Unclassified **NEA/CNRA/R(2014)1**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

06-Jan-2014

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

NEA/CNRA/R(2014)1
Unclassified

WORKING GROUP ON OPERATING EXPERIENCE [WGOE]

REPORT ON FUKUSHIMA DAIICHI NPP PRECURSOR EVENTS

JT03350819

Complete document available on OLIS in its original format

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation’s statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the OECD Secretary-General.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 31 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Russian Federation, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information.

The NEA Data Bank provides nuclear data and computer program services for participating countries. In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

The Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (NEA) is an international committee made up primarily of senior nuclear regulators. It was set up in 1989 as a forum for the exchange of information and experience among regulatory organisations.

The committee is responsible for the programme of the NEA, concerning the regulation, licensing and inspection of nuclear installations with regard to safety. The committee's purpose is to promote cooperation among member countries to feedback the experience to safety improving measures, enhance efficiency and effectiveness in the regulatory process and to maintain adequate infrastructure and competence in the nuclear safety field. The CNRA's main tasks are to review developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them or avoid disparities among member countries. In particular, the committee reviews current management strategies and safety management practices and operating experiences at nuclear facilities with a view to disseminating lessons learned.

The committee focuses primarily on existing power reactors and other nuclear installations; it may also consider the regulatory implications of new designs of power reactors and other types of nuclear installations.

In implementing its programme, the CNRA establishes cooperative mechanisms with the Committee on the Safety of Nuclear Installations (CSNI) responsible for the programme of the Agency concerning the technical aspects of the design, construction and operation of nuclear installations. The committee also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH) and NEA's Radioactive Waste Management Committee (RWMC) on matters of common interest.

TABLE OF CONTENT

1. INTRODUCTION

1.1 Task Description

During its 26th meeting held in December 2011, the CNRA assigned the WGOE the task to report on new operating experience lessons learned from the 2011 Fukushima Daiichi NPP accident [1]. The main objective of the task is to identify and analyse previous operating events that have significant similarities to the Fukushima Daiichi NPP accident. The task focused on a review of these previous nuclear power plant operating events to address the following questions:

- The Fukushima Daiichi NPP accident, could it have been prevented?
- If there is a next severe accident, may it be prevented?

The main safety goal of the nuclear power industry is the prevention of accidents and continuous assurance of public health and safety. The proper implementation of the lessons learned from the evaluation of operating experiences is one of the major ways to achieve this goal. The worth of such lessons learned has been recognized in the nuclear industry over the last several decades. The accident at Three Mile Island in 1979 initiated the international exchange of information related to nuclear power plant operating events, their root causes and the related lessons learned. The Incident Reporting System (IRS) was started by the NEA in 1981 and extended to the non-OECD countries in 1983. Now, the IRS is jointly run by the IAEA and the NEA and been renamed the International Reporting System for Operating Experience. The IRS was one main focus of the Principal Working Group 1, the predecessor of the WGOE.

Despite this long international data exchange and numerous in-depth topical investigations, the accident at Fukushima Daiichi NPP raised questions if previous operating experience may have highlighted areas of concern, and if properly addressed, could have either minimized the potential for core damage or enhanced the mitigation of the event. Therefore the CNRA requested the WGOE to investigate the international operating experience feedback response from the previous operational events related to the Fukushima Daiichi NPP accident. The CNRA further asked whether the events were adequately addressed prior to Fukushima Daiichi NPP accident and what could be improved in the international operating experience feedback programme.

Furthermore, the WGOE was asked to interact with other working groups who could provide insights in this area. This task report includes information on significant precursor events developed by the CSNI Working Group on Risk Assessment (WGRISK).

1.2 Approaches of the report

The Fukushima Daiichi NPP accident serves as a case study for various disciplines within nuclear sciences. Researchers worldwide in health physics, radio-ecology, severe accident analysis, and human and organisational factors have investigated the progression of the accidents and their consequences. The WGOE is focused on the lessons learned from operating experiences, and the Fukushima Daiichi NPP accident is an extremely important source for deriving generic lessons. The main goal of the operating experience feedback is to prevent such accidents. Therefore, this report analyses whether and why this accident could not be prevented. To understand the role operating experience could play in identifying plant vulnerabilities and minimizing the potential of severe accidents leading to significant public health consequences, the identification of the initiating events and the barriers that failed during the Fukushima Daiichi NPP accident is necessary.

The approach followed by the WGOE in this report is consistent with the working group approach for generic reports on the evaluation of operating experiences. It is developed in Chapters 2 and 3 and includes the following steps:

- Analysis of the triggering event to clarify the event sequences and the initiating events.
- Selection of a set of previous events with similar initiators.
- Summary of the main generic lessons derived from the in-depth analyses of these events.

The report focusses on the initiators and event sequences. A root cause analysis has not been performed. The answer to the question “Why it was not prevented?” is not part of this report.

The main tool for event evaluation of WGOE is the IRS [2] that was established by the NEA in 1981 and is now jointly operated with the IAEA. It contains safety significant events with important lessons to be learned.

Thus the analysis starts with a description of the sequences of the Fukushima Daiichi NPP accident from a technical view-point. The evaluation focusses on the initiating events and the main system unavailabilities during the accident sequences. A detailed analysis of the accident management within the accident sequence is not part of the report. Neither is there an evaluation of the safety culture or of the safety management at TEPCO before the accident. These aspects are dealt with by other NEA working groups.

The leading question to the first part is: have similar sequences happened before? A search of the IRS database was performed to identify events with similar characteristics as the Fukushima Daiichi NPP accident. The results of the search are used to identify precursors that cover a wide range of characteristics and phenomena observed in the accident.

The evaluation of the five events that share similarities with the accident at Fukushima Daiichi NPP focusses on two questions:

- How were severe core damage accidents prevented during these events? Addressing this question an analysis of the effective barriers is required that stopped the event sequence.
- What are the main – and generic – lessons to be learned from these events? For most of the events studied, additional documentation was used beyond that available in the IRS database.

These lessons learned should address potential plant vulnerabilities and – if correctly implemented – minimize the potential for severe core damage events. These lessons learned are related to the question whether or not operating experience could provide significant insights that may have mitigated the accident at Fukushima Daiichi NPP.

In addition to the IRS based investigation performed by the WGOE, the WGRISK was asked to identify important precursor events that could offer further insights into the basis of their risk significance. To that end, the WGRISK developed four criteria to select risk-significant events for consideration by the WGOE. These precursor events have also been analysed regarding their initiators, their effective barriers and their main lessons learned. The WGRISK contribution is embedded in Chapter 4.

2. MAIN FUKUSHIMA DAIICHI NPP ACCIDENT FEATURES

2.1 Description of the Fukushima Daiichi NPP accident features

The Fukushima Daiichi NPP accident was initiated by an earthquake and flooding resulting from the subsequent tsunami. The earthquake itself has not led to any relevant damage to safety significant systems or structures. But, the earthquake caused the breakdown of a large part of the external electric power grid. At the Fukushima Daiichi NPP site, the external grid was lost after the earthquake shocks.

The tsunami caused a flooding of the site far beyond the design basis assumptions. This affected each of the units in slightly different manners [3], which are shortly described below. For more details on the event sequences and further descriptions of the accident please, refer to other reports like [3]. The Fukushima Daiichi NPP accident had similarities with the following types of main initiating events and conditions:

- Loss of off-site power.
- Loss of ultimate heat sink.
- Loss of residual heat removal.
- Loss of DC power.
- Loss of AC power.
- Loss of control room.
- Loss of containment function.
- Fuel rod-water-interaction, hydrogen formation and combustion.

2.2 Short description of the accident sequences of the Units 1-4

After the earthquake the Units 1, 2 and 3 of Fukushima Daiichi NPP tripped. As the external power supply was not available, the emergency diesel generators (EDGs) started as per design. The earthquake did not cause significant adverse effects on the functioning of the safety systems. About 40-50 minutes after the earthquake a series of seven tsunamis hit the coast and flooded the NPPs site. As a result of the flooding the emergency power supply system failed. A large fraction of the batteries of the uninterruptable power supply system were unavailable.

Unit 4 was in outage. All fuel was stored at the spent fuel pool.

Because of the destruction caused by the tsunami the emergency (or essential) service water system was damaged and not available.

Due to the full station blackout (SBO), the failure of the batteries and the unavailability of the emergency service water systems, the residual heat removal systems and the emergency cooling systems of the NPPs failed. Owing to the absence of the residual heat removal the core got damaged and hydrogen was produced. Steam and hydrogen release/leakage led to the rise of pressure in the containment.

It is supposed, that the containments got damaged and hydrogen was released into the reactor building, which led to explosions at Units 1, 3 and 4.

Unit 1

After the reactor shutdown and loss of offsite power, the steam line isolation operated as per design. The pressure inside RPV increased over 70 bars. Both Isolation Condensers (ICs) started automatically but were switched off manually to avoid a decrease of temperature faster than 55 K/h. Until the tsunami hit, one IC was switched on and off several times.

After the tsunami hit, the EDGs and batteries were flooded and unavailable. Due to the loss of power, the isolation condensers were unavailable. Because of the SBO and the additional loss of DC power, there was no system available for feeding the reactor and removing the residual heat.

After the pressure inside RPV increased the safety relief valves opened and steam was released to the wetwell. The water level inside the vessel decreased while the pressure and temperature inside the wetwell increased.

Several attempts to establish the ICs by opening valves manually were unsuccessful.

