing factor was a weakness in the interpretation of the safety significance of staff activities during normal operation. The protective means might have been adjusted in a way that turned out inadequate for their required safety performance. The AC/DC-converter was adjusted with priority to the optimization of battery loading but contrary to a required safety function. The adverse adjustment caused that in consequence of the electrical transient the current flow was disrupted in both flow directions. The separation from the AC-Voltage grid was a necessary protective measure to block the electrical transient. But inappropriately the current flow of DC-voltage from the batteries supplying safety related equipment was disrupted simultaneously. This led to the loss of emergency diesel generators.

In retrospect the management of Forsmark concluded that in view of the progress of the company's safety culture a gradual deterioration over the last few years had taken place. A systematic investigation aimed on internal structures and conditions was started.

Overall it seems only due to fortunate circumstances, that the adverse combination of technical and organizational failures could be brought under control.

9.2.6 Generic Issues – Reactor Sump Plugging

In many occasions a technical issue is discovered through an incident in an individual nuclear power plant that turns out to be valid for several plants, sometimes for dozens or even more units. Occasionally these discoveries are made by pure coincidence, in particular during maintenance work.

One of the issues that turned out to be generic on an international scale is the problem of the potential plugging of the filter system of the reactor sump. In the case of a loss of coolant accident, the leaked water is caught under the reactor vessel in order to be pumped back into the system. The loss of the recirculation function would be a severe handicap in many accident scenarios. The phenomenon was first discovered in a Swedish nuclear power plant and later in many other reactors around the world.

9.2.6.1 28 July 1992, Barseback-2 (Sweden)

In July 1992 a leaking pilot valve in the Swedish boiling water reactor in Barseback caused a safety valve for the reactor vessel to open. Safety functions like reactor scram, high-pressure safety injection, core spray and containment spray systems were initiated automatically in response to the event. The steam jet from the open safety valve was impinging on thermally insulated equipment. The amount of dislodged insulating material exceeded the estimated amount significantly. Insulating material was washed into the suppression pool and affected the emergency core cooling system. The strainers on the suction side of the sump pumps became partially plugged with mineral wool. This caused a decreasing pressure across the strainers and indications of cavitation in one pump. Increasing consequences were avoided because a back flushing of the strainers was carried out successfully.

The emergency core cooling system is essential for the heat removal. In case of a leak the reactor coolant is collected and has to be circulated through the sump of the building. An improper pressure drop in the suction line of a pump as indicated in Barseback may cause cavitation followed by the damage of the pump. If the back flushing is unsuccessful the heat removal might become disabled and the risk of overheating of the core is increased.

A small pipe leak or an inappropriately opened valve is supposed to be considered as design basis accident. The Barseback incident illustrated that design conditions to control this type of accident were incorrectly assessed and the issue turned out to be a generic fault.

The simplified model was based on a leak occurring in a naked steal pipe as imaged in technical drawings. The actual situation on-site was disregarded. It was characterized among other things by insulation material surrounding the leaking pipe and exposed to the leak stream. The dimension and the impact of material dislodging were underestimated. The following course of adverse effects seems to be predictable but insufficiently considered. The phenomena that became obvious in Barseback are transferable to other reactors in Sweden and elsewhere.

In 1993, at Perry Unit 1 (USA), the emergency core cooling system (ECCS) strainers twice became plugged with debris. On 16 January 1993, ECCS strainers were plugged with suppression pool particulate matter, and on 14 April 1993, an ECCS strainer was plugged with glass fiber from ventilation filters that had fallen into the suppression pool. On both occasions, the affected ECCS strainers were deformed by excessive differential pressure created by the debris plugging.

On 11 September 1995, at Limerick Unit 1 (USA), following a manual scram caused by a stuck-open safety pressure relief valve, operators observed fluctuating flow and pump motor current on one of the cooling systems. The operator later attributed these indications to a thin mat of fiber and sludge that had accumulated on the suction strainer.[89]

By the end of 2003, it had become clear that all 34 French 900 MW reactors were facing the same problem.

This is an example of generic weakness of safety analysis, which may concern a large number of facilities. The phenomena of sump clogging have been investigated in many countries operating nuclear power plants.

---

[89] NRC, *Safety Evaluation by the Office of Nuclear Reactor Regulation Related to NRC Generic Letter 2004-02, Nuclear Energy Institute Guidance Report (Proposed Document Number NEI 04-07), "Pressurized Water Reactor Sump Performance Evaluation Methodology",* December 2004

More than ten years after the Barseback incident the sump clogging issue became urgent again in the German Biblis nuclear power plant. Randomly it was discovered that the suction strainers of the sump pumps in the emergency core cooling system were not dimensioned in accordance with the approved specification. Significant changes were implemented during the construction phase. The documentation was never updated. For years, the surface and the configuration of the sump strainers did not reach the specified state. The basic design of the sump strainers and the compliance with the specification were not verified since the commissioning of the plant. Even the Barseback incident did not trigger a general and systematic review. During the whole period of operation a leak in the primary cooling circuit might have caused an extent of sump clogging that would have led to a loss of the core cooling system, essential to control this type of accident.

Subsequently experts started discussing variables influencing sump clogging: e.g. specific behavior of different insulation materials, retention at structures, transport effects, debris on the sump strainers, deposition of insulation material inside the core and overall the evaluation of influences on the function of pumps and the efficiency of core cooling. The complex interrelations are not yet entirely clarified. Uncertainties in view of the capability of nuclear power plants to control sump clogging in case loss of coolant accidents remain and indicate a latent weakness in the design of vital safety systems.

9.2.7 Natural Events

There are various types of natural events that can impact on the safe operation of a nuclear facility, in particular earthquakes, wild fires, storms and lightning. Floods can originate in heavy rainfalls, dam breaks, storms and tsunami type phenomena or a combination of these phenomena. On the other side, droughts can lead to low water levels in rivers needed for cooling and extended heat periods can overheat containments beyond design specifications. The changing weather patterns that accompany global climate change are now established to trigger an increasing frequency of extreme weather events that might more frequently exceed design basis specifications of nuclear facilities around the world.

9.2.7.1 27 December 1999, Blayais-2 (France)

The unusual storms at the end of 1999 led to the flooding of the Blayais nuclear power plant site. Certain key safety equipments of the plant were flooded, for example the safety injection pumps and the containment spray system of units 1 and 2. The electrical system was also affected. For the first time, the national level of the internal emergency plan (PUI) was triggered. The IAEA's Operational Safety Review Team (OSART) report on Blayais notes "The plant's communication department has had a hard task after the 1999's flood to recover the lost credibility, but now the situation is considered to be good again."[90]

At the end of 1999 heavy weather caused high degree of damage to the French electricity grid. Many high-voltage towers broke down and the Blayais site suffered the loss of the grid. Units 1, 2 and 4 were operating. Unit 3 was down for refueling. First, at 18h00, the auxiliary 225 kV power supply for the four reactors at the site is lost after a tree fell on the lines. A second line is automatically linked up and the three reactors keep operating but an hour and a half later the second line is also lost. At the same time flooding of roads makes access to the site very dangerous. On the site itself, flying objects and debris render any intervention dangerous. A cleaning staff person is caught by the storm and breaks a leg. The operator and security relay is delayed. At 20h50 the units 2 and 4 scram (shut down automatically) in order to auto-protect

[90] IAEA, *Report of the Operational Safety Review Team (OSART) Mission to the Blayais Nuclear Power Plant*, 2 - 18 May 2005, IAEA-NSNI/OSART/05/131

against excessive tension on the 400 kV power evacuation line that they supply. The switch to house load operation – the power plant uses its own power to operate essential auxiliaries – as planned after the disconnection from the grid, failed. Following the loss of the auxiliary lines, the emergency diesel generators start up in order to provide on-site power. Forty minutes later unit 4 is brought back on the auxiliary 225 kV supply and the diesels are stopped, but the grid connection fails in the case of unit 2 that remains on diesel supply until 23h20.

Water is pushed over the protective dyke. The water invades the site through underground service tunnels. At around 22h00 water penetrates the fuel building of units 1 and 2. Around midnight at unit 2 the flooding of the safety injection and containment spray system pumps – essential in the case of a loss of coolant accident to supply coolant and decrease pressure and radioactivity levels in the reactor building – is identified as well as the non-availability of a number of associated valves. At 00h30 unit 1 scrams probably due to debris that was sucked into a service water system. No unit on site produces power at this point. External staff on standby is called into the plant one by one. At 2h00 the flooding of the safety injection and containment spray system pumps of unit 2 is identified. At 2h50 the internal emergency plan (PUI level 1, local) is activated and the relay staff takes up its shift. Shortly after EDF's national crisis teams are activated. At 7h00, at unit 1, the flooding of two of the four pumps of the auxiliary cooling system is identified. At 9h00 the national nuclear safety authority requests the activation of the national level of the internal emergency plan (PUI level 2) as precautionary measure in the case of the loss of the two remaining pumps of the auxiliary system (which did not occur). PUI level 2 implies the automatic information of 150 EDF staff, the Nuclear Safety Authorities, the Institute for Radiation Protection and Nuclear Safety (IRSN)[91] and the Directorate of Defense and Civil Security (DDSC).

Later it was revealed that rooms containing electrical feeders led to the loss of certain electrical switchboards.

Numerous pumps were operated for almost 44 hours to evacuate over 100,000 m3 of water that had flooded the various buildings.

Basic flood protection criteria were violated at Blayais. Safety related equipment was placed at a level at least as low as the maximum water level. The invading of external water was not blocked due to unsuitable protection measures at the lower platforms, e.g. fire doors. The water could penetrate and reach reactor safety equipment. The design assumptions concerning flooding events were insufficient. The adverse coincidence of strong winds and rising tide as happened was disregarded. Furthermore the planning to raise of the protective dyke at the site as recommended in a safety analysis report had been delayed.

Up to the occurrence of this event the design was considered safe. The consequences of partial flooding of the site and appropriate counter-measures were not analyzed. More serious consequences were been avoided only because of a number of lucky circumstances: The emergency power supply by diesel generators functioned without disturbance for several hours until the site was successfully reconnected to the grid. And an accident, which would have led to the need to operate the safety systems lost by flooding, did not take place during this period.

The event had a significant aftermath. The safety authorities carried out 20 inspections in four months at the site. Unit 2 was down for over four months. Numerous upgrading actions had to be implemented. Investigations about the flooding risk were requested by the nuclear safety authority not only at all the other 18 nuclear power plant sites, but also at five other major nuclear sites including Pierrelatte and Marcoule.

[91] At the time of the event, there were still two separate entities, the Institute of Nuclear Protection and Safety. (IPSN) and the Office for the Protection against Ionizing Radiation (OPRI) that have merged after to form the IRSN.

9.2.8 Security Events and Malicious Acts

The possibilities for malicious acts in a nuclear facility are only limited by imagination. Reality has already demonstrated an impressive number of criminal activities in and around nuclear plants. Systematic falsification of technical documentation and manipulation of equipment test conditions, theft of equipment, radioactive and nuclear materials, threats and armed attacks. It is obvious that the potential threat dimension has significantly changed after the 11 September 2001 events. Especially the recent systematic deployment of suicide bombers of international sub-national organizations makes the protection of a nuclear facility and its radioactive inventory highly vulnerable.