After the installation of temporary control room lighting and instrumentation, venting was prepared on account of high containment pressure. After several attempts failed, opening the affected valves was only possible by installing a temporary pressured air supply. As a decrease of containment pressure was confirmed, a successful venting is supposed. One hour later, an explosion occurred, supposable caused by the probably untight containment.

By a station fire engine, water was pumped into RPV, as an alternative water injection, using the fire-extinguishing system and core spray system lines. These measures were interrupted several times as water storages got empty. It is not clear how long these interruptions lasted.

Offsite power was restored to Unit 1 nine days after the event.

Unit 2

After the reactor shutdown and loss of offsite power, the steam line isolation operated as per design. The pressure inside RPV increased over 70 bars. The safety relief valves (SRVs) opened so water level and pressure inside the vessel decreased.

Several times RCIC was started manually to feed RPV, but was switched off automatically due to high water level.

The pressure of RPV was controlled by SRVs. Steam from the RCIC turbine and SRVs led to an increase of the temperature at the wetwell. RHR-pumps and the emergency service system were started.

After the tsunami hit, the EDGs and batteries were flooded and unavailable. Further the emergency service water system was damaged. As a consequence of the loss of DC power the instrumentation was not available, which caused the unavailability of HPCI control. All RHR-pumps failed and the heat removal of the wetwell stopped. Temperature and pressure increased both in the wetwell and the drywell.

After reconstructing the instrumentation, a constant level inside the RPV was measured. This led to the assumption that RCIC worked and was feeding water into RPV. Later the water intake of RCIC was manually switched from condensate tank to wetwell. Eventually, RCIC has continued to run for approximately 70 hours with DC power lost.

Due to increasing pressure inside, the drywell venting was tried but no pressure decrease was observed. It is not confirmed whether venting was successful or not.

Works to establish a temporary feeding of RPV were interrupted by the explosion at Unit 3. The water level in RPV began to decrease, so it is supposed that RCIC tripped and RPV feeding stopped. To feed RPV fire engines were prepared but could not inject water due to high RPV pressure. Using additional batteries the DC supply of SRVs could be established. So it was possible to decrease the pressure and feed the RPV by a fire-engine through the core spray system.

Offsite power was restored to Unit 2 nine days after the event.

Unit 3

After the reactor shutdown and loss of offsite power, the steam line isolation operated as per design. The pressure inside RPV increased over 70 bars. The safety relief valves opened so water level and pressure inside the vessel decreased.

RCIC was started manually to feed RPV, but was switched off automatically due to high water level.

After the tsunami hit the EDGs tripped. In contrast to Units 1 and 2 the batteries were not completely damaged, so DC supply was partially available. A part of the instrumentation was not available, but RCIC could be put into operation.

RCIC tripped unexpectedly due to malfunction of a valve and could not be established once again after running for approximately 20 hours. One hour after the RCIC trip, HPCI automatically started on low water level in RPV but was switched off manually 14 hours later considering the possibility of HPCI turbine line break due to vibration caused by decreased turbine rotation speed. HPCI could not be restarted due to depletion of batteries. Starting RCIC was not successful, too. As pressure inside RPV increased, a feeding by alternative measures was not possible.

Venting was initiated, and due to decreasing pressure inside the containment it is supposed that this measure was successful.

After this, feeding the RPV with sea water was possible. On 14 March 2011, an explosion occurred and the fire engines and hoses feeding RPV were damaged. RPV feeding was interrupted.

Offsite power was restored to Unit 3 eleven days after the event.

Unit 4

The unit was in a refuelling outage and all of the fuels were placed in the spent fuel pool (SFP). As during outage the process computer was not available no recordings of a probable successful start of one of two EDGs is documented (the other EDG was out-of-service for maintenance).

The SFP cooling was lost due to loss of offsite power, but no actions were taken to restore the cooling, e. g. restarting RHR, because of sufficient water level in the pool and low water temperature. After the tsunami hit power supply was lost, so a cooling of SFP was not possible any more.

On 15 March 2011 a hydrogen explosion occurred in the reactor building. It is most widely accepted that the cause of hydrogen explosion is associated with the backflow of gases from Unit 3 during venting through the standby gas treatment system lines.

On 20 March 2011, a sporadic feeding of SFP was initiated by using the water cannons

On 22 March 2011, a water supply to SFP was commenced by using concrete pumping trucks.

Subsequent analyses and inspections determined that the SFP water levels never dropped below the top of fuel and that no significant fuel damage had occurred.

2.3 Coding Fukushima Daiichi NPP accident in the IRS database

As a first step to identify potential precursor events to Fukushima Daiichi NPP accident, a coding of the Fukushima Daiichi NPP accident using the IRS codes was tried [2]. As a basis to this task the code category "characteristics of the event" was selected. Thus, the Fukushima Daiichi NPP accident could be characterized according to its main features respectively initiators. It is obvious that some of the initiators mentioned in Section 2.1 are not directly respected in the guide words. The second step included the search of the IRS database in order to select events that have been coded with the same characteristics.

Table 1. **Results of the coding using IRS guidewords "Characteristics of the event"**

IRS Key Words	Total records in IRS	Fukushima
7.0 Other characteristics	605	?
7.1 Degraded fuel	68	Yes
7.2 Degraded reactor coolant boundary	476	Yes
7.3 Degraded reactor containment	118	Yes
7.4 Loss of safety function	131	Yes
7.5 Significant degradation of safety function	626	Yes
7.6 Failure or significant degradation of the reactivity control	255	Yes
7.7 Failure or significant degradation of plant control	211	Yes
7.8 Failure or significant degradation of heat removal capability	530	Yes
7.9 Loss of off-site power	180	Yes
7.10 Loss of on-site power	226	Yes
7.11 Transient	530	?
7.11.0 Other transient	39	?
7.11.1 Power transient	154	?
7.11.2 Temperature transient	100	?
7.11.3 Pressure transient	162	?
7.11.4 Flow transient	109	?
7.12 Physical hazards (internal or external to the plant)	199	Yes
7.13 Discovery of major condition not previously considered or analysed	435	Yes
7.14 Fuel handling event	94	No
7.15 Radwaste event	61	No
7.16 Security, safeguards, sabotage or tampering event	13	No

2.4 Results of the coding and the database search

Table 1 shows the results of the search. It is obvious that more than half of the characteristics can be applied to the Fukushima Daiichi NPP accident. The codes starting with "7.11 Transient" could be chosen for the Fukushima Daiichi NPP accident, but these types of transients did not play a major role in the accident sequence. The numbers of events reported to the IRS and having one or more of these characteristics are shown in the second column. In most cases hundred or several hundreds of events have been given these codes. It is interesting that there are comparatively few events that have been characterised with “Degraded fuel”. On the other hand, among these events there are three with molten or severely degraded fuel: St. Laurent in France [4], Paks in Hungary [5], TMI-2 [6] and Fukushima itself, as part of an event report of another country [7] presenting requirements for its national NPPs based on the Fukushima Daiichi NPP accident.

It has to be taken into account that the results of the search depend on the date of the search since the database is continuously growing.

Several major nuclear accidents are not part of the IRS database, either because they occurred before the IRS was set up in 1982 or the event was not reported to the IRS (Chernobyl-4). One main reason may be that there have been published very detailed event investigation reports that are out of scope of the IRS. Another fact should also be respected: not all countries with commercial nuclear power plants are member of the IRS. Thus, at least one interesting event (loss of off-site power and loss of emergency power for 7 hours) could not be described here, because there is neither an IRS report nor other authorised reports available.

The result of the short task is that the main characteristics of the Fukushima Daiichi NPP accident have been reported before to the IRS database. All characteristics of the Fukushima Daiichi NPP accident could easily be coded with the existing IRS guide words. There is no need to improve the coding based on this task.

3. DESCRIPTION OF FUKUSHIMA DAIICHI NPP PRECURSOR EVENTS

3.1 Definition of Fukushima Daiichi NPP precursor events

The investigation of the Fukushima Daiichi NPP accident was focused on the initiating events that have triggered the catastrophe. The sequence of main Fukushima initiators led to following main initiators (see Section 2.1):

- Earthquake (Even if the earthquake did not cause any major damage at the plant, but it was the origin of the tsunami.).
- Tsunami.
- Flooding (which was a direct consequence of the tsunami).
- Loss of off-site power due to loss of the grid caused by the earthquake.
- Loss of EDG (here it was a consequence of the flooding).
- Loss of AC/DC power (here it was a consequence of the flooding).
- Loss of control room (mainly caused by the loss of DC power).
- Loss of residual heat removal (mainly caused by the tsunami).
- Hydrogen combustion / explosion (caused by the long term loss of the residual heat removal).

This long list of initiators in combination with the main characteristics of the accident (see Chapter 2) set up the basis for the selection of events that are further analysed.