9.2.8.1 7 February 1993, Three Mile Island (USA)

On Sunday, 7 February 1993, at approximately 06:53, an unauthorized vehicle traveling at around 60 km/hr entered the owner-controlled area (OCA) of the Three Mile Island nuclear power plant through the outbound lane of a two-lane access road. Although a guard booth was present at the entrance to the OCA, no physical barriers were present to delay access. The vehicle continued onward to the protected area (PA) of the nuclear plant and collided with one of the entry gates, which failed, allowing the vehicle to pass through. It then crashed through a corrugated metal door and entered the turbine building of the Unit 1 reactor, which was operating at full power. The vehicle stopped 19.2 meters inside the turbine building, striking and damaging a resin liner and the insulation on an auxiliary steam line. When the vehicle was approached by security officers at 07:02, the driver was nowhere to be found.

After some initial confusion as to the exact nature of the event (one technician reported that the turbine building door had been blown down by “wind”), the shift supervisor declared a Site Area Emergency at 07:05, the second highest emergency classification level. This was the second time this had occurred at the TMI plant (the first being the TMI Unit 2 meltdown in 1979).

The response to the event by the TMI operator, GPU Nuclear Corporation, was marred by glitches that revealed wider problems with the security and emergency operations at TMI. In particular, a sequence of bad decisions resulted in a delay of more than forty-five minutes in notifying the utility’s off-site emergency personnel of the incident, although the requirement is that all off-site notifications be completed within fifteen minutes of an emergency declaration. The plant had a phone-based pager system, located outside of the control room in the shift supervisor’s office that could automatically notify State and local officials and the utility’s Initial Response Emergency Organization (off-site emergency personnel) in the event of an emergency. However, the shift supervisor and other responsible personnel were unable to access the pager system. This is because the shift supervisor on duty in the control room had ordered the control room fire doors locked as a security precaution upon learning of the intrusion.

As a result, the shift supervisor ordered one of the control room personnel to manually make all notifications from a telephone in the control room. However, the telephone numbers for the offsite emergency personnel were not available in the control room, but were in the shift supervisor’s office. So the control room doors had to be unlocked so that the numbers could be retrieved. But instead of using the pager system in the shift supervisor’s office, the list of phone numbers was brought back into the control room, resulting in further delays. If the intrusion had been a radiological sabotage attack on the plant, precious minutes would have been lost in executing the emergency response plan, putting plant employees and the public at risk.

These problems should have come as no surprise to TMI management. In fact, numerous deficiencies in off-site notification procedures at TMI had been observed during emergency planning drills only months before the incident. The TMI operator had apparently not corrected those deficiencies.

The intruder was not apprehended until 10:57, four hours after he entered the site, when he was discovered hiding in a small space under the condenser pit in the turbine building. The condenser pit was first searched hours earlier, but the search was halted because lighting was insufficient. (The second search team came with a brighter flashlight.) The unarmed intruder was a mentally ill man who had recently been discharged from a psychiatric hospital and who apparently said before the event that he was "going to do something to become famous."

The NRC sent an Incident Investigation Team to investigate the event and concluded that "the event resulted in no actual adverse reactor safety consequences and was of minimal safety significance." But if the intruder had had malicious intent, the outcome could have been significantly worse. While detonation of a car bomb in the turbine building would not necessarily have led to core damage by itself, if coordinated with an attack on another system like the transmission lines leading into the plant, the attack could have been devastating. It is also possible at some nuclear plants that destruction of a single "target" could result in significant core damage. Therefore, at such plants, the potential exists for a single knowledgeable adversary equipped with explosives to cause a core melt unless access to the vulnerable target is denied to the intruder.

In any case, the event did reveal significant deficiencies in the utility's security and emergency response programs, as well as in the NRC's regulations. At the time, the NRC did not require that nuclear plants be protected against forced vehicle intrusions. Partly as a result of this incident, the NRC amended its regulations to require the deployment of vehicle barrier systems. The goal of these requirements was to provide protection against a vehicle bomb as well as against forced vehicle intrusions. However, the current requirements do not provide protection against multiple vehicle bombs (in which the first bomb is used to breach a vehicle barrier, enabling a second vehicle to enter the protected area), even though such tactics are being increasingly used by paramilitary groups around the world.[92]

9.2.8.2 July 2000, Farley (USA)

Between 1991 and 2001, the NRC conducted a program known as the "Operational Safeguards Response Evaluation," or OSRE. This program consisted of performance exercises designed to evaluate whether nuclear power plant security forces could effectively defend against an adversary team with a defined set of characteristics: number, weaponry, equipment and tactics. (This set of characteristics is known as the "design basis threat," or DBT. Although the details of the DBT are classified as "safeguards information" by the NRC, it is well-known that no more than three external attackers were used in these exercises.) In these war-game-type exercises, a mock adversary force would carry out a series of four attack scenarios, with the objective of simulating the destruction of enough plant equipment to cause a core meltdown (known as a target set). The NRC would then evaluate the performance of the nuclear plant security force in preventing the adversary team from achieving its goal.

During the July 2000 OSRE at the Farley Nuclear Plant in Columbia, Alabama, the security force at Farley could not prevent the mock adversary team from simulating the

[92] Iraqi insurgents, for example, use the two truck tactics. Two suicide truck bombs were used against the Abi Tamaam Police Station in eastern Mosul on 19 October 2006. "The first truck bomb exploded near the station's entry control point, blowing down protective walls and creating a sizeable crater in the road. The second truck, unable to penetrate the police station's perimeter due to the crater and debris left over from the first truck bomb, detonated in the street." (see www.defenselink.mil/news/NewsArticle.aspx?ID=1766) While the action failed, it is obvious that the objective was that the first truck bomb clears the way for the second one.

destruction of entire target sets in two out of four exercises (and therefore simulating a meltdown); and simulating the destruction of "significant plant equipment" in a third exercise.

Part of the reason for this poor performance was the "failure to adequately perform multiple portions of the response strategy." According to an NRC inspection report of the exercise, adversaries were not detected in time to allow security officers to defend pieces of vital safety equipment; responders could not leave defensive positions without making themselves vulnerable to the adversary; and some security officers were outside of the protected area and took too long to respond after the attack.

The OSRE failures at Farley were so severe that the NRC initially proposed to issue a "yellow" finding, the second-worst category, indicating the poor results had "substantial safety significance" and resulted from a "broad programmatic problem." However, the plant operator, the Southern Nuclear Operating Company, contested the finding, arguing that the test was unfair because the mock adversary team used certain equipment and tactics that were "beyond the designed or required capability" of its protective strategy. It also argued that the exercises did not accurately simulate real conditions and therefore should not be considered representative of real attacks. Finally, it argued that even if the attacks had been real, plant operators would have been able to arrest any core damage before any radioactivity was released.

At the time, the OSRE program was subject to an aggressive challenge by the nuclear industry, which was being repeatedly embarrassed by the widespread security failures that the exercises revealed, and being required to make expensive upgrades to their security programs to correct them. In particular, the industry argued that the OSREs were unfair because the adversary team did not utilize the same capabilities at each site.

The NRC ultimately relented under pressure and concluded that only one of the two exercises in which a target set was destroyed represented a conclusive failure of the protective strategy. It then reduced the significance of the OSRE failure to "white," meaning that it did not represent a "broad, programmatic problem." But the reason for this was not because the exercise found the Farley response strategy was effective, but because the adversaries used tactics, which the Farley security force were not expecting. Of course, if this exercise had been a real attack, it isn't likely that the attackers would voluntarily refrain from using certain weapons or tactics because it would be unfair to the Farley security force.

9.2.8.3 29 August 2002, 17 TEPCO Reactors (Japan)

The Tokyo Electric Power Company (TEPCO) is the largest electricity utility in Japan and one of the largest in the world. It operates 17 boiling water reactors – as many units as operate in the whole of Germany – with a total installed capacity of 17,300 MW. TEPCO was also one of the most respected large companies in Japan.

On 29 August 2002 the Japanese Nuclear Industrial Safety Agency (NISA), shocked the nation with the public revelation of a massive data falsification scandal at TEPCO. At that point 29 cases of "malpractice" had been identified, including the falsification of the operator's self-imposed inspection records at its nuclear power plants over many years (see Annex 4 for a chronology of events). In the follow-up, all of the 17 TEPCO units had to be shut down for inspection and repair. The case is unique in the world, not only because of the extent of malpractice but also in its effect on the national power system of a country (see figure 12). It was

also reported later that these practices had gone on for as long as 25 years and the total number of events is put at nearly 200.[93]

The 29 original cases of malpractice identified include the following:

• Five cases involved the entry of false dates as the dates of discovery of specific problems. When the safety authorities requested countermeasures and instructed the examination of the parts concerned, the operator did not report to the agency the problem, which it had already identified.
• Five cases involved inadequate record keeping and falsification. In one case, the licensee failed to keep a record of aging degradation incidents, such as cracks or indications of cracks found in the core shroud by an outside contractor. In another case, the licensee did not conduct follow-up inspections of the results of analysis that an outside contractor had carried out regarding causes of detected flaws. In other cases, although faults such as cracks were identified or repaired, the operator "ordered an outside contractor to delete the record of initiation or repair of the faults in order to cover up the problem, and the licensee falsified the date of discovery of the incident".[94]

The problem was not limited to TEPCO nuclear power plants. On 20 September 2002 additional cases of malpractice were revealed. Two other nuclear operators, Chubu Electric Power Company and Tohoku Electric Power Company, had failed to report to the safety authority that cracks had been identified in the recirculation system pipes of their reactors – a crucial part of the emergency core cooling system in case of a loss of coolant accident (see also 9.2.6.1).