3.2 Selection of events

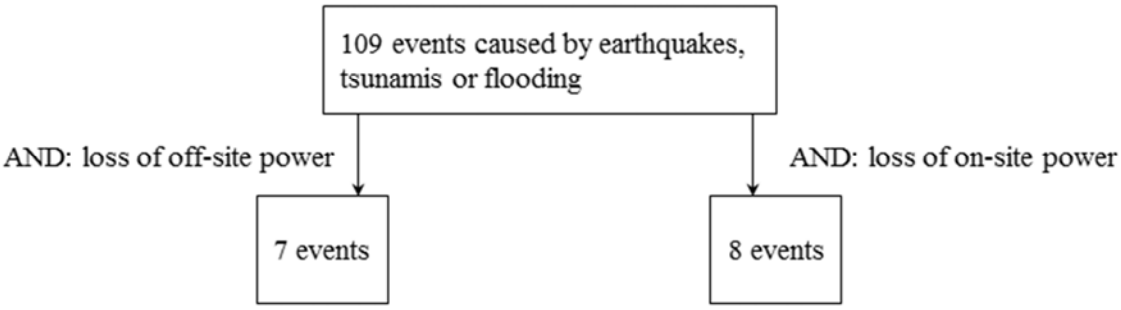
This long list of causes in combination with the main characteristics of the accident (see Chapter 2) found the basis for the selection of events that are further analysed by screening of the IRS database, using the codes listed in the table below.

Table 2. **Correspondence between main Fukushima causes / characteristics and IRS codes**

Causes	Characteristics	IRS coding	Comments
Earthquake		5.1.7.4	Code 5.1.7 “environmental (external to the plant)” was used also.
Tsunami		5.1.7.4 or 5.1.7.2	
Flooding		5.1.7.2 or 5.1.6.4	Covers both external and internal flooding.
	Loss of off-site power	7.9	
	Loss of EDG	7.10	Code 7.10 “Loss of on-site power” covers these two categories
	Loss of AC/DC	7.10	
	Loss of Control Room	7.7	
	Loss of Residual Heat Removal	7.8	
	Hydrogen combustion / explosion	7.12	This code corresponds to “Physical hazards (internal or external to the plant)” such as flooding, fire and explosion

The IRS search engine does not allow the use of the Boolean tool "AND" so each code has been searched in the IRS database and the results have been combined in an Excel spreadsheet to identify the events which a sequence of causes / characteristics similar to the Fukushima Daiichi NPP accident.

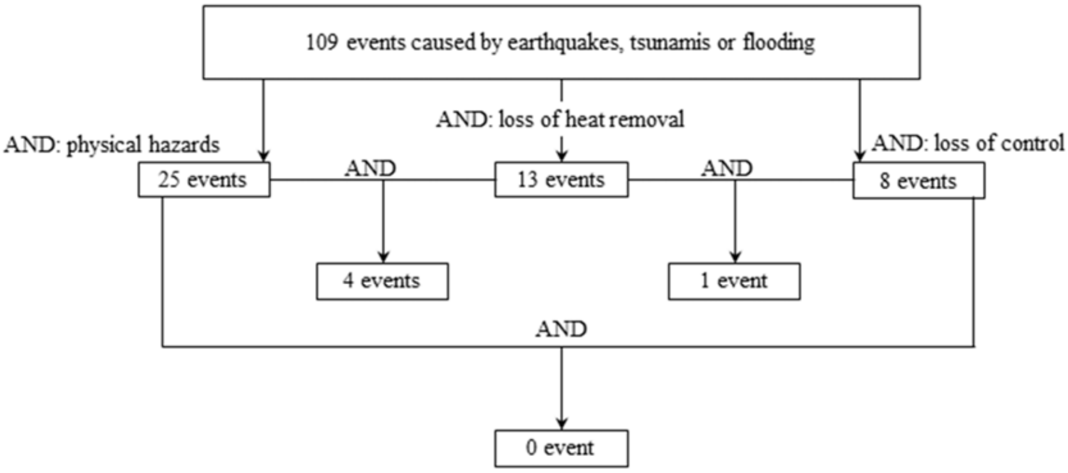
Figure 1.



All 13[1] event reports were analysed and not all are relevant for the present report: some of them relate to flooding in a limited area, flooding with limited consequences on the power supply or to events caused by the Tohoku earthquake. At the end, only one event report was retained as relevant for this report: Blayais-1, France, 27 December 1999 (IRS 7342) [8-9].

Considering the small number of events, it was decided to extend the search by removing the filter on "Loss of off-site power" and "loss of on-site power", *i.e.* to identify the events caused by earthquake / tsunami / flooding and including the loss of control room, loss of heat removal or hydrogen explosion.

Figure 2.



All 5 event reports combining 2 characteristics of Fukushima Daiichi NPP accident and caused by the relevant hazards have been analysed.

Out of these 5 events, one only can be considered relevant for the Fukushima Daiichi NPP accident: it is the event which occurred at Vandellos-1 in 1989 (fire followed by a significant flooding and challenges to the core cooling) [10-11].

1. Two event reports combine the codes of "loss of off-site power" and "loss of on-site power": one is an US NRC information notice (IRS 1465) and does not correspond to a specific event and the other one is IRS 7158 (Bruce-4, Canada, 19 December 1997) where in fact the loss of on-site power was partial.

To cover as much as possible the Fukushima scenario, it was also decided to extend the search regardless of the events causes in order to identify the events with as many characteristics of the Fukushima Daiichi NPP accident as possible. This search revealed that 4 IRS report cumulate 4 of the 5 codes corresponding to the characteristics of the Fukushima Daiichi NPP accident (7.7, 7.8, 7.9, 7.10 and 7.12).

These 4 event reports were analysed: one reflects a NUREG report and does not concern a specific event. All three other events (Vogtle-1 in 1990 [12], Kola-1 in 1993 [13] and Narora-1 in 1993 [14-15]) relate to Station Black-Out which lasted from 36 minutes for Vogtle-1 and about 35 minutes for Kola-1 until 17 hours for Narora-1. The first SBO was caused by a truck demolishing the transformer in use, combined with EDG failure, the second by a tornado damaging the off-site grid combined with EDG failure and the last one by a fire destroying the electrical cables of all power supply (including uninterruptible AC and DC suppliers).

The Narora-1 is also remarkable by the evacuation of the control room and by the loss of indication in the emergency control room due to the loss of control power supply. This event is analysed further on in this report.

A specific event occurred at the Swedish NPP Forsmark-1 in 2006. This event highlighted the vulnerability of the secured AC/DC power supply in case of a transient at the high voltage system or at the grid. The control room was partially lost during the event. It caused important international work resulting in a comprehensive report [16] that summarizes important lessons learned regarding – amongst others – the robustness of the electrical system. One major link to the Fukushima event is the troubleshooting action of the personnel to control the event.

Finally, as no events analysed in the previous steps could show similarities with the last sequence of the Fukushima Daiichi NPP accident, i.e. hydrogen explosion following Zircon-Oxygen reaction, the search was extended to all IRS reports with the code 7.12 “Physical hazards (internal or external to the plant)” and containing the word “explosion”, which yielded 23 event reports.

Eight of these events are related to explosions at the turbo-generators (hydrogen explosion or oil ignition), three of them concern transformers and the other events relate to hydrogen piping, gas storage, explosions at switchboards, etc. No event report concerns hydrogen explosion following interaction Zirconium/Oxygen but one concerns a gas explosion due to hydrogen production by water radiolysis, which seems the most similar to the Fukushima Daiichi NPP accident. This event occurred at Brunsbüttel in 2001 (IRS 7659) [17].

In summary, further investigation of the events reported to the IRS led to the selection of 5 events that will be described in more detail in the report:

- Vandellos-1, Spain, 19 October 1989 (massive internal flooding and loss of safety systems) [10-11].
- Narora-1, India, 31 March 1993 (among else loss of control room, loss of residual heat removal) [14-15].
- Blayais-1, France, 27 December 1999 (external flooding, loss of safety systems, multi units issue) [8-9].
- Forsmark-1, Sweden, 25 July 2006 (partial loss of vital DC power) [16,18].
- Brunsbüttel, Germany, 14 December 2001 (hydrogen explosion) [17].

It has to be taken into account that there may be more safety significant events recorded in the IRS database. The selection is therefore not intended to be complete. Nevertheless, the selected events are good examples to underline the findings described in the summary.

3.2.1 Vandellos-1

Vandellos-1 was a Gas Cooled Reactor (GCR) of 480 MWel and was taken into service in 1972. The plant was finally shut-down after the event. The description of the event is based on the IRS report [10] and the ASSET mission report [11]. Please refer to these reports for more details.

The core is fuelled with natural uranium, moderated by graphite and cooled with CO_2 by four gas circulators (TS). The CO_2 is cooled in the main heat exchanger, which is divided into four independent circuits (quarters). Each quarter feeds steam to the auxiliary turbine of each circulator and every two quarters feed also the turbine of a main turbogroup. Additionally there is a shutdown heat exchanger (RAiE) to remove residual heat in shutdown operations. Each circulator has its own condenser and two emergency feedwater pumps of a 100% capacity.

At 21:39 on 19 October 1989, vibrations on one of the two turbine generators led to an automatic trip of the No. 2 turbine generator. Shortly afterwards a flash was seen in the area of the turbine generator. The shift supervisor manually tripped the reactor. A fire was observed in the high pressure turbine housing and in the generator vent in the exciter side.

The fire was located in the high pressure turbine area and the lower level of the turbine building, affecting seriously the following equipment:

- Turbine generator group No. 2 and auxiliary equipment, main condenser, control valves and electric wiring.
- One of the two trains of the plant cooling circuit (component cooling water system).

The fire destroyed electrical cables, mainly on the levels +9.0 and +3.3. On level +3.3 electrical cables supporting the main auxiliaries of the gas circulators 3 and 4 and the shutdown heat exchanger are arranged. The damage of these cables caused the unavailability of the gas circulators 3 and 4 as well as of the shutdown heat exchanger. Because of the spatial separation of the electrical cables supporting the main auxiliaries of the gas circulators 1 and 2 these components remained available.