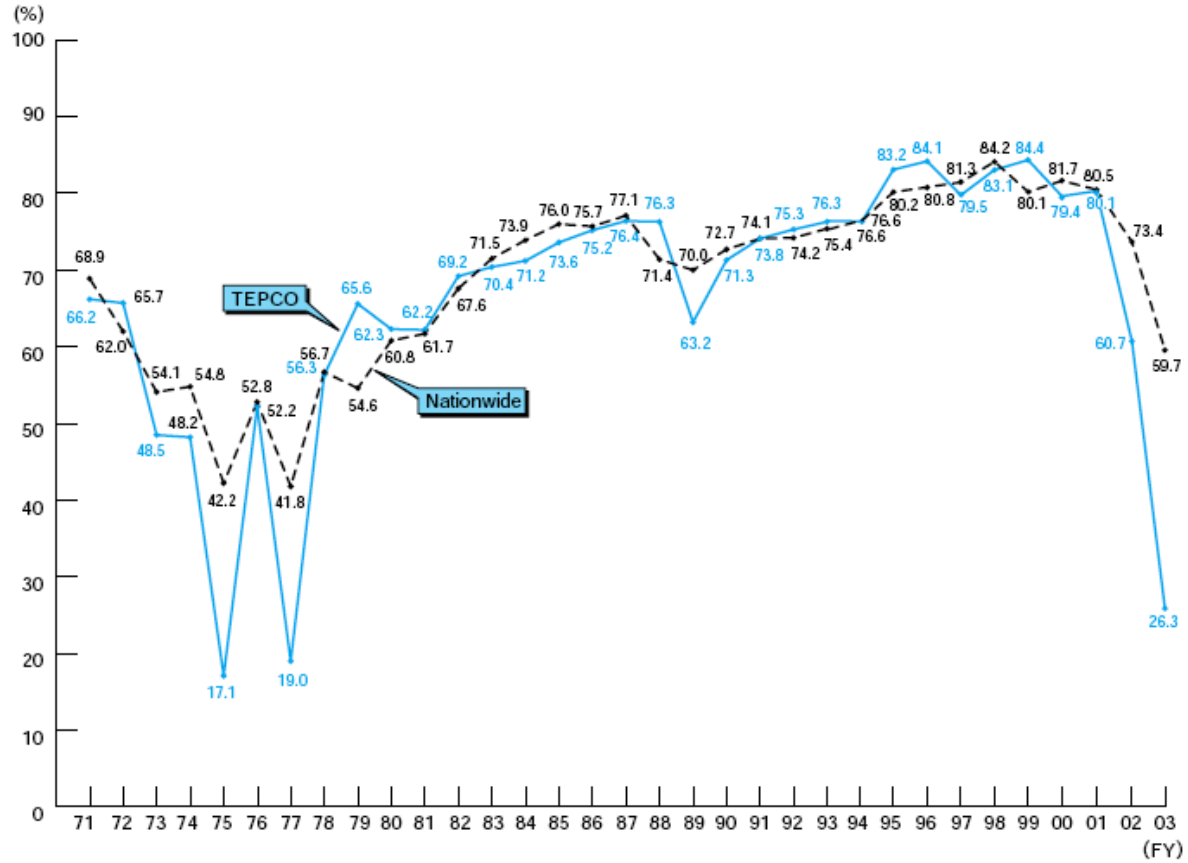
In its interim report, dated 1 October 2002, the official nuclear safety agency NISA concluded:

> *"As nuclear safety regulatory authorities, NISA regards the recent cases as a very serious problem, not only with safety arrangements at licensees who have performed inappropriate acts but also with Japan's nuclear safety regulatory administration itself. The cover-up cases have made us painfully aware that we must frankly reflect on what we have done, take the plunge and mend our ways. As nuclear safety regulatory authorities, we must seriously recognize that the relevant cases caused tremendous anxiety among local residents living near nuclear facilities, and destroyed public trust in nuclear safety regulations."*[95]

On 12 December 2002 the *Association to Accuse TEPCO of Its Nuclear-Damage Cover-Ups* filed a complaint to the district public prosecutor's offices in Niigata, Fukushima and Tokyo to pursue TEPCO for its responsibility in a series of falsification cases. The complainant consists of 982 citizens of Niigata Prefecture, 509 of Fukushima Prefecture, and 1,689 from all over the country, amounting to a total of 3,180 people.[96]

Figure 12: Load Factor Crash in Japan as Consequence of Data Falsification Scandal

[93] "TEPCO said that it discovered falsifications of technical data on nearly 200 occasions from 1977 to 2002 at three nuclear power plants, and reported them to the Ministry of Economy, Trade and Industry as requested." see
[94] NISA, *Interim Report on the Falsified Self-imposed Inspection Records at Nuclear Power Stations*, 1 October 2002
[95] ibidem
[96] http://cnic.jp/english/newsletter/nit93/nit93articles/nw93.html



Source: TEPCO

Other cases of data falsification have been reported in Japan. In one of the latest ones, revealed on 15 November 2006, a computer program used by a Chugoku Electric thermal power plant had been altered to reduce the temperature difference shown between intake and outflow water. While there is no immediate safety significance to the event – intake outflow difference in temperature is limited for environmental protection reasons – the incident gives an idea of the criminal energy that is present amongst some of the plant operators and management. Subsequent checks of all nuclear and thermal power plants revealed similar alterations at seven nuclear reactors at various plants of different operators.[97] "At some the outflow temperature was lowered, while at others the intake temperature was raised, indicating that the data was falsified independently at each plant and that data falsification was routine practice."[98]

On 5 March 2007, *World Nuclear News* reported:

> *"Tokyo Electric Power Company admitted six further occasions when workers failed to record safety issues at nuclear plants to the Nuclear Industrial Safety Agency on 1 March, in addition to three already known. One of the new events concerns the breakdown during trial of a diesel back-up generator at Kashiwazaki-Kariwa 3 that went unrecorded in 1995. An emergency shutdown of one of the Kashiwazaki-Kariwa units in 1992 was also unrecorded. Another concerned the exceeding of thermal output by 0.1% at Fukushima 1 on five occasions between 1991 and 1998 for which workers entered figures below actual*

[97] Kashiwazaki-Kariwa (Tokyo Electric), Fukushima I (Tokyo Electric), Onagawa (Tohoku Electric), Tsuruga (Japan Atomic Power Company), Ohi (Kansai Electric)

[98] http://cnic.jp/english/newsletter/nit116/nit116articles/nw116.html#datafals

output. "We apologize from the bottom of our heart for causing anxiety to the public and local residents, " said Tepco vice President Katsutoshi Chikudate."

The scandal of the data falsification, cover-up and misleading of safety authorities does not seem to end. On 3 April 2007, the industry online news magazine Nuclear Engineering International reported under the headline "Japanese criticality revealed":

"Hokuriku Electric has admitted to a criticality incident almost eight years ago at its Shika 1 BWR.

The 18 June 1999 event was not reported until recently after regulators instructed utilities to examine their records and declare any previously undisclosed incidents. According to the utility, during the 15-minute localised criticality, temperatures increased slightly in the 540 MWe unit. However, no other consequences arose from the event.

Following the announcement by Hokuriku, the director general of Japan's Nuclear and Industrial Safety Agency (NISA) handed the president of Hokuriku a document ordering the company to submit a report as stipulated by law. NISA ordered the immediate halt of operations at Shika 1 so that a full safety inspection could be carried out. NISA also warned other power suppliers to take actions to prevent similar accidents.

According to Hokuriku, the incident occurred in the fifth periodic inspection of the BWR after three of the 89 control rods had moved out of position during preparations for a routine test. The reactor reached a state of criticality, setting off the automatic 'stop' signal. However, the control rods were not automatically inserted at that point as the isolation valves were closed for the test. Some 15 minutes later the operators reopened the valves, and the control rods were reinserted.

The Hokuriku incident has been followed by two similar, though unconfirmed, incidents in which two of 89 control rods at Tohoku Electric's Onagawa 1 reactor failed in 1988, and three of 185 control rods at Chubu Electric's Hamaoka 3 were found to be out of position during a 1991 inspection.

Both events were apparently caused by malfunctioning valves, which affected water pressure in the control rod drive systems."

10. Summary and Conclusions

Residual Risk

An Account of Events in Nuclear Power Plants Since the Chernobyl Accident in 1986

by Georgui Kastchiev*, Wolfgang Kromp*, Stephan Kurth[+], David Lochbaum[++], Ed Lyman[++], Michael Sailer[+], Mycle Schneider**,
*Institute of Risk Research, University of Vienna, Austria; [+]Öko-Institut, Darmstadt, Germany; [++]Union of Concerned Scientists, Washington, D.C., USA; **Mycle Schneider Consulting, Paris, France;

Coordinated by Mycle Schneider
Commissioned by Rebecca Harms, Member of the European Parliament
With the support of: Altner-Combecher Stiftung für Ökologie und Frieden and Hatzfeldt Stiftung

Fifty years ago, on 25 March 1957, the EURATOM Treaty was signed. Article 1 stipulates that *"it shall be the task of the Community to contribute to the raising of the standard of living in the Member States and to the development of relations with the other countries by creating the conditions necessary for the speedy establishment and growth of nuclear industries".* Half a year later, on 10 October 1957, the fire at a Windscale reactor in the United Kingdom released massive amounts of radioactivity with, as a direct consequence and for the first time in Europe, very large quantities of contaminated milk and vegetables having to be destroyed.

Nevertheless, the Windscale accident had surprisingly little effect on public opinion Europe wide. In the UK the then fledgling civil nuclear industry pressed on with its designs for the first nuclear power stations, Magnox, which like Windscale had no secondary containment whatsoever and the UK government maintained its military imperative of plutonium production, seemingly ignoring the risk of a second radioactive release with its continued operation of the second identical Windscale reactor.

By the mid 1960s nuclear power was firmly established in Europe and its expansion continued apace. However, in March 1979 with a total worldwide experience of more than 1,000 years reactor operation, the pressurized water reactor (PWR) at Three Mile Island (TMI) in the United States sustained a severe fuel core melt and the potential for a very significant release of radioactivity to the environment. Such was the impact of TMI and although the nuclear industry implemented substantial upgrading programs in reactors and reactor designs thereafter, no nuclear plant has been ordered in the United States since and over one hundred projects have been completely abandoned. In Europe the majority of nuclear power plants that had been ordered and/or were under construction at the time of TMI were continued with, in account of design modification delays and construction times, installed capacity continuing to rise until by the end of 1985 a total of 155 power reactors were installed and in operation in the European Union.

In fact by 1986 the European nuclear industry was generally quite buoyant because it had, after all, ridden out the TMI storm albeit having to implement some significant backfitted and expensive safety measures. But then Chernobyl occurred, the worst nuclear power plant accident to date, resulting in a massive and hitherto unimaginable radioactive release that spread contamination widely throughout Europe, with its food and agricultural bans preying on the collective conscious of the general public.

The inexplicable nature and very severity of Chernobyl necessitated significant re-examination of nuclear safety, public explanations were demanded from the industry and its regulators; it practically stopped construction of new nuclear power plants. In the 27 current Member States of the European Union a peak of 177 power reactors was reached within two years of the Chernobyl accident. Thereafter and although a number of pre-Chernobyl ordered reactors had been completed and commissioned, plant closures outweighed new commissionings and resulted in a steady decline of operational reactors in Europe down to the level of 145 units of today.

The lessons learned from TMI had not been sufficient to prevent the Chernobyl accident.

At first the worldwide nuclear industry response to the Chernobyl disaster was defensive: it arose because of defective Soviet technology, demoralized operatives, lack of secondary containment, and so on, so much so that Chernobyl was a peculiarly Soviet accident *'just waiting to happen'* and that *'it could never happen here'*. Away from public scrutiny, however, the nuclear regulatory authorities in the European Union and elsewhere have been implementing revised regulatory regimes. These have required the operators to incorporate numerous improvements in human factor and management procedural aspects of plant operation, enhanced training programs and, where practicable, backfitting modifications and revisions to existing plants.

Significantly, for new nuclear builds the regulatory philosophy has nudged the plant designers to increase the role of passive systems to hold or return the plant and its nuclear processes to a stable, safe state; the outcome of abnormal incidents is now more firmly related to the radiological consequence and individual risk of health detriment; incidents and projected radioactive releases have now to be quantified so that an effective off-site emergency response might be prepared in advance; and, perhaps, most of all, the nuclear industry had to be 'transparent' and demonstrate that for continuing operation of its nuclear plants the *'risks were acceptable and the consequences tolerable'*.

Today, 21 years since Chernobyl with 8,000 reactor-years experience accumulated worldwide this post-Chernobyl period has passed without major accident, large-scale contamination and severe radiological consequences – is this an achievement or just simply luck?

To answer this question we have scrutinized the safety records of nuclear power plants in selected countries since Chernobyl, noting that large numbers of abnormal events continue to occur. We endeavor to analyze in depth a selection of these events although there are significant obstacles to a systematic and comparative analysis, including:

- Comparing severe events affecting different types of nuclear power plants worldwide is difficult because, first, there are many terms and definitions describing what could be called a nuclear incident and, second, there is no objective, internationally agreed and recognized definition for particularly severe events, both internal and external, that bear the potential for severe radiological consequences.
- Systems evaluating such nuclear events and their potential are not harmonized and are varying markedly from country to country. The quantification or indices determined do not provide a comparable indication of either safety levels or safety achievement.
- Even in case of the International Atomic Energy Agency's INES (IAEA's International Nuclear Event Scale) the values attributed to the events are those reported by the operators of the affected plants or of the national regulatory authorities. There is no system of independent evaluation to make comparisons meaningful and, moreover, in some states the nuclear safety regulator may not be entirely free of political persuasion.

- The INES definitions also exclude a large number of events from technically appropriate rating only because they do not involve any immediate radiological effect. On the whole, there seems to be a tendency towards underestimating the importance of events. Although the IAEA developed the INES from the basis of the former French national event scale, it is the national nuclear authorities of the IAEA member states that determine the final index of the event potential, particularly in that the IAEA gives no direction on how 'cliff edge' situations are to be evaluated in the INES.
- No reporting system has been devised that can unambiguously classify the events and accidents rooted in a huge variety of possible causes. For example was the Davis-Besse reactor pressure vessel head hole (see 9.2.1.2 for details) a (i) materials defect, (ii) management failure which arose from an inadequate, plant-wide safety culture, (iii) a cascade of human errors linking inspection and surveillance, and/or a (iv) quality assurance program failure, or yet some other cause?
- In general a caution approach is adopted when the *possible* progression of a pulled-up (arrested) event is postulated. Analysis is tending to be based on those remaining downstream safety systems and countermeasures coming into play promptly and effectively, qui in contrast to the fact that a number of upstream safety systems had already failed, which is portraying an optimistic view of what could have resulted into a much more serious event.
- Whilst reactor shutdowns are generally publicly known, the events that cause them are not always publicized. The international nuclear event database maintained by the IAEA is confidential to its members[99], and some countries tend to keep details of nuclear event reporting as privileged information that is not subject to public disclosure. Furthermore, post 9/11 much more information relating to plant performance under abnormal operation situations is being held back.

The IAEA does not impose nor require that much discipline for signatory countries when evaluating and reporting incidents. In other words, since there are no clearly established internationally agreed benchmarks to describe, categorize and risk assess events from one country to another, it is not clear how useful statistics could be arrived at. Thus, any one country that reports a large number of events could be revealing a severe safety problem in that country or, on the other hand, it could also be the honest characterization of a specific reporting system with unusual openness in communicating events.

This opportunity for anomaly is revealed by comparing just three countries, France, Germany and the United States.

In recent years the French nuclear power plant operator, EDF, has reported annually between 600 and 800 *'significant incidents'* (increasing tendency) to the nuclear safety authorities. Of over 10,000 events that were reported between 1986 and 2006, most were considered below the INES scale or Level 0 while 1,615 incidents were rated INES Level 1 and 59 Level 2. One event has been given a Level 3 rating[100]. In comparison, since the implementation of INES in 1991 Germany reported over 2,200 events as Level 0 or below, while 72 events were rated Level 1 or higher. On its part, the US Nuclear Regulatory Commission, over the same time period, has only

[99] The International Atomic Energy Agency did not respond to repeated information requests by the coordinator of the present study.
[100] Gravelines-3 incident, dated 16 August 1989

reported 22 events to the IAEA and rated them on the INES scale, of which 6 below scale, 7 Level 0, 3 Level 1, 5 Level 2 and 1 Level 3.

This apparent disharmony arises because there are simply no common criteria established to compare frequency and severity of nuclear events from country to country. In this respect, any reliance upon the present collage of INES rated events statistics to establish an international safety evaluation would be grossly misleading.

The **first conclusion** of this study is that many nuclear safety related events occur year after year, all over the world, in all types of nuclear plants and in all reactor designs and that there are very serious events that go either entirely unnoticed by the broader public or remain significantly under-evaluated when it comes to their potential risk (see the 16 selected events hereafter).

A recent joint IAEA/NEA (Nuclear Energy Agency of the OECD) Report on "Nuclear Power Plant Operating Experiences" covering the years 2002-2005 concluded:

> *"Almost all of the [200] events reported during that period have already occurred earlier in one form or another. It shows that despite the existing exchange mechanisms in place at both national and international levels, corrective measures, which are generally well-known, may not reach all end-users, or are not always rigorously or timely applied."*

The widespread belief that nuclear safety will be actually enhanced because of a lessons-learned process turns out ill-conceived. It is an open question whether the actual discussions within the nuclear expert community can lead to an improvement of nuclear safety in the reality of nuclear power plant operation.

Abnormal events are triggered by a variety of reasons: some are directly a result of design errors, sometimes fundamental or sometimes apparently trivial; other events can be traced back to latent construction, manufacturing and materials faults and/or deficiencies that have remained hidden in the plant; and there are unforeseen and unprepared for external events that unexpectedly challenge the plants and their safety systems; and finally there is the human dimension, including simple slip ups, omissions and misunderstandings, or more complex and deeply rooted institutional errors and, of increasing concern following 9/11, the possibility of organized malicious acts against nuclear plants.

Some of these events and incidents that have occurred could have evolved into serious accidents, had the defects, malfunctions, etc. not been discovered in time (near-misses); other incidents might be taken as early warnings or as precursors of serious accidents; and there are the so-called recurring events whereby a pattern of failures is repeated time after time at different plants. Sometimes, there develops an element of self-congratulation by the nuclear industry when an incident is brought to a 'successful' close, so much so that this overrides the various serious concerns that the incident should not have been triggered in the first place.

Not that those who lead the worldwide nuclear industry are complacent over these issues. During a biennial general meeting of the World Association of Nuclear Operators (WANO)[101], Chairman Hajimu Maeda warned of a creeping lethargy that begins with "*loss of motivation to learn from others...overconfidence...(and) negligence in cultivating a safety culture due to severe pressure to reduce costs following the deregulation of the power market*." Those troubles, if

[101] WANO, General Meeting, Berlin, October 2003

ignored, "*are like a terrible disease that originates within the organization*" and can, if not detected, lead to "*a major accident*" that will "*destroy the whole organization".*

Nuclear plants are complex, hazardous facilities. It follows that this very complexity spawns a multifaceted array of potential failure mechanisms and routes, so many in fact that it is seemingly impossible to marshal these into any semblance of order.

The **second conclusion** is that no great reliance should be placed on the International Nuclear Event Scale (INES), either for determining the absolute severity of one abnormal event from another nor, indeed, for determining the absolute safety achievements of any one country. However, in one respect the INES can be quite revealing: as three countries operating much the same type of nuclear power plant, under much the same regulatory and management systems in place, should not produce such disparencies in their respective nuclear safety achievements, the summarized data above are solely an indicator of their openness and/or reporting practices within INES.

The **third conclusion** of this research is that because the INES reporting system serves very little purpose there is need for its overhaul and modification – if at all possible – to provide a comprehensive reporting system that identifies not just the severity and potential impact of abnormal incidents, which the present INES barely achieves, but which sets out unifying rules of post-accident analysis and categorization so that existing trends may be monitored and emerging cause of failure identified. Such a revised INES reporting system should include facility to analyze and categorize human actions, including terrorist acts.

A selection of significant events that might assist in the framework development of a new INES reporting and analyzing system is annexed to this summary. These events illustrate the major categories of cause of failure in plants over the past 20 years but, that said, given the complexity of engineered systems and the ingenuity of mankind there are other causes of accidents that have yet to be discovered.

The present report should be seen as a precursor investigation into what should be a longer-term extensive study into the identification, notification, systematic analysis and evaluation, risk assessment, classification and lessons-learned action implementation of safety relevant events in *all* nuclear facilities in *all* countries.

So long as nuclear plants and facilities continue to operate there will remain a residual risk. Precursive events cannot be eliminated, the possibility of a future severe accident cannot be entirely excluded and it is unwise to dismiss the possibility of any undesirable incident occurring on the grounds of its remote probability alone. Finally, it is folly indeed to assume that all initiating events might be reasonably foreseen – after all, who foresaw the nature and mode of operandi of the 9/11 attacks?

Sixteen Selected Significant Events in Nuclear Power Plants in Nine Countries *Since* the Chernobyl Accident in 1986

The Residual Risk Project Team has selected 16 events from nine countries that illustrate that nuclear reactor safety remains far from perfect. This is not a ranking of the most significant events but rather a selection of known significant events that also reflect the specific knowledge and experience of the members of the Residual Risk Project Team. The selected events are presented in more detail in chapter 9. They were classified into nine categories (for easy reference, the respective chapter numbers are indicated in brackets).

Advanced Material Degradation (before break) (see 9.2.1)

3 April 1991 Shearon Harris (USA) (see 9.2.1.1)

On 3 April 1991 workers at the Shearon Harris pressurized water reactor in New Hill, North Carolina discovered damaged piping and valves within the alternate minimum flow system provided for the pumps in the emergency core cooling system. The piping and valve damage was serious, had an accident occurred the water needed to cool the reactor core would have instead poured out onto the floor through the ends of broken components. The NRC calculated the severe core damage risk from this event to be 6×10^{-3} or 0.6% per reactor year. The event was not rated on the IAEA INES scale.

6 March 2002 Davis Besse (USA) (see 9.2.1.2)

On 6 March 2002, workers discovered a pineapple-sized hole in the carbon steel reactor vessel head at the Davis-Besse pressurized water reactor in Oak Harbor, Ohio. The boric acid of the primary coolant had completely eaten through the 6-inch (15 cm) thick carbon steel wall to expose the 5 mm thin stainless steel liner. A government study estimated that the hole would have widened to the point where the liner ruptured in another 2 to 11 months of operation. Because Davis-Besse ran 18 months between refueling outages, had the damage been missed during the 2002 outage, it seems likely that a loss of coolant accident would have occurred. The NRC calculated the severe core damage risk from this event to be 6×10^{-3} or 0.6% per reactor year and rated it INES level 3.