Due to the loss of 48 V control busses the necessary transfer from main feedwater to auxiliary feedwater was performed manually, as it could not be done from control room. Through these actions the gas circulators 1 and 2 were able to maintain core cooling. Thus, the core cooling was never completely lost.

The damage of electrical cables caused also the stopping of two of four compressors generating compressed air for the control air system. The drop of the pressure in the instrument air system was accelerated by damages on the system. To avoid the trip of auxiliary group and steam supply of the remaining gas circulators 1 and 2 several manually actions were necessary to maintain a minimum level of pressure. These actions included the closure of valves of the compressed air supply of non-safety relevant components. So 2 of 4 gas circulators were still available and core cooling could be maintained.

Furthermore due to the damage of the instrument air system the controlling of the level in the circulating condensers and the auxiliary feedwater tank caused difficulties. Too low water level caused a continuous on and off switching of the feed water pumps, which led to an insufficient heat removal with an increase of CO_2-pressure. Manual control was started and maintained for 15 hours. In addition the CO_2-amount was controlled manually, too, to avoid actuating the safety valves and the rupture of the rupture disk. The manual controlling was necessary until the instrument air system was full available.

The partial loss of the instrument air system caused anomalies in the automatic feeding of the steam generator and in the component cooling system. To restart the failed steam/water system of the gas circulators 3 and 4 as well as of the two failed air compressors several manual actions were taken.

The reactor building was flooded due to several reasons. The first one was the damage of the condenser cooling system of turbine generator 2. The outlet of seawater was interrupted when due to loss of voltage the cooling water pumps stopped. In addition to the seawater there was also a release of demineralized water. Some valves opened or remained open wrongly because of control failures due to the loss of instrument air and 48 V control busses. These valves were closed manually.

The Vandellos-1 event is an example of (internal) flooding that caused the loss of major safety systems. The reactor survived, because a part of the operational systems remained in service. The main effective barrier was the separation between operational systems and safety systems. The event was classified as Level 3 in the INES scale.

3.2.2 Narora-1

The unit 1 of the Narora Atomic Power Station started commercial operation in 1991. It is PHWR design with 202 MWel. The description is based on the IRS report [14] and a dedicated presentation to WGOE [15].

At 03.31 hours in the morning, a fire incident occurred in the Turbine Building, accompanied by a hydrogen explosion. After the turbine trip and the activation of several alarms due to the fire the reactor was tripped manually. The cool down of the Primary Heat Transporting System was initiated, but on observing the gravity severity of the situation, crash cool down was also started by opening large Atmospheric Steam Discharge Valves. Secondary Shutdown System got actuated.

At Narora-1 there was a complete loss of power supply, including class I (suppliers with uninterruptable direct current to the essential auxiliaries) and class II (suppliers with uninterruptable alternating current to the essential auxiliaries) suppliers. There was then an extended station blackout (SBO) which lasted for about 17 hours. The incident was a “Beyond Design Basis Accident”, as SBO including class I and II failure was not considered during the design stage. Due to the ineffective fire barriers fire spread rapidly and finally a large amount of smoke ingressed into the control room, so the staff had to leave. It was not possible to take charge of the situation from the emergency control room, as by reason of the loss of control power supply no indications on Narora-1 panel were available. Important parameters had to be directly measured from field. This resulted in the blind operation of the plant.

Firefighting was started by using two diesel engine driven fire water pumps.

To establish the heat sink diesel driven fire water pumps were started to feed the secondary side of the steam generator. Therefore it was necessary to open valves on the fire water back up circuit to the steam generator and to enter the primary containment. This was only possible because, as shown by the radiation surveys carried out, that inside the primary and secondary containment radiation values inside the primary and secondary containment were normal. Before taking these actions the inventory of the steam generator provided the heat sink.

To ensure subcriticality boron poison was added manually through the Gravity Addition of Boron (GRAB) system. The GRAB system has been specially engineered to face a SBO situation.

Due to these measures the reactor could be maintained in safe shutdown condition. The major fire was put out after 1 hour and 30 minutes.

During the incident, station diesel generators of Narora-1 started, but tripped automatically due to the loss of control power. The third diesel generator (EDG-3) could be started with control power drawn from Unit 2 and after 6 hours one of the class III buses (they supply alternating current to essential equipment required for an orderly safe shutdown of the reactor) could be charged. Essential equipment was started in a planned manner. One of the shutdown cooling pumps was started after 17 hours. Core cooling was maintained during this time by natural circulation (thermo-siphoning effect), the heat being released in the atmosphere through the Atmospheric Steam Discharge Valves, and the steam generators being fed by the diesel-powered fire water pumps.

The Narora-1 event represents loss of several safety systems and operational systems due to an internal hazard (internal fire). The main systems lost were the AC and DC buses, the control room and the emergency control room. The effective barriers were the successful emergency actions by the personnel, several passive design features (including the low thermal power) and a third EDG placed sufficiently physically separated from the plant. The event was classified as Level 3 in the INES scale.

3.2.3 Blayais

The Blayais site consists of 4 standard 900-MWel PWRs of French design. Blayais-1, the most affected plant, was put into commercial operation in 1981. The description of the event and its consequences follows the IRS report [4] and the generic IRS report on flooding events [9].

On 27 December 1999 at 19:30, due to a storm, the auxiliary power supply (225 kV) of all 4 units was lost as well as off-site power (400 kV) of Units 2 and 4. These two units failed to be powered in island mode, which led to the reactors automatic shutdown and to the EDG automatic start-up. The EDGs supplied power until off-site power was retrieved about 3 hours later. Off-site power of Units 3 and 4 remained available during the event.

During the night of 27-28 December 1999, these exceptionally bad weather conditions combined with inadequate protection measures against external flooding caused by swell, resulted in the flooding of rooms of the power plant nuclear islands and safety related systems. The severe weather also led to disturbances on the electrical network: the 225 kV auxiliary electrical power supply of all four units was lost for about 24 hours and the 400 kV main electrical power supply of Units 2 and 4 was also lost for several hours.

The water infiltrated into the duct cover slabs located in the North part of the nuclear power plant, flooding the sub-levels of the administrative buildings and common auxiliaries building. Then, the water propagated into the rooms of Units 1 and 2 through doors and openings, reaching the sub-levels of the electrical buildings, the connection galleries of the water pumping station, the sub-levels of the peripheral and fuel buildings. This flooding mainly led to the loss of the following systems:

- In Unit 1, the train A of ESW (essential service water system).
- In each of Units 1 and 2, both trains of the low-pressure injection systems and containment spray into the containment.

As a result of this flooding, Units 1 and 2 were brought to shutdown state with the steam generators used for cooling the primary coolant and ready for connection to the reactor heat removal (RHR) system. Meanwhile, Unit 4 was shut down and then brought to hot shutdown state (Unit 3 was already shut down for maintenance and was kept to normal cold shutdown state with the shutdown RHR used for cooling during the event).

Once Units 1 and 2 reached the targeted state (steam generators used for cooling the primary coolant and ready for connection to RHR), the first concern was to ensure the long-term operation of the auxiliary feedwater (AFW) system of each unit. This was achieved by permanently restoring the reserves of water contained in the tanks of these systems from the site demineralized water supplies and operation of the demineralisation station. Units 1 and 2 were kept shut down and cooled by the steam generators, until it was established that the national power grid had stabilized, that all the electrical systems (external power supplies and electrical switchboards) as well as the entire Essential Service Water system of the plant were available, and that one of the trains of both the safety injection and containment spray systems (whose pumps had been immersed in the flooding) was requalified.

It has to be noted that, during the first hours of the incident, the arrival of the additional teams from outside the nuclear power plant was impossible owing to the damage resulting from the storm (flooding of the access routes, many tree falls…).

The French NPPs' design principles regarding flooding risk and protection methodology were reviewed and applied to each French NPP. This new methodology was aimed at taking all measures required to protect NPPs against the risk of external flooding; particularly, those to cope with the NPPs' isolation caused by external flooding were thoroughly analysed [9].

The event in Blayais was caused by an external flooding of the whole site. Due to some damages and the location of the low pressure injection system and the containment spray system adjacent to each other at the basement of the reactor building, these safety systems were completely lost for two units. The reactors remained in stable conditions because the criticality control was not affected and the residual heat removal via the steam generators were operating as designed. There was during the entire sequence no challenge for the safety systems lost. The effective barrier was thus the continued operation of the RHR as designed. The event is nevertheless an example of several units affected at the same time by one external hazard. It was classified as Level 2 in the INES scale.

3.2.4 Forsmark-1

At the Forsmark site, three reactors are operating. Forsmark-1 is a 984 MWel BWR of ABBATOM. It went into commercial operation on 1980. The description is based on the IRS report [18] and the report of the international DIDELSYS task group [16] of CSNI that was established in the aftermath of this event.

Forsmark 1 was on 25 July 2006 in full power operation when a disturbance occurred in the offsite 400 kV switchyard during maintenance work causing the reactor trip. The event caused two transients on the power supply to the unit. The first one was an over voltage transient that led to the trip of rectifiers and inverters belonging to two UPS units in the battery backed-up 500 V and 220 V AC grids, subdivisions A and B (although it was a common cause failure, related to a wrong selectivity of component protections, subdivisions C and D were not affected). The 220 V AC is necessary for the operation of the emergency diesel generators (EDG). The second one was a low frequency transient which made the safety related bus bars disconnect from the offsite power line; the under frequency protection of the generators' breakers did not work as expected due to a faulty phase coupling in this protection.