Significant Primary Coolant Leaks (see 9.2.2)

18 June 1988, Tihange-1 (Belgium) (see 9.2.2.1)

On 18 June 1988, while the pressurized water reactor was operating, a sudden leak occurred in a short, unisolable section of emergency core cooling system (ECCS) piping. The leak rate was in the order of 1,300 liters per hour. The source of leakage was a crack – 9 cm long on the inside surface of the pipe and 4.5 cm long on the outside surface – extending through the wall of the piping. The risk of a pipe rupture in the emergency core cooling system is considerable if the emergency safety injection system is activated as large quantities of cooling water are injected in case of a loss of coolant accident in an already degraded safety situation.

12 May 1998, Civaux-1 (France) (see 9.2.2.2)

The Civaux-1 pressurized water reactor was shut down for five days, when, during start-up tests, a 25 cm diameter pipe of the main residual heat removal system cracked open and a large leak (30,000 liters per hour) occurred in the primary cooling circuit. The reactor core needs to be cooled permanently, even when it is shut down, in order to evacuate the significant amount of residual heat of the fuel. It took nine hours to isolate the leak and reach a stable situation. An

18 cm long crack on a weld was identified and 300 m3 of primary coolant had leaked into the reactor building. The unit had been operating for only six months at 50% power level maximum prior to the event. The operator, EDF, suggested rating this event at level 1 on the INES scale, but the safety authorities decided on level 2.

9 February 1991 Mihama-2 (Japan) (see 9.2.2.3)

A steam generator tube rupture occurred at Mihama-2 pressurized water reactor. This was the first such incident in Japan where the emergency core cooling system was actuated. The utility investigated the rupture and found that it was a complete circumferential tube failure. The utility found that the failure due to high cycle fatigue caused by vibration. By design, all tubes in specific locations in the steam generator are supposed to be supported by anti-vibration bars. However, the subject tube was found not to be supported appropriately because of a reported "incorrect insertion" of the adjacent anti-vibration bars.

Reactivity Risks (see 9.2.3)

12 August 2001, Philippsburg (Germany) (see 9.2.3.1)

A deviation from the specified boron concentration – a neutron absorber needed to slow down or stop the nuclear reaction – in several flooding storage tanks during the restart of the plant was reported to the authorities. In addition, the liquid level had not reached the required value fixed in the operational instructions for the start-up and was only implemented with a delay. The emergency core cooling system will only work effectively if it is operated according to the design basis conditions. Subsequent investigations revealed that significant deviations from start-up requirements and violations from related instructions seemed to be common probably for several years and took place in other German nuclear plants.

1 March 2005 Kozloduy-5 (Bulgaria) (see 9.2.3.2)

In the process of power reduction at the Russian designed pressurized water reactor (WWER) the operators identified that three control rod assemblies remained in the upper end position. The follow-up movement tests of the remaining control rod assemblies identified that 22 out of 61 could not be moved with the driving mechanisms. The exact number of control rod assemblies unable to scram (to drop due to the gravity only) remains unknown but it is thought to be between 22 and 55. The WWER-1000 scram system is designed to put the reactor in safe shutdown if one control rod assembly at the most is jammed in the upper position. The operator had originally rated the incident INES level 0, but the safety authorities finally admitted to a level 2 rating.

Fuel Degradation (outside reactor core) (see 9.2.4)

Paks (Hungary) 2003 (see 9.2.4.1)

Design deficiencies of a chemical system built to clean 30 partially irradiated fuel assemblies from magnetic deposits in a special tank (outside of the vessel of the pressurized water reactor) caused insufficient cooling of all assemblies, which were heavily damaged. A subsequent IAEA investigation identified eight separate design errors. The system was developed, manufactured and delivered by AREVA NP. During the accident radioactive releases were about four times the noble gases and almost 200 times the Iodine-131 and aerosols released by all 58 French pressurized water reactors during the whole of 2003. The event was reclassified as Level 3 on the INES scale after an initial Level 2 rating.

Fires and Explosions (see 9.2.5)

14 December 2001, Brunsbüttel (Germany) (see 9.2.5.1)

A hydrogen explosion caused a high degree of damage to the spray system piping of the boiling water reactor. The head spray line is used for cooling the inner surface of the reactor pressure vessel head and the flange area upon plant shutdown. Some parts of the 5.6 mm diameter pipes were ruptured. An approximately 2.7 m long piping section had burst and was completely destroyed. Some sections of the piping were missing. Prior to this event the possibility of severe explosions caused by radiolysis gas during normal operation was nearly excluded.

Station Blackout (see 9.2.6)

18 March 2001 Maanshan (Taiwan) (see 9.2.6.1)

The pressurized water reactor was affected by a total loss of external and internal power supply. Power supply is crucial to evacuate residual heat from the reactor core. The plant is situated near the sea. Salt deposit on insulators due to foggy weather caused instability of the high voltage grid. During a switch to the grid a short circuit in a power switch of the emergency power line occurred and caused a cable fire. A breaker and switchgear was totally destroyed by the fire and the diesel generators could not be started up manually because of heavy smoke. It took about two hours to restore power supply.

25 July 2006, Forsmark, Sweden (see 9.2.6.2)

A short circuit in an outdoor switching station of the grid nearby the boiling water reactors caused the emergency shutdown (scram) of unit 1 and, in a complex scenario, led to a number of subsequent failures at the plant. Due to a design error, the disconnection of the plant from the grid and the switch to house load operation – where the power plant uses its own power to operate essential auxiliaries – did not function as planned. An inappropriate converter adjustment led to the failure of the attempt to connect safety related equipment to the emergency power supply. The start up of two of the four emergency diesel generators was aborted, which lead to a partial blackout even in the main control room. Due to the lack of information about the important parameters for a period of time the exact state of the plant and the consequences of potential actions to perform were unclear. The shift team decided nevertheless to try to reconnect the plant to the grid, which was performed successfully.

Generic Issues – Reactor Sump Plugging (see 9.2.7)

28 July 1992, Barseback-2 (Sweden) (see 9.2.7.1)

A leaking pilot valve in the boiling water reactor in Barseback initiated automatically safety functions like reactor scram, high-pressure safety injection, core spray and containment spray systems. The steam jet from an open safety valve was impinging on thermally insulated equipment. Insulating material was washed into the suppression pool and affected the emergency core cooling system, which is essential for heat removal in case of a leak the reactor coolant. Similar incidents occurred in several countries and the problem turned out to apply to many, if not most, of the light water reactors in the world.

Natural Events (see 9.2.8)

27 December 1999, Blayais-2 (France) (see 9.2.8.1)

The Blayais nuclear power plant site was flooded after heavy storms resulting in certain key safety equipments of the plant being under over 100,000 m3 of water, for example safety

injection pumps and the containment spray systems of units 1 and 2. The electrical system was also affected. Power supply was interrupted. Flying objects and debris rendered any intervention dangerous. All four units on the site were shut down. For the first time, the national level of the internal emergency plan (PUI) was triggered. The event was given an INES Level 2 rating.

Security Events and Malicious Act (see 9.2.9)

7 February 1993, Three Mile Island (USA) (see 9.2.9.1)

An unauthorized vehicle entered the owner-controlled area (OCA) of the Three Mile Island (TMI) nuclear power plant. No physical barriers were present to delay access. The vehicle continued to the protected area (PA) of the nuclear plant, smashed one of the entry gates, before crashing through a corrugated metal door and entering the turbine building of the Unit 1 reactor, which was operating at full power. The vehicle stopped 19 meters inside the turbine building, striking and damaging the insulation on an auxiliary steam line. A Site Area Emergency, the second highest emergency classification level, was declared. This was the second time this had occurred at the TMI plant (the first being the TMI Unit 2 meltdown in 1979). The intruder was not apprehended until four hours after he entered the site.

July 2000, Farley (USA) (see 9.2.9.2)

During an "Operational Safeguards Response Evaluation," or OSRE – war-game-type exercise to evaluate whether nuclear power plant security forces could effectively defend against an adversary team – the security force at Farley could not prevent the mock adversary team from simulating the destruction of entire target sets in two out of four exercises (and therefore simulating a core meltdown); and simulating the destruction of "significant plant equipment" in a third exercise.

29 August 2002, 17 TEPCO Reactors (Japan) (see 9.2.9.3)

The Tokyo Electric Power Company (TEPCO) operates 17 boiling water reactors and was also one of the most respected large companies in Japan. On 29 August 2002 the Japanese Nuclear Industrial Safety Agency (NISA), shocked the nation with the public revelation of a massive data falsification scandal at TEPCO. At that point 29 cases of "malpractice" had been identified, including the falsification of the operator's self-imposed inspection records at its nuclear power plants over many years. In the follow-up, all of the 17 TEPCO units had to be shut down for inspection and repair. It was reported later that these practices had gone on for as long as 25 years and the total number of events is put at nearly 200 so far. However, revelations of cover-ups and malpractice have extended to all major nuclear operators in Japan and continue to date. In the latest case, in early April 2007 Hokuriku Electric has admitted to a criticality incident at its Shika-1 boiling water reactor. The event had been covered up for almost eight years.

11 Annexes

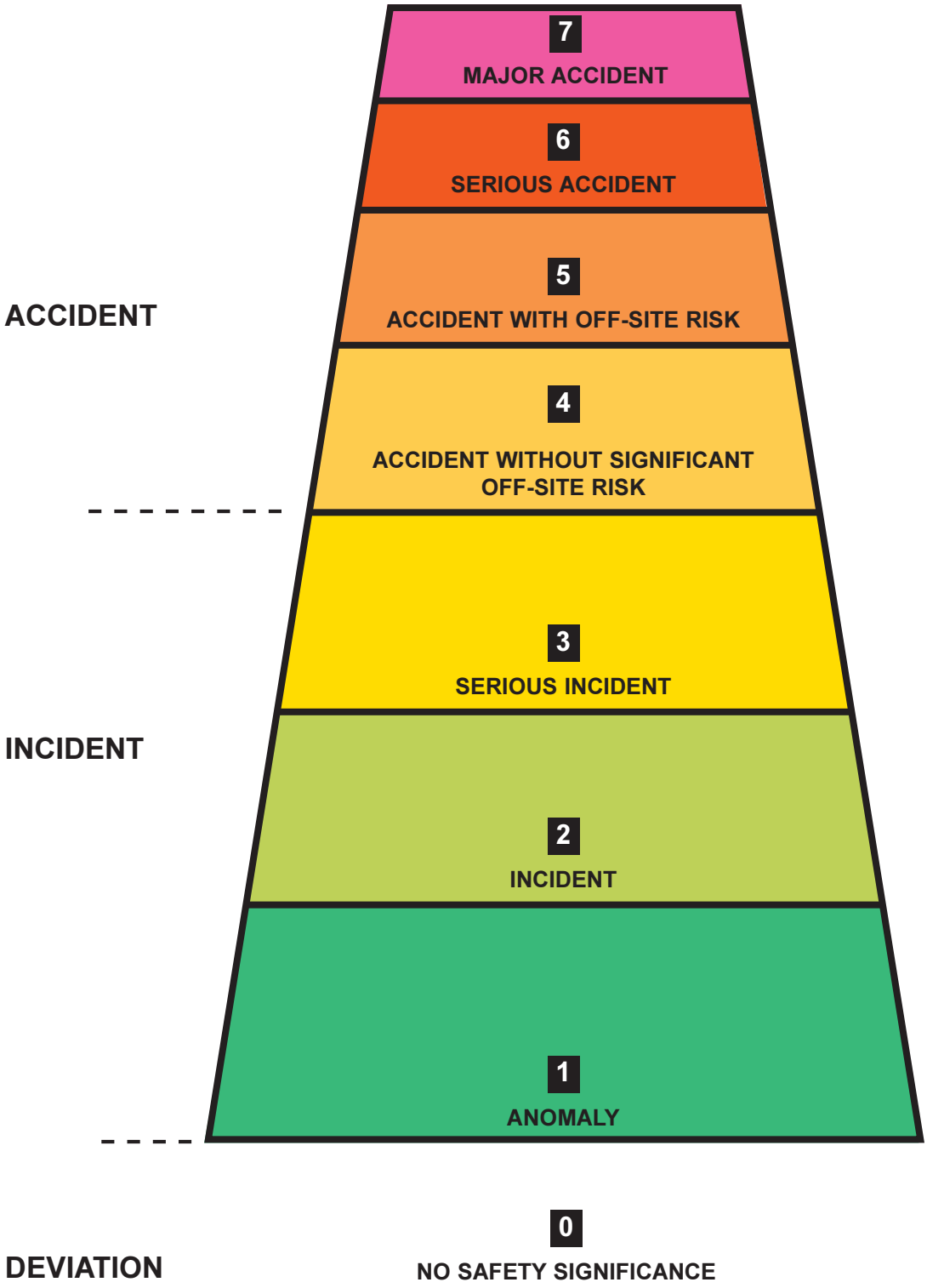
11.1 IAEA International Nuclear Event Scale (INES)
11.2 Chronology of Data Falsification at the Fukushima Nuclear Power Plant in Japan
11.3 Biographical Notes on the Authors