The transient resulted in an automatic reactor power reduction, through a partial reactor scram, and reduction of the speed of the primary circulation pumps. The unit went shortly into house load operation before signals for reactor scram, isolation of the primary containment, and start-up of the reactor safety systems were received.

All four emergency diesel generators (EDG) started automatically, but EDG A and EDG B did not connect to their respective bus bar due to loss of power in the same divisions of the battery backed-up 220 V AC grid (this grid feeds EDGs' rotational speed protection).

In this situation two out of four trains in each safety system were operating (auxiliary feed water system, core spray system and containment spray system). However, the loss of the two 220 V AC bus bars caused however several isolation signals and loss of information in the control room. After 22 minutes, the operators reconnected offsite power to subdivisions A and B thus all power was available at the unit. After 45 minutes since the beginning of the event, the operators could confirm that the unit was in a safe and stable shutdown mode.

In the unit safety analysis report (SAR), the event “Loss of external power” is analysed, together with a postulated coincident loss of power in one safety system subdivision. The actual event sequence represents thus a more serious event than analysed in SAR.

The Forsmark-1 event is characterized by the propagation of failures in the electrical systems from the external grid to the uninterruptible DC power supply. In that sequence the power to the control room was partly lost and the control of the event was thus very complicated – as during the Fukushima Daiichi NPP accident. The effective barrier was the quick manual troubleshooting actions – that were not described in the SAR – to re-establish the emergency power based on the competence of the personnel. The event was classified as Level 2 in the INES scale.

3.2.5 Brunsbüttel

Brunsbüttel is a KWU type BWR (so called SWR-69) of 771 MWel. It went into commercial operation in 1977. The description is based on the IRS report [17].

On 14 December 2001, a steam leakage inside the containment at the reactor pressure vessel head spray (RPVHS) line occurred at Brunsbüttel NPP during full power operation. The leakage could be manually terminated in about 4 minutes in the event by closing a valve in the drain line of the RPVHS line. Later investigations revealed that a section of about 2.7 m of the RPVHS line was completely destroyed. The cause of the rupture was a radiolysis gases explosion inside the piping. The radiolysis gases could accumulate due to insufficient drainage of the RPVHS line. The event had no direct consequences, but the potential safety significance of such a radiolysis gases explosion may be high.

Immediately after the event, the shift personnel reduced the reactor power down to 60% (minimum speed of the recirculation pumps). After the first analyses, control room staff assumed that only a small leakage at a flange in the RPVHS line had occurred. At the time of the event there was no in-situ inspection of the affected location because the operating staff decided not to go into the containment (the radiation level at the location of the leakage was high); it took more than two months to decide reducing power in order to carry out an in-situ inspection. The visual inspection revealed several damages on the RPVHS line, even a piping part of about 2.7 m length was missing and the debris parts of the destroyed section of the RPVHS line impacted on the rector pressure vessel thermal insulation, on cable trays, on a ventilation duct and a steel beam.

Regarding accumulation of radiolysis gases, the licensee concluded from the data available that due to inner leakages of the RPVHS containment isolation valves relatively cold water from the reactor water purification system reached the lower part of the RPVHS line. The drainage of this water was disturbed, because the valve in the drain line connected to the lower part of the RPVHS line was only 1/3 open. Thus a layer of sub-cooled water could form in the lower horizontal part of the piping. Because of this layer of relatively cold water the condensation rate of the main steam entering the RPVHS line via the drain line increased. Calculations performed revealed that due to the increased condensation rate about 7 times more radiolysis gases were generated than originally expected.

The Brunsbüttel event as mainly two aspects: the technical aspect comprises the potential effect that such a radiolysis gas explosion could damage the primary circuit and the containment simultaneously. Thus the risk for a release outside the containment cannot be fully excluded (for a higher volume of radiolysis gas). The organisational aspects are twofold, the pipeline was not taken into account to install hydrogen combiners and the plant was not shut down after explosion occurred. These aspects shall not be analysed here. The effective barriers in the Brunsbüttel were the physical strength of the containment and the leak tightness of a check valve at the RPV upper head. Both barriers are passive barriers.

3.3 Evaluation of the effective barriers

The consequences of the five events selected are much lower than these from the Fukushima Daiichi NPP accident. This is due to the fact that the event sequences could be stopped at points of time before the core cooling was endangered. The differences of the selected events refer to variety of these barriers that have remained effective.

The analysis of the effective barriers shows different barriers for the events described:

- Vandellos-1:
  The core cooling was never lost completely. Electrical power was available on the site during the entire event sequence. Thus also operational systems could be operated or remained in operation. The main effective barrier was the separation between systems.
- Narora-1:
  The electrical power supply was completely lost. The residual heat removal by forced circulation was ensured only by the water inventory of the steam generators for about 5 hours until the diesel-driven fire water pumps fed them. Reactor cooling was maintained by a combination of natural circulation (thermosyphoning), addition of fire water to the secondary side of the boilers, and opening of atmospheric steam release valve(s). Planned emergency measures were successful including manual actions inside the reactor building. Other effective barriers were some passive design features to extend the time for manual actions and to control criticality.
- Blayais-1/2:
  The core cooling was never lost. Heat removal could be ensured by steam dump to the atmosphere over a rather long time. The event sequence could be stopped before the demineralized water source had been exhausted. Electrical power (at least emergency power) was available during the entire event sequence. The main effective barrier was the separation between systems.
- Forsmark-1:
  The event was restricted by chance only to two out of four redundancies. Thus electrical power was never completely lost. The event sequence could be stopped - even under unfortunate conditions – by unplanned human actions. The heat removal was not lost completely. The main effective barrier was manual action.
- Brunsbüttel:
  The event did not affect plant operation directly, the plant remained in power operation. The effective barriers were the physical strength of a check valve and the containment vessel head; they stayed undamaged despite the explosion. Thus the barriers were passive barriers.

Table 3. **Main features of the five events selected**

NPP	**Loss Off-site Power**	**Loss DC Power**	**Loss Heat Removal**	**Loss Criticality Control**
Vandellós-1	No	Partial	Partial	No
Narora-1	Yes	Yes	Short Loss	No
Blayais 1/2	Partial	No	Partial	No
Forsmark-1	Partial	Partial	Partial	No
Brunsbüttel	No	No	No	No

3.4 Analysis of selected IRS reports

The sequences of the five events were stopped, before a core melt started. During the entire event sequences the fuel elements in the cores (and also in the spent fool pools) were sufficiently cooled.

But, based on the safety relevance of the events selected, a significant number of generic lessons learned have been derived. In the following the main generic lessons from these IRS reports are discussed. They form the basis for the following analysis.

3.4.1 Vandellós-1

The main damages to safety systems were caused by fire and flooding. The root causes were deficiencies in physical separation of redundancies, buildings and fire zones, respectively. The flooding of the reactor building via the turbine hall caused the loss of several safety systems. The spread of the fire affected various cable trays and thus the 48-V-DC power supply.

The Vandellós event can be divided into the following sequences:

A. Loss of control air due to fire
   - Main consequence: Inoperability of the AFW system (Regulating valves failing in positions that blocked or diverted the AFW flow).
   - Root cause: Design review oversight (the initial design review did not include analysis of the effect of loss of control air to the AFW valves).

B. Loss of electrical power supply due to fire
   - Main consequence: Loss of 2/4 turbo blowers, loss of 4/4 shutdown cooling pumps and loss of 2/4 AFW trains.
   - Root cause: Lack of implementation of modifications (cable segregation, effective protection against fire in the cable route) suggested in a re-evaluation program required by the CSN, and lack of any interim measures in the meantime.

C. Inoperability of 4 shutdown cooling exchanger pumps due to flooding
   - Main consequence: Inoperability of shutdown heat removal.
   - Root cause: Protection of safety-related systems in the reactor building against flooding from outside neglected during installation, and also after a later safety re-evaluation concluding lack of tightness in the reactor building (no interim/short-term measures were taken prior to implementing final modifications).

D. Breaking of turbine blades due to high local stress concentration and corrosion
   - Main consequence: Vibrations that caused the breakage of 4 oil pipes.
   - Root cause: NPP surveillance program unable to detect corrosion (surface tests but not volumetric ones). Design and manufacturing did not take into account possible high local stress concentration and likely corrosion due to humid and high temperature steam.

The event triggered the final shutdown of the plant. Thus the generic lessons learned discussed below were not implemented at the reactor. Nevertheless, the implementation of the lessons learned, which are a selection taken from the IRS report [10] and the ASSET report [11], could help to avoid events at other NPPs or at least reduce their potential consequences.

These lessons learned are:

- The electrical power system supplying electrically operated actuators of the safety system should include full physical separation between trains.
- Layout of power cables and protection against common mode failure such as fire or flooding should be reviewed carefully. If it is not possible to achieve this on older established plants, additional defences should be supplied. Alternatives to consider are addition of fire retardant materials around cables, additional fire detection and suppression systems, additional physical barriers between components, and compartments to contain spillages.

- In addition to the systems used to ensure operability of safety systems at all time (reliable and redundant components), provisions should be made to ensure that they will never be made inoperable by any internal aggressive element, whether gas, liquid or solid (water flooding, floating oil fire, chemical product corrosion, steam, etc.). Preventive measures should take into consideration all the possible events.
- The air system supplying instruments and air operated actuators of the safety systems should be separated from any other air supply.