Annex 1

11.1 IAEA International Nuclear Event Scale (INES)

The International Nuclear Event Scale

For prompt communication of safety significance



General Description of the Scale

The International Nuclear Event Scale (INES) is a means for promptly communicating to the public in consistent terms the safety significance of events reported at nuclear installations. By putting events into proper perspective, the Scale can ease common understanding among the nuclear community, the media, and the public. It was designed by an international group of experts convened jointly in 1989 by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency (NEA) of the Organisation for Economic Co-operation and Development. The Scale also reflects the experience gained from the use of similar scales in France and Japan as well as from consideration of possible scales in several other countries.

The Scale was initially applied for a trial period to classify events at nuclear power plants and then extended and adapted to enable it to be applied to any event associated with radioactive material and/or radiation and to any event occurring during transport of radioactive material. It is now operating successfully in over 60 countries.

The INES Information Service, the communication network built up on request receives from and disseminates to the INES National Officers of 60 Member States, Event Rating Forms that provide authoritative information related to nuclear events. Event Rating Forms are circulated when events are significant for:

- operational safety (INES level 2 and above)
- public interest (INES level 1 and below)

The communication process has therefore led each participating country to set up a structure which ensures that all events are promptly rated using the INES rating procedure to facilitate communication whenever they have to be reported outside.

Events are classified on the Scale at 7 levels; the upper levels (4–7) are termed accidents and the lower levels (1–3) incidents. Events which have no safety significance are classified below scale at level 0 and are termed “deviations”. Events which have no safety relevance are termed “out of scale”. The structure of the Scale is shown opposite, in the form of a matrix with key words. Each level is defined in detail within the **INES User’s Manual**. Events are considered in terms of three safety attributes or criteria represented by each of the columns: off-site impact, on-site impact, and defence in depth degradation.

The second column in the matrix relates to events resulting in off-site releases of radioactivity. Since this is the only consequence having a direct effect on the public, such releases are understandably of particular concern. Thus, the lowest point in this column represents a release giving the critical group an estimated radiation dose numerically equivalent to about one-tenth of the annual dose limit for the public; this is classified as level 3. Such a dose is also typically about one-tenth of the average annual dose received from natural background radiation. The highest level is a major nuclear accident with widespread health and environmental consequences.

The third column considers the on-site impact of the event. This category covers a range from level 2 (contamination and/or overexposure of a worker) to level 5 (severe damage to the reactor core or radiological barriers).

All nuclear facilities are designed so that a succession of safety layers act to prevent major on-site or off-site impact and the extent of the safety layers provided generally will be commensurate with the potential for on- and off-site impact. These safety layers must all fail before substantial off-site or on-site consequences occur. The provision of these safety layers is termed “defence in depth”. The fourth column of the matrix relates to incidents at nuclear installations or during the transportation of radioactive materials in which these defence in depth provisions have been degraded. This column spans the incident levels 1–3.

An event which has characteristics represented by more than one criterion is always classified at the highest level according to any one criterion.

Events which do not reach the threshold of any of the criteria are rated below scale at level 0.

The back page of this leaflet gives typical descriptions of events at each level together with examples of the classification of nuclear events which have occurred in the past at nuclear installations.

Using the Scale

- The detailed rating procedures are provided in the INES User’s Manual. This leaflet should not be used as the basis for rating events as it only provides examples of events at each level, rather than actual definitions.
- Although the Scale is designed for prompt use following an event, there will be occasions when a longer time-scale is required to understand and rate the consequences of an event. In these rare circumstances, a provisional rating will be given with confirmation at a later date. It is also possible that as a result of further information, an event may require reclassification.
- The Scale does not replace the criteria already adopted nationally and internationally for the technical analysis and reporting of events to Safety Authorities. Neither does it form a part of the formal emergency arrangements that exist in each country to deal with radiological accidents.
- Although the same Scale is used for all installations, it is physically impossible at some types of installation for events to occur which involve the release to the environment of considerable quantities of radioactive material. For these installations, the upper levels of the Scale would not be applicable. These include research reactors, unirradiated nuclear fuel treatment facilities, and waste storage sites.
- The Scale does not classify industrial accidents or other events which are not related to nuclear or radiological operations. Such events are termed “out of scale”. For example, although events associated with a turbine or generator can affect safety related equipment, faults affecting only the availability of a turbine or generator would be classified as out of scale. Similarly, events such as fires are to be considered out of scale when they do not involve any possible radiological hazard and do not affect the safety layers.
- The Scale is not appropriate as the basis for selecting events for feedback of operational experience, as important lessons can often be learnt from events of relatively minor significance.
- It is not appropriate to use the Scale to compare safety performance among countries. Each country has different arrangements for reporting minor events to the public, and it is difficult to ensure precise international consistency in rating events at the boundary between level 0 and level 1. The statistically small number of such events, with variability from year to year, makes it difficult to provide meaningful international comparisons.
- Although broadly comparable, nuclear and radiological safety criteria and the terminology used to describe them vary form country to country. The INES has been designed to take account of this fact.

Examples of Rated Nuclear Events

- The 1986 accident at the Chernobyl nuclear power plant in the Soviet Union (now in Ukraine) had widespread environmental and human health effects. It is thus classified as Level 7.
- The 1957 accident at the Kyshtym reprocessing plant in the Soviet Union (now in Russia) led to a large off-site release. Emergency measures including evacuation of the population were taken to limit serious health effects. Based on the off-site impact of this event it is classified as Level 6.
- The 1957 accident at the air-cooled graphite reactor pile at Windscale (now Sellafield) facility in the United Kingdom involved an external release of radioactive fission products. Based on the off-site impact, it is classified as Level 5.
- The 1979 accident at Three Mile Island in the United States resulted in a severely damaged reactor core. The off-site release of radioactivity was very limited. The event is classified as Level 5, based on the on-site impact.
- The 1973 accident at the Windscale (now Sellafield) reprocessing plant in the United Kingdom involved a release of radioactive material into a plant operating area as a result of an exothermic reaction in a process vessel. It is classified as Level 4, based on the on-site impact.
- The 1980 accident at the Saint-Laurent nuclear power plant in France resulted in partial damage to the reactor core, but there was no external release of radioactivity. It is classified as Level 4, based on the on-site impact.
- The 1983 accident at the RA-2 critical assembly in Buenos Aires, Argentina, an accidental power excursion due to non-observance of safety rules during a core modification sequence, resulted in the death of the operator, who was probably 3 or 4 metres away. Assessments of the doses absorbed indicate 21 Gy for the gamma dose together with 22 Gy for the neutron dose. The event is classified as Level 4, based on the on-site impact.
- The 1989 incident at the Vandellos nuclear power plant in Spain did not result in an external release of radioactivity, nor was there damage to the reactor core or contamination on site. However, the damage to the plant’s safety systems due to fire degraded the defence in depth significantly. The event is classified as Level 3, based on the defence in depth criterion.
- The vast majority of reported events are found to be below Level 3. Although no examples of these events are given here, countries using the Scale may individually wish to provide examples of events at these lower levels.

Basic Structure of the Scale

(Criteria given in matrix are broad indicators only)
Detailed definitions are provided in the INES User's Manual

	CRITERIA OR SAFETY ATTRIBUTES		
	OFF-SITE IMPACT	ON-SITE IMPACT	DEFENCE IN DEPTH DEGRADATION
7 MAJOR ACCIDENT	MAJOR RELEASE: WIDESPREAD HEALTH AND ENVIRONMENTAL EFFECTS		
6 SERIOUS ACCIDENT	SIGNIFICANT RELEASE: LIKELY TO REQUIRE FULL IMPLEMENTATION OF PLANNED COUNTERMEASURES		
5 ACCIDENT WITH OFF-SITE RISK	LIMITED RELEASE: LIKELY TO REQUIRE PARTIAL IMPLEMENTATION OF PLANNED COUNTERMEASURES	SEVERE DAMAGE TO REACTOR CORE/RADIOLOGICAL BARRIERS	
4 ACCIDENT WITHOUT SIGNIFICANT OFF-SITE RISK	MINOR RELEASE: PUBLIC EXPOSURE OF THE ORDER OF PRESCRIBED LIMITS	SIGNIFICANT DAMAGE TO REACTOR CORE/RADIOLOGICAL BARRIERS/FATAL EXPOSURE OF A WORKER	
3 SERIOUS INCIDENT	VERY SMALL RELEASE: PUBLIC EXPOSURE AT A FRACTION OF PRESCRIBED LIMITS	SEVERE SPREAD OF CONTAMINATION/ACUTE HEALTH EFFECTS TO A WORKER	NEAR ACCIDENT NO SAFETY LAYERS REMAINING
2 INCIDENT		SIGNIFICANT SPREAD OF CONTAMINATION/ OVEREXPOSURE OF A WORKER	INCIDENTS WITH SIGNIFICANT FAILURES IN SAFETY PROVISIONS
1 ANOMALY			ANOMALY BEYOND THE AUTHORIZED OPERATING REGIME
0 DEVIATION	**NO**	**SAFETY**	**SIGNIFICANCE**
OUT OF SCALE EVENT	**NO SAFETY RELEVANCE**		

The International Nuclear Event Scale

For prompt communication of safety significance

LEVEL/ DESCRIPTOR	NATURE OF THE EVENTS	EXAMPLES
ACCIDENTS **7** **MAJOR ACCIDENT**	• External release of a large fraction of the radioactive material in a large facility (e.g. the core of a power reactor). This would typically involve a mixture of short and long-lived radioactive fission products (in quantities radiologically equivalent to more than tens of thousands of terabecquerels of iodine-131). Such a release would result in the possibility of acute health effects; delayed health effects over a wide area, possibly involving more than one country; long-term environmental consequences.	Chernobyl NPP, USSR (now in Ukraine), 1986
6 **SERIOUS ACCIDENT**	• External release of radioactive material (in quantities radiologically equivalent to the order of thousands to tens of thousands of terabecquerels of iodine-131). Such a release would be likely to result in full implementation of countermeasures covered by local emergency plans to limit serious health effects.	Kyshtym Reprocessing Plant, USSR (now in Russia), 1957
5 **ACCIDENT WITH OFF-SITE RISK**	• External release of radioactive material (in quantities radiologically equivalent to the order of hundreds to thousands of terabecquerels of iodine-131). Such a release would be likely to result in partial implementation of countermeasures covered by emergency plans to lessen the likelihood of health effects. • Severe damage to the installation. This may involve severe damage to a large fraction of the core of a power reactor, a major criticality accident or a major fire or explosion releasing large quantities of radioactivity within the installation.	Windscale Pile, UK, 1957 Three Mile Island, NPP, USA, 1979
4 **ACCIDENT WITHOUT SIGNIFICANT OFF-SITE RISK**	• External release of radioactivity resulting in a dose to the critical group of the order of a few millisieverts.* With such a release the need for off-site protective actions would be generally unlikely except possibly for local food control. • Significant damage to the installation. Such an accident might include damage leading to major on-site recovery problems such as partial core melt in a power reactor and comparable events at non-reactor installations. • Irradiation of one or more workers resulting in an overexposure where a high probability of early death occurs.	Windscale Reprocessing Plant, UK, 1973 Saint-Laurent NPP, France, 1980 Buenos Aires Critical Assembly, Argentina, 1983
INCIDENTS **3** **SERIOUS INCIDENT**	• External release of radioactivity resulting in a dose to the critical group of the order of tenths of millisievert.* With such a release, off-site protective measures may not be needed. • On-site events resulting in doses to workers sufficient to cause acute health effects and/or an event resulting in a severe spread of contamination for example a few thousand terabecquerels of activity released in a secondary containment where the material can be returned to a satisfactory storage area. • Incidents in which a further failure of safety systems could lead to accident conditions, or a situation in which safety systems would be unable to prevent an accident if certain initiators were to occur.	Vandellos NPP, Spain, 1989
2 **INCIDENT**	• Incidents with significant failure in safety provisions but with sufficient defence in depth remaining to cope with additional failures. These include events where the actual failures would be rated at level 1 but which reveal significant additional organisational inadequacies or safety culture deficiencies. • An event resulting in a dose to a worker exceeding a statutory annual dose limit and/or an event which leads to the presence of significant quantities of radioactivity in the installation in areas not expected by design and which require corrective action.	
1 **ANOMALY**	• Anomaly beyond the authorised regime but with significant defence in depth remaining. This may be due to equipment failure, human error or procedural inadequacies and may occur in any area covered by the scale, e.g. plant operation, transport of radioactive material, fuel handling, waste storage. Examples include: breaches of technical specifications or transport regulations, incidents without direct safety consequences that reveal inadequacies in the organisational system or safety culture, minor defects in pipework beyond the expectations of the surveillance programme.	
DEVIATIONS **0** **BELOW SCALE**	• Deviations where operational limits and conditions are not exceeded and which are properly managed in accordance with adequate procedures. Examples include: a single random failure in a redundant system discovered during periodic inspections or tests, a planned reactor trip proceeding normally, spurious initiation of protection systems without significant consequences, leakages within the operational limits, minor spreads of contamination within controlled areas without wider implications for safety culture.	**NO SAFETY SIGNIFICANCE**

* *The doses are expressed in terms of effective dose equivalent (whole dose body). Those criteria where appropriate can also be expressed in terms of corresponding annual effluent discharge limits authorized by National authorities.*

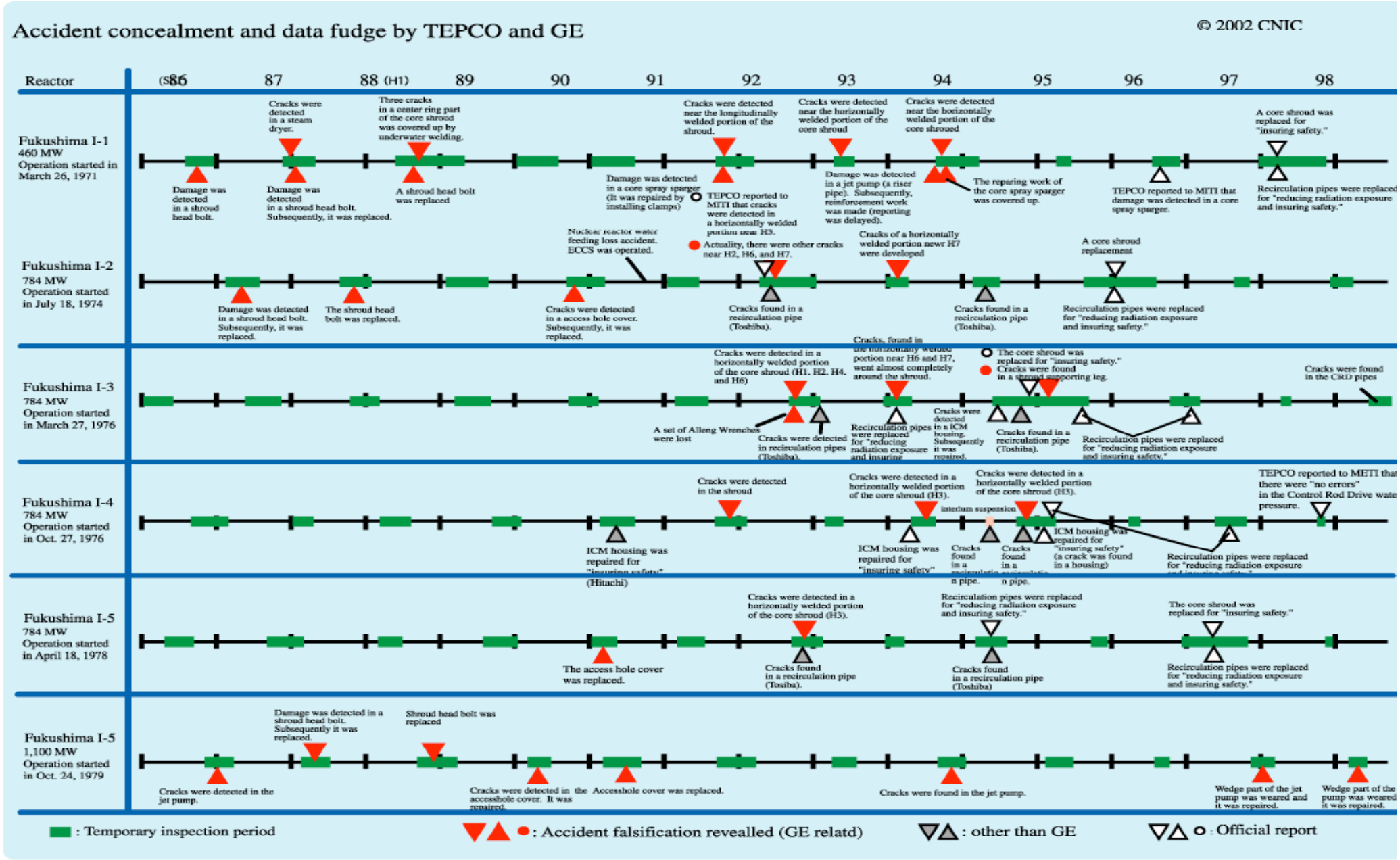
99-00305/FS-05

International Atomic Energy Agency
Wagramerstrasse 5
A-1400 Vienna, Austria

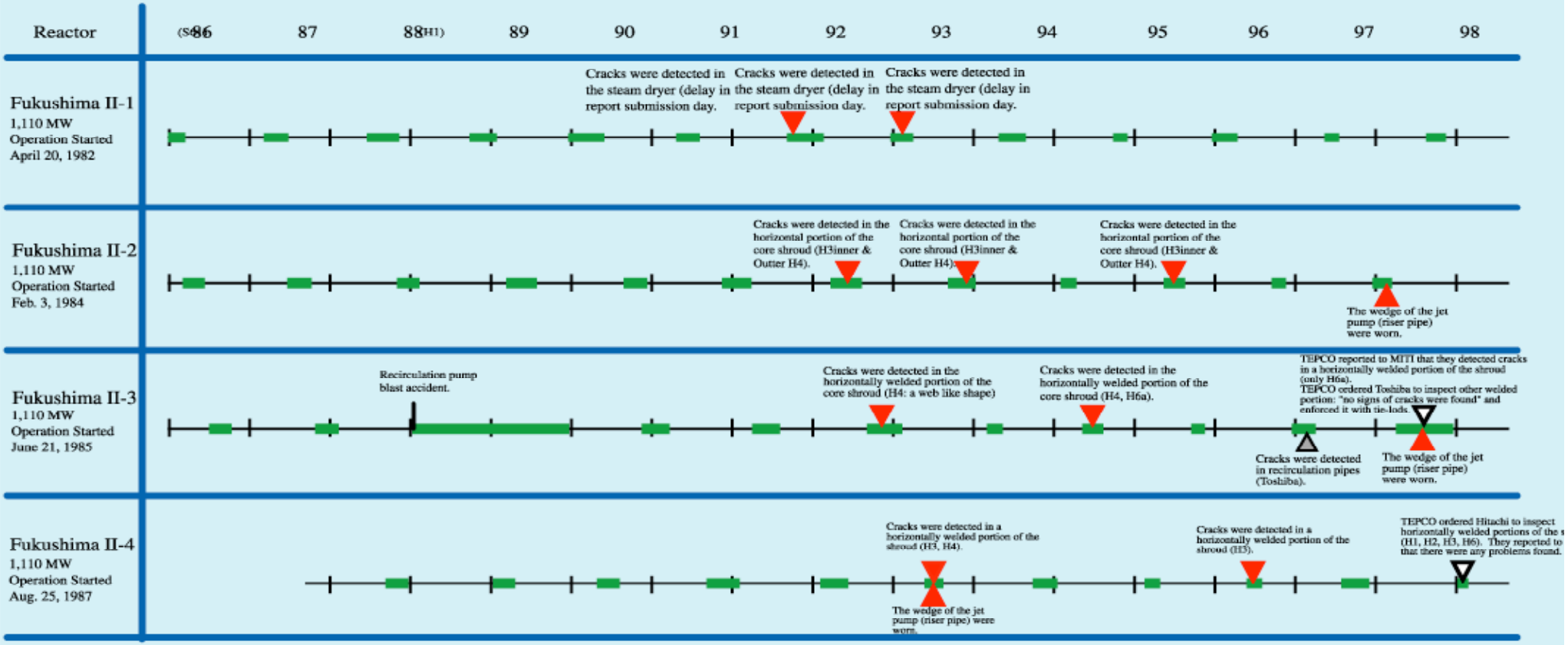
OECD Nuclear Energy Agency
Le Seine Saint-Germain-12
Boulevard des Iles
92130 Issy-les-Moulineaux, France