The safety air supply system should include the necessary provisions to ensure permanent operability at all times, redundancy of components, physical separation, backup systems such as accumulators to enable normal operation of actuators in case of short time loss of air. In the case of total failure the air operated actuators should move to the safest position which may be open or closed.

When safety related systems are actuated by electrical or hydraulic means, the similar rules should be applied to those systems to ensure that failures model are considered and whenever practicable a fail-safe philosophy is adopted.

- The surveillance programme of each plant should be completed with a careful review of all safety systems, especially for old plants. Trending of the early signals for identification of potential safety issues and systematic root cause analysis of all issues, even the most benign, should be part of the activity of surveillance at nuclear power plants to ensure effective prevention of incidents.
- Regulatory bodies should consider their role as essential to achieve an adequate balance between the degree of fulfilment of the required investigations and the time frame for the implementation of necessary hardware and software modifications once they have been determined. Sometimes an alternative interim solution in terms of simple changes could reduce the possibility of occurrence of events or event effects.
- Progress should be made in the application of the re-evaluation of safety to re-examine the application in the plant design of the defence in depth criteria, redundancies, physical and functional separations and defence against common mode failures. The analysis of the new codes and regulations should be concentrated more on the basic reasons that have made them necessary rather than in their formal aspects, which could result in difficult application or direct translation to the older stations or to those stations of different technology.

The adequacy and vulnerability protection of the means of communication when faced with potential incidents and accidents should be verified.

- The training of the teams responsible for measures of emergency and the teams of intervention should be increased, especially for those responsible for fire fighting. The emergency organisation plans should be revised to ensure that they are adapted to the situations that could occur during the potential incidents and accidents, their possibility of derivation to incidents of important proportions and effects that could contribute to a situation of uncontrolled fire.
- The incident has confirmed that the existence of an Emergency Room independent from the control room, where an emergency group could assemble, would have facilitated the job of organisation.

3.4.2 Narora-1

The Narora-1 event demonstrated the robustness of PHWR design that survived a complete loss of power supply for a period of 17 hours without any radiological impact either on the plant workers or in the public domain. Core cooling was maintained by thermo-syphoning on primary side and rejecting heat into atmosphere through Atmospheric Discharge Valves on secondary side. Nevertheless, the operator and the licensing authority draw several generic lessons to prevent recurrence of such an event.

After the event, the following measures were taken:

- Several turbine generator systems related improvements were established.
- Emergency Operating Procedure/Guidelines and provisions for handling Station Black Out (SBO) were improved. The existing guidelines and procedures were reviewed and revised in the light of the incident. Capability to handle extended station blackout conditions (with Class I&II also not available) was reviewed along with the duration of the station blackout.
- Manual valves required for feeding firewater to steam generators during SBO were relocated to a more convenient/accessible location. The reliability and capability of fire water system to inject water to the steam generators, as well as fight fire simultaneously, was established by tests.
- Facility for injecting firewater to end-shields has been incorporated as a part of design.
- The regulatory body expressed that there was a need to strengthen quality assurance at all stages (design, commissioning, operating).

The following lessons learned were also raised:

- In-depth review of physical separation and fire protection provisions for power & control cables should be carried out to guard against common mode failure such as fire.
- Control room habitability should be ensured under adverse outside conditions.
- Detailed design safety review of systems outside nuclear steam supply system with potential of affection reactor safety should be carried out.

3.4.3 Blayais

Severe weather conditions caused a flooding of the reactor building basement and thus the simultaneous failure of major safety systems. Due to the availability of electrical power (either from the grid or from EDGs) the plants could be shut down and cooled via operational systems. Nevertheless, the event showed that events affecting more than one unit on a site could result in additional difficulties as some auxiliary systems are common to all units on the site

It has revealed also some weaknesses in the site protection against external flooding related to:

- The extreme meteorological conditions considered in the design of the site protection. For the Le Blayais' site, high storm-driven waves coincident with high water level in the Gironde estuary had not been initially considered.
- The warning system and its criteria, allowing the anticipation of severe weather (verification of the protection devices, implementation of movable equipment…) and the shutdown of the plants in a timely schedule.
- The site accessibility (blocked roadways), highlighting both the need for additional staff of operating and emergency response personnel prior to the arrival of the severe flooding conditions and the need for an adequate self-sufficiency of the site (water quality and fuel supply…).
- The flooding-related procedures and the on-site emergency organisation, considering all the diverse aspects linked to the flooding conditions including:
  - The accessibility of the equipment located outside of the protected buildings.
  - The simultaneous impact on several plants, with a potential risk of losing both the external power supplies and the ultimate heat sink.
  - The isolation of the site and the difficulties to provide rescue staff and equipment.
- The detection of water in the flooded rooms, allowing a quick response of the operating staff for implementing the necessary action, like the implementation of movable pumping devices.
- The faults in electrical isolation, likely to lead to some electrical busbars loss whereas the external grid may be lost due to the severe weather conditions.
- The management of release of the water collected in the flooded facilities.

- The penetrations and the doors which were built under the platform level and at the periphery of buildings containing safety-classified equipment to ensure reactor shutdown, have to be watertight and sized to resist to water height induced by the external flooding of reference.

After the event, the general approach to re-examine the NPP design possibilities was re-examined depends based on a safety re-examination assessment related to an exceptional event. This approach consisted in identifying and quantifying methodically all the events and combination of events likely to generate an external flooding of a power plant. The phenomena retained were classified into two categories:

- Those determined as per the applicable rules (fluvial, maritime or estuary flood, dam failure…).
- Those examined using an additional approach (swell, splashing, thundery or continuous downpours, circuit or engineering failure, intumescence, raise of table water).

With respect to those events and combinations of events, the adequacy of the existing material and/or organisational protection measures was checked so as to define the modifications which would be required. The measures to take in order to cope with the power plant isolation were particularly studied. This new methodology was applied to each of the 19 French nuclear power plants, and aimed at taking all measures required to protect all nuclear power plants against the risk of external flooding [9].

3.4.4 Forsmark-1

The NEA Committee on the Safety of Nuclear Installations (CSNI) authorised formation of a task group in January 2008 to examine Defence in Depth of Electrical Systems and Grid Interaction with nuclear power plants (DIDELSYS) [16]. The task was triggered by the July 2006 Forsmark-1 event. The investigations therefore went much more in-depth especially for generic lessons learned than usual.

This event identified a number of design deficiencies related to electrical power supply to systems and components important to safety in nuclear power plants. While plant-specific design features at Forsmark-1 contributed to the severity of the sequence of events which occurred during the event, a number of these design issues are of a generic nature as they relate to commonly used approaches, assumptions, and design standards for voltage protection of safety related equipment.

Recent international operating experience has indicated that generally accepted design practices and standards which have been relied upon for decades to assure defence in depth have not kept pace with on-going changes in technology and in changes in the organisation of electrical suppliers. These on-going changes, if not commensurately addressed by improved practices and design standards could eventually result in events with serious nuclear safety implications.

Examples of major technology changes include: replacements of robust, but maintenance intensive, motor-generator sets with less robust solid state UPS units for supplying vital control and instrument power, and replacement of older hardwired relay-based control and protection devices with microprocessor-based devices which can be more sensitive to degraded input power supplies.

Examples of changes in the organisation of electrical suppliers include the reorganisation of electrical industries into separate generating companies, transmission system operators, and local electrical distribution companies who may have competing market interests on where power is needed.

The DiDElSys report concluded regarding the current LWRs that their safety relies on the availability of preferred power sources for operation of emergency core cooling and decay heat removal systems. The defence in depth of nuclear power plant electrical systems can be viewed as a combination of the following design and operational practices:

- Preventing electrical grid and plant generated electrical faults which are capable of interrupting the preferred source of power to decay heat removal systems.

- Robustness of nuclear power plant electric power systems to cope with electrical grid and internal plant generated electrical faults without further fault propagation or degradations to safety related equipment.
- Continuously improving nuclear power plant and external transmission system operator training, procedures, and information capabilities to deal with possible degraded electrical systems.
- Coping capability of nuclear power plants to deal with severe electrical grid and internal plant generated electrical faults.
- Ability to recover offsite electric power by co-ordinated actions of the nuclear power plant and transmission system operator.

The DiDElSys group observed that practices implemented in one country to address their specific operating experience were not necessarily being communicated or adopted in counterpart organisations in other countries, or to international design standards bodies such as IEEE or IEC. The DiDElSys group did make substantive observations where specific practices had "gaps" and where design standards need to be upgraded. These can be summarised as follows. Please refer for further details to [16].

- Recommendations related to preventing electrical grid and plant generated electrical faults.
- Recommendations related to robustness of nuclear power plant electric power systems The DIDELSYS Task Group review found that many critical nuclear power plant safety systems are directly connected to the preferred power source (offsite power transmitted to plant safety systems via a transformer connection). A large rapid surge can propagate to these systems in some cases faster than alarms or active protective devices can respond. This presents the possibility for a common cause failure such as has been observed in the 2006 Forsmark event.
- Recommendations related to improving training, procedures, and information capabilities.
- Recommendations related to coping capability of nuclear power plants.
- Recommendations related to electrical system recovery.

3.4.5 Brunsbüttel

The hydrogen explosion in the Brunsbüttel event demonstrated the potential for a significant hydrogen accumulation in pipework close to the reactor pressure vessel. The rupture location was close to a check valve at the RPV head and the containment closure head. It cannot be excluded that the explosion could have resulted in a simultaneous loss of coolant from the RPV and damage to the containment at higher explosion pressures. Even if a core melt would have been prevented by the safety systems, the evaporation of primary circuit steam could have resulted in a release to the environment above the operating limits.

In addition, the NPP was not manually shutdown, because the measurements showed no significant change of the primary and containment conditions. The affected pipe was sufficiently isolated from both ends.

Several actions were taken and some generic lessons were drawn, mainly:

- to implement a permanent temperature monitoring program in order to prevent accumulation of radiolysis gases. Altogether about 200 temperature measurements were implemented at all piping where radiolysis accumulation cannot be excluded.

3.5 Lessons learned from the Precursor events

Edward D. Blandford and Michael M. May form the American Academy of Arts and Sciences have issued an interesting booklet on the "lessons learned from the lessons learned" with the subtitle "the Evolution of the Nuclear Power Safety after Accidents and Near-Accidents" [19]. The main results derived by the authors can be transferred to this study nearly one by one. Among their nine general observations one shall be quoted below as an example:

> *3. All three of the major nuclear power accidents [for explanation: TMI-2, Chernobyl-4 and Fukushima Daiichi NPP] as well as several of the lesser-known close calls had precursors in previous incidents, although often not at the same location or in the same country. The lessons learned reviews completed after the accidents have often contained specific useful points. Some of those points have been implemented —that is, the lessons were learned — but others have not been. Not surprisingly, implementation steps that translated into more efficient operations, such as better, more standardized operating procedures, were carried out more often than steps that required immediate expenditures to avoid uncertain disaster, such as better defenses against possible flooding. Further analysis may find other, less obvious correlations.*

The analysis of the initiating events at Fukushima was based on the guide words on event characteristics from the IRS database. The initiators were already frequently reported but most of them with significantly minor safety related importance. The Fukushima Daiichi NPP accident was initiated by a “once in a thousand years” external event which is comparable to the initiator frequency of the Blayais flooding [9]. Such initiator frequencies are in most cases within the design basis assumptions.

Precursors can give interesting insights of event sequences. The precursors selected for this study cover the range of the major initiators or major occurrences of the Fukushima Daiichi NPP accident. There are without any doubt significant differences between the precursors selected and the Fukushima Daiichi NPP accident, but nevertheless some of these precursors selected led to in-depth studies. Several generic lessons learned were derived in these studies. The importance of the separation between systems for the same function as well as the protection against hazards (here: flooding and fire) are highlighted in several studies. The need for adequate instrumentation for accident conditions was also mentioned several times. The shift staff and further personnel need this information as basis for their actions. In addition, emergency procedures and emergency rooms were mentioned as not fully adequate.

But which barriers prevented the selected precursors to develop to core melt accidents? All but one of the selected events did not experience a full loss of core cooling. In cases which experienced a station black-out, internal or external power supply could be established quite quickly. Thus, even if the defense-in-depth measures were not always completely successful, diverse means of e.g. heat removal remained available or could be established in a short time.

Another generic item was the availability of process information in such a situation. If the DC power is lost, the instrumentation and control of the NPP by the plant staff is extraordinarily difficult. Even the operating experience is available, uprates for emergency instrumentation for such accident situations (like completely independent and separated power supply) have not been backfitted widely. Only after the Fukushima Daiichi NPP accident did some regulatory bodies include requests for related backfitting measures in their lessons learned. This lesson is among the important lessons to be learned derived by the CNRA Senior-level Task Group on Impacts of the Fukushima Daiichi NPP accident [20].

The analysis of the events showed also that staff intervened sometimes in very challenging environmental conditions (smoke, obscurity…) but fortunately the staff was able to overcome these conditions and to complete locally the needed actions. Would have it been the case however in worse conditions (heat or radiation level)? This strengthens the findings mentioned above that local human actions should be accounted in the emergency procedures only as the last actions and that recovery actions should be ensured in first line by the remote instrumentation and control, which implies a very high level of robustness (qualification to environmental conditions, robust power supply, redundancy…).

As a summary it can be noted that the main initiators of the Fukushima Daiichi NPP accident have been experienced before in other NPPs. The in-depth investigations revealed a great number of generic lessons learned that – if implemented – could prevent accident sequences like those of the Fukushima Daiichi NPP accident, even if some of the lessons are difficult to implement in existing plants like the strict separation of redundancies, including electrical and I&C systems. The result of this investigation demonstrates the crucial importance of an efficient international operating experience feedback system.

It can be summarized that the international operating experience feedback system and WGOE produce sufficient lessons learned to prevent accidents. The challenge for each NPP and each regulatory body is the timely implementation of these lessons. The key point is correct priority setting for the implementation of the lessons learned.

4. OTHER PRECURSOR EVENTS WITH HIGH RISK

To complete this report, the WGOE asked the CSNI Working Group on Risk Assessment (WGRISK) for additional information on significant severe accident precursors. Representatives from WGOE participated in discussions at two WGRISK annual meetings in order to receive the most valuable input.

The WGOE request was to identify the most significant precursor events of the last 25 years. The idea was to evaluate whether other significant operational events that were not identified through a search and analysis of the IRS database could offer further insights relevant to the Fukushima Daiichi NPP accident. Further analysis was done to determine whether the implementation of the lessons learned from these additional events could have addressed potential vulnerabilities or otherwise mitigated the events associated with the Fukushima Daiichi NPP accident.

The WGRISK developed the following criteria to select risk-significant events for consideration by the WGOE:

1. The event was risk significant as defined by a PSA-based event analysis. Typical screening values for consideration are a change in core damage frequency (ΔCDF) of 10^{-4}/year or greater or conditional core damage probability (CCDP) of 10^{-4}. In cases where formal quantitative estimates of ΔCDF or CCDP are not available, a qualitative assessment of the risk significance may suffice.
2. The circumstances associated with the event remain as potentially risk significant issues today. In cases where implementation of effective corrective actions for the plant or plant-type affected by the event may have reduced the potential risk significance for specific plant(s), consideration should still be given to including an event if it may impact plants that have not implemented similar corrective actions. For example, while events such as the Blayais flooding event may no longer be risk significant for French nuclear plants, this type of event could remain risk significant for plants that have not yet implemented effective corrective actions. However, events where effective corrective actions have been widely implemented should not be included (for example, events such as the Salem anticipated transient without scram (ATWS) event in 1983 should be avoided since significant regulatory improvements and plant changes have been made as a result of the event).
3. The event occurred after 1990 (this date is intended to provide to provide sufficient time for the implementation of corrective actions arising from the Three Mile Island Accident and reflect more modern operational standards and maintenance practices).
4. The event meets either of the following additional criteria:
   - The event's key features bear a reasonable similarity with those observed during the Fukushima Daiichi NPP accident (e.g., involves external flooding or a seismic event, long term station blackout, loss or significant challenge to dc control power, loss or significant challenge to the ultimate heat sink)

   or
   - The event involved key contributing factors observed during the Fukushima Daiichi NPP accident. These include but are not necessarily limited to:
      i. Significant human or organisational factors.
      ii. Adequacy of engineering assessments.
      iii. Timeliness in addressing known hazards.
      iv. Severe accident management issues.

Using the above criteria, the WGRISK identified the following events for the WGOE consideration.

Plant(s)	CCDP or ΔCDF	Date	Description	Comments
Davis-Besse (US)	6×10^{-3}/year (ΔCDF)	2/27/02	Concurrent, multiple degraded conditions, including cracking of control rod drive mechanism (CRDM) nozzles and reactor pressure vessel (RPV) head degradation; potential clogging of the emergency sump; and potential degradation of the high-pressure injection (HPI) pumps. (LER 346/02-002)	Risk significant event that involves failures to conduct timely and adequate evaluations of known degraded conditions
North Anna 1 (US)	2×10^{-4} (CCDP)	8/23/11	Dual unit loss of offsite power caused by earthquake that coincided with the Unit 1 turbine-driven auxiliary feedwater (AFW) pump being out-of-service because of testing and the subsequent failure of a Unit 2 EDG. (LER 338/11-003)	Risk significant event that involves a seismic event greater than assumed in the design basis
Barsebäck 2 (Sweden)	–	7/28/92	The strainer blockage incident (IRS-1294). The incident in Barsebäck 2 on 28 July 1992 indicated that the operation of the emergency core cooling and containment spray systems in the event of a pipe rupture could be jeopardized due to clogging of the inlet strainers for the emergency core cooling water by mineral wool insulation which had been flushed down, and that clogging could occur considerably faster than had been assumed in the safety assessments which formed the basis of the operating licenses.	Risk significant event involving potential loss of cooling due to clogging of strainers.
All units in Sweden affected	–	12/27/83	LOOP event (IRS 401) On 27 December 1983, a power grid failure occurred encompassing the southern half of the national Swedish power grid. The IRS Report 401 gives detailed information about the behaviour of the Swedish plants.	Risk significant event involving long term loss of offsite power for many Swedish plants. Note that a similar widespread grid-related loss of offsite power (LOOP) occurred in the United States on 14 August 2003 which resulted in LOOPs at nine commercial nuclear power plants (see US NRC NUREG/CR-6890).
Cruas Unit 4		12/01/09	Total loss of heat sink, further to the clogging of the trash racks by a massive arrival of vegetable matter (IRS 8068) During the night of 1 December 2009, a massive amount of vegetable matter (around 50 m^3 compared with a monthly average of 5 m^3) blocked the water intake of the common pumping station of Cruas NPP units 3 and 4, by clogging the pre-filtration trash racks. The total loss of heat sink of unit 4 lasted 10 hours.	Other plant units were also impacted by the clogging of the trash racks: plant units 2 and 3 partially lost their heat sink.