11.2 Chronology of Data Falsification at the Fukushima NPP, Japan

by Citizens' Nuclear Information Center, Tokyo


Accident concealment and data fudge by TEPCO and GE
© 2002 CNIC
Reactor
(S)86
87
88 (H1)
89
90
91
92
93
94
95
96
97
98
Fukushima I-1
460 MW
Operation started in
March 26, 1971
Damage was detected in a shroud head bolt.
Cracks were detected in a steam dryer.
Damage was detected in a shroud head bolt. Subsequently, it was replaced.
Three cracks in a center ring part of the core shroud was covered up by underwater welding.
A shroud head bolt was replaced
Damage was detected in a core spray sparger (It was repaired by installing clamps)
Cracks were detected near the longitudinally welded portion of the shroud.
TEPCO reported to MITI that cracks were detected in a horizontally welded portion near H3.
Cracks were detected near the horizontally welded portion of the core shroud
Damage was detected in a jet pump (a riser pipe). Subsequently, reinforcement work was made (reporting was delayed).
Cracks were detected near the horizontally welded portion of the core shroud
The repairing work of the core spray sparger was covered up.
TEPCO reported to MITI that damage was detected in a core spray sparger.
A core shroud was replaced for "insuring safety."
Recirculation pipes were replaced for "reducing radiation exposure and insuring safety."
Fukushima I-2
784 MW
Operation started
in July 18, 1974
Damage was detected in a shroud head bolt. Subsequently, it was replaced.
The shroud head bolt was replaced.
Nuclear reactor water feeding loss accident. ECCS was operated.
Cracks were detected in a access hole cover. Subsequently, it was replaced.
Actuality, there were other cracks near H2, H6, and H7.
Cracks found in a recirculation pipe (Toshiba).
Cracks of a horizontally welded portion newr H7 were developed
Cracks found in a recirculation pipe (Toshiba).
A core shroud replacement
Recirculation pipes were replaced for "reducing radiation exposure and insuring safety."
Fukushima I-3
784 MW
Operation started
in March 27, 1976
Cracks were detected in a horizontally welded portion of the core shroud (H1, H2, H4, and H6)
A set of Alleng Wrenches were lost
Cracks were detected in recirculation pipes (Toshiba).
Cracks, found in the horizontally welded portion near H6 and H7, went almost completely around the shroud.
Recirculation pipes were replaced for "reducing radiation exposure and insuring
Cracks were detected in a ICM housing. Subsequently it was repaired.
The core shroud was replaced for "insuring safety."
Cracks were found in a shroud supporting leg.
Cracks found in a recirculation pipe (Toshiba).
Recirculation pipes were replaced for "reducing radiation exposure and insuring safety."
Cracks were found in the CRD pipes
Fukushima I-4
784 MW
Operation started
in Oct. 27, 1976
ICM housing was repaired for "insuring safety" (Hitachi)
Cracks were detected in the shroud
Cracks were detected in a horizontally welded portion of the core shroud (H3).
ICM housing was repaired for "insuring safety"
interim suspension
Cracks found in a n pipe.
Cracks found in a n pipe.
Cracks were detected in a horizontally welded portion of the core shroud (H3).
ICM housing was repaired for "insuring safety" (a crack was found in a housing)
Recirculation pipes were replaced for "reducing radiation exposure
TEPCO reported to METI that there were "no errors" in the Control Rod Drive water pressure.
Fukushima I-5
784 MW
Operation started
in April 18, 1978
The access hole cover was replaced.
Cracks were detected in a horizontally welded portion of the core shroud (H3).
Cracks found in a recirculation pipe (Tosiba).
Recirculation pipes were replaced for "reducing radiation exposure and insuring safety."
Cracks found in a recirculation pipe (Toshiba)
The core shroud was replaced for "insuring safety."
Recirculation pipes were replaced for "reducing radiation exposure and insuring safety."
Fukushima I-5
1,100 MW
Operation started
in Oct. 24, 1979
Cracks were detected in the jet pump.
Damage was detected in a shroud head bolt. Subsequently it was replaced.
Shroud head bolt was replaced
Cracks were detected in the accesshole cover. It was repaired.
Accesshole cover was replaced.
Cracks were found in the jet pump.
Wedge part of the jet pump was weared and it was repaired.
Wedge part of the pump was weared it was repaired.
: Temporary inspection period
: Accident falsification revealled (GE relatd)
: other than GE
: Official report

（2） Accident concealment and data falsification by TEPCO and GE



Annex 3

Biographical Notes on the Authors

Georgui Kastchiev

Senior Scientist at the Institute of Risk Research, University of Vienna, Faculty of Earth Sciences, Geography and Astronomy. G. Kastchiev graduated from University of Sofia in Bulgaria in 1972 as a diploma physicist. In 1972 he started his career as reactor physicist in NPP Kozloduy. He received a Ph.D. in reactor physics and safety from the University of Sofia in 1987. Dr. Kastchiev worked as a lecturer at the Institute of Nuclear Engineering, Kozloduy/Sofia from 1989 to 1993 and as a guest engineer in the AP 600 Project, Westinghouse, USA in 1994. During 1995-1997 Dr. Kastchiev acted as a consultant to the Institute of Risk Research, University of Vienna, Austria, until he was appointed head of the Bulgarian Nuclear Safety Authority in 2002. He worked there for four years and spent one year as a guest professor at the Tokyo Institute of Technology. Since 2006 he is back in the Institute of Risk Research, University of Vienna, Austria.

Wolfgang Kromp

Professor, Ph.D. in Physics, University of Vienna, head of the 'Institute of Risk Research' of the University of Vienna, Faculty of Earth Sciences, Geography and Astronomy, holds forty years of experience in research and teaching at university level, extended research fellowship and visiting professorship at the Max-Planck Institute in Stuttgart, Germany and the Carnegie-Mellon University in Pittsburgh, USA. Research in the area of material related problems, using ultrasonic techniques for material testing and composition; focus on material related questions concerning nuclear safety. He is member of the Nuclear Advisory Board to the Austrian Federal Chancellor, the Scientific Commission of the Austrian Federal Ministry of Defense and the Technical Committee for Standardization ON-K 246 Risk, Safety and Crisis Management of the Austrian Standards Institute. Konrad Lorenz Environmental Award 1991 of the Austrian Ministry of Science and Research. Participation in safety assessments of several nuclear power plants and spent fuel interim storages; research on radioactive contamination and risk perception; socio-economic research on fusion (SERF). Feasibility and risk studies on sustainable energy production from biomass. Study on security of food production in oil reduced agriculture.

Stephan Kurth

Dipl.-Ing, since 1993 with Oeko-Institut e.V. - Institute for Applied Ecology, Darmstadt, Germany. Head of the Plant Safety Group of the Nuclear Engineering & Plant Safety Division. Focus on safety assessment, event analysis, environmental impact assessment and regulation. Member of official national advisory committees dealing with safety issues of nuclear and non-nuclear plants.

David Lochbaum

Director, Nuclear Safety Project, Union of Concerned Scientists (UCS), leads UCS's efforts to ensure the safety of nuclear power in the United States by monitoring civilian nuclear plants to identify and publicize safety risks. Mr. Lochbaum has more than 17 years experience in nuclear power plant start-up testing, operations, licensing, software development, training, and design engineering. He worked at the Hope Creek and Salem (New Jersey), Brunswick (North Carolina), Perry (Ohio), Limerick and Susquehanna (Pennsylvania), Wolf Creek (Kansas), Haddam Neck (Connecticut), Fitzpatrick and Indian Point 3 (New York), Grand Gulf (Mississippi), Browns Ferry (Alabama), and Hatch (Georgia) nuclear plants. In 1992, he and a colleague identified deficiencies in the design for spent fuel pool cooling at the Susquehanna plant and reported their concerns to the plant owner, to the Nuclear

Regulatory Commission, and then to Congress. Their efforts resulted in safety improvements at Susquehanna and at other nuclear plants with similar problems.

Ed Lyman

Edwin Lyman is a Senior Staff Scientist in the Global Security program at the Union of Concerned Scientists in Washington, DC, a position he has held since May 2003. Before coming to UCS, he worked at the Nuclear Control Institute for nearly eight years, first as scientific director, and then as president. He earned a doctorate in physics from Cornell University in 1992. From 1992 to 1995, he was a postdoctoral research associate at Princeton University's Center for Energy and Environmental Studies.
His research focuses on security and environmental issues associated with the management of nuclear materials and the operation of nuclear power plants. He has published articles and letters in journals and magazines including Science, The Bulletin of the Atomic Scientists and Science and Global Security. He is an active member of the Institute of Nuclear Materials Management. In the spring of 2001, he served on a Nuclear Regulatory Commission expert panel on the role and direction of the NRC Office of Nuclear Regulatory Research and briefed the Commission on his findings. In July 2001, he was again invited to a Commission meeting to discuss the licensing of new nuclear reactors in the United States.

Michael Sailer

Dipl.-Ing., since 1980 with Oeko-Institut e.V - Institute for Applied Ecology, Darmstadt/Freiburg/Berlin, Germany, currently Deputy Director of the Institute, Coordinator of the Nuclear Engineering & Plant Safety Division, numerous publications on reactor safety and radioactive waste disposal issues, member of official advisory committees on both national and European levels.

Mycle Schneider

Independent Consultant on Energy and Nuclear Policy. Between 1983 and April 2003 he was executive director of the energy information service WISE-Paris. He has given evidence and held briefings at Parliaments in eight countries and at the European Parliament. Since 2004 he teaches within the International MSc for Project Management for Environmental and Energy Engineering at the *Ecole des Mines* in Nantes. In 2005 he has been appointed as nuclear security specialist to advise the UK Committee on Radioactive Waste Management (CoRWM). In 2006-07 he has been part of a consultant consortium that assessed nuclear decommissioning and waste management funding issues on behalf of the European Commission. Between 1998 and 2003 he has been an advisor to the French Environment Minister's Office and to the Belgian Minister for Energy and Sustainable Development. Since 2000 he is a consultant on nuclear issues to the German Environment Ministry.
Mycle Schneider has provided information and consulting services to a large variety of clients. Media representatives from around the world have inquired for his information, advise or complete features including many TV and radio stations, electronic and print media. His numerous publications cover the analysis of nuclear proliferation, security and safety, as well as environmental and energy planning issues.
In 1997 he was honored with the Right Livelihood Award ("Alternative Nobel Prize") together with Jinzaburo Takagi for their work on plutonium issues (http://rightlivelihood.org/recip.htm).