It is also worth pointing several factors that WGRISK considered when responding to this request:

- It is extremely difficult to answer the question "What is the next Fukushima". PSA techniques can provide valuable insights into risk-significant accident contributors, but cannot be used to predict when or where a future accident will occur. A better question would be what are the major risk insights currently available from PSA studies (rather than focusing on past events), but even this question is very broad and depends heavily on design and site-specific factors. Even in countries where standardized plant designs are employed, site specific factors such as electrical distribution, ultimate heat sink configuration, and the external hazard profile (winds, seismic, flooding, etc.), impact the risk profile. These factors make generalization of risk insights challenging.
- Precursor events are defined in terms of a specific end state of interest. Typically, PSA analysts consider precursors events to core damage. The WGOE request focused on precursors for an event similar in nature to the Fukushima Daiichi NPP accident. The PSA techniques for identifying core damage precursors are well defined and implemented by numerous countries. The question of identifying a precursor to a specific event type (such as Fukushima Daiichi NPP) is more difficult in that it involves not only addressing initiating events, but also the considering the specific details of the accident sequence of interest (and even then, one could question how predictive this is of a future event). WGRISK tried to strike a balance with the above criteria.
- It is important to note that most, if not all, NEA members represented by WGRISK have active precursor and operating experience programs. It is important that the discussion of accident precursors presents a balanced picture in that there are many successes that can be identified where members have utilized operating experience and precursor information to make effective changes to plants to reduce risk. There is always more that could be done, but existence of a specific operating event does not provide the whole story, we must also consider what was ultimately done with that information and how it affected the overall risk profile.

These five events can be separated into two groups:

- Fukushima related events:
LOOP: all Swedish plants (IRS 401) [21]
Loss of ultimate heat sink: Cruas-4 (IRS 8068) [22]
Earthquake: North Anna-1 [23-24]
- Events indirectly related to Fukushima (from a technical point of view):
Primary leakage: Barsebäck-2 (IRS 1294) [25]
Potential for primary leakage: Davis Besse [26]

The effective barriers during the event sequences with Fukushima related initiators have been adequate back-up power sources after the LOOP (Swedish black-out, North Anna-1) respectively the heat removal capabilities by steam dump to the atmosphere with sufficient water to add to the secondary circuit.

The primary leakage at Barsebäck-2 occurred during start-up after refuelling outage and caused in itself no difficult situation (performance of planned procedures). At the Davis Besse event there was no direct impact on plant operation, since the condition was detected during outage. At the previous cycle no related problems had occurred. However, the Barsebäck event highlighted a condition where the design basis for the emergency core cooling system strainers was inadequate in that it did not account for additional debris generated as a result of a loss of coolant accident. For the Davis Besse precursor, the linkage to Fukushima Daiichi NPP involves missed opportunities to identify and resolve a significant degraded condition by the organisation over an extended period of time, which is analogous to the situation faced by TEPCO when faced with updated tsunami information. Therefore, both the Barsebäck and Davis Besse issues highlight key contributing factors that were similar to the Fukushima Daiichi NPP accident.

The evaluation of the event sequences reveals more interesting insights. These are mainly the reasons for the high risk perceptions related to the events.

The Swedish black-out event may represent the risk for multiple plants to be affected at the same time. Just by adding the additional risk value for all plants the overall risk for public can be explained. Other large area black-outs can be found in [27] and [28]. Similar findings have been drawn after generic findings at the French quite homogenous fleet of reactors, e. g. see IRS 8164 [29].

The loss-of-coolant event in Cruas [22] has the additional aspect that 3 out of 4 reactors at the site had been affected by the same problem. But, only at Cruas-4 both redundant cooling trains failed simultaneously. The IRS report [22] mentions also a precursor event from 2003 at the same plant that also deals with the complete loss of both essential service water trains. The problems had been addressed by the development of specific emergency procedures. These were effectively applied in both events.

The North Anna-1 and 2 [23-24] event is included in this subset of events because it serves as another example of NPP performance in response to an earthquake. During the earthquake, one-of-three auxiliary feed water (AFW) pumps at Unit 1 was temporarily unavailable because it was undergoing maintenance; however, this pump was restored within about 30 minutes of the earthquake. The AFW system is an engineered safeguards system that includes two motor-driven pumps and one turbine-driven pump; providing redundancy and diversity to ensure proper system response to demands. Additionally, one-of-two emergency diesel generators (EDG) at Unit 2 failed during the loss of offsite power (LOOP) following the earthquake. These issues presented minimal challenges to the plants' overall responses to the event in part because of redundancy and diversity inherent in safety systems. For example, the AFW pumps are powered from diverse sources, and a station blackout diesel generator was available to provide power to selected loads that had been lost as a result of the failed EDG. The North Anna site's response to the earthquake and ensuing LOOP is typical of what is expected from a Generation 2 PWR because of redundancy and diversity in safety systems. However, this event also highlights that there is a notable increase in risk associated with LOOP events that are coincident with failures of decay heat removal methods.

The analyses of the two other events (Barsebäck [25] and Davis Besse [26]) show that in both instances all safety systems were available. During the Barsebäck event, some safety systems had been challenged and operated according to the design. The high PSA number of Davis Besse is based on the assumption that a leak out of the vessel would have been likely in the next cycle. The most likely failure was estimated to be a small break LOCA within the next five months.

The WGRISK analyses provide two main insights: first, if an important number of NPPs is affected by the same hazard, the total risk increases significantly; second, besides the initiators that affected Fukushima Daiichi NPP there are also other safety significant initiators that should not be overlooked.

5. SUMMARY

This report on the precursor events to the Fukushima Daiichi NPP accident was initiated by the CNRA in the framework of tasks to be performed in the aftermath of the Fukushima Daiichi NPP accident. WGOE formed a small task group to develop the content of this report with support from the CSNI Working Group on Risk Assessment (WGRISK). The main questions to be answered by this report were:

- The Fukushima Daiichi NPP accident, could it have been prevented?
- If there is a next severe accident, may it be prevented?

To answer the first question, the report addressed several aspects. First, the report investigated whether precursors to the Fukushima Daiichi NPP accident existed in the operating experience; second, the reasons why these precursors did not evolve into a severe accident. Third, whether lessons learned from these precursor events were adequately considered by member countries; and finally, if the operating experience feedback system needs to be improved, based on the previous analysis.

To address the second question which is much more challenging, the report considered precursor events identified through a search and analysis of the IRS database and also precursors events based on risk significance. Both methods can point out areas where further work may be needed, even if it depends heavily on design and site–specific factors. From the operating experience side, more efforts are needed to ensure timely and full implementation of lessons learnt from precursor events. Concerning risk considerations, a combined use of risk precursors and operating experience may drive to effective changes to plants to reduce risk.

The first question to be answered was “have events adequately been addressed prior to Fukushima?” Actually, there are related precursor events in the IRS database. First of all, it had to be evaluated which categories of the IRS coding criteria are met by the Fukushima Daiichi NPP accident. In this report the Fukushima Daiichi NPP accident sequence was analysed. It was not tried to identify all its potential causes and root causes. Compared to the main key words of the IRS system, nearly all aspects of the Fukushima Daiichi NPP accident could be described sufficiently. The result of the analyses was that operating experiences have been disseminated internationally related to the main initiators and conditions that have been observed during the Fukushima Daiichi NPP accident. The accident did not show unknown initiators, sequences, or consequences. However, the combination and the severity of initiating events had not occurred before and the evolution of the accident in three different units simultaneously was also a new aspect. Currently, there are no major changes to the IRS database because of the Fukushima Daiichi NPP accident, but updates might be necessary once a full understanding of the accident is available.

The report also contains a short description and evaluation of selected precursors that are related to the course of the Fukushima Daiichi NPP accident. The main question to be answered in this section was “what barriers stopped these precursor events before they turned into accidents?” The effective barriers have been analysed and discussed. These barriers were specific to the events’ sequences, to the severity of the events and the design of the NPPs affected. There was no single effective barrier, it was a combination of systems, design features and in some instances operator actions that formed these barriers. There is no simple solution to prevent future accidents only from the barrier analysis.

The report addresses the question whether operating experience feedback can be effectively used to identify plant vulnerabilities and minimize potential for severe core damage accidents. Based on several of the precursor events national or international in-depth evaluations were started. The vulnerability of NPPs due to external and internal flooding has clearly been addressed. Also the dependency on the function of electrical systems is well known. But the combination of rare events – such as flooding, station black-out or loss of instrumentation and control – had not yet been reported to the IRS. In addition, the severity of reported events is not comparable with the Fukushima Daiichi NPP accident. Such single rare events have resulted in important lessons learned that have been issued and spread worldwide into the responsible institutions. The combination of these events had not sufficiently been taken into account.

Major events cause intensive national and international work to analyse the causes and to derive lessons to be learned. For some of them, the final lessons learned are derived only after several years of analysis. The number of significant lessons learned is very large. The challenge is the assessment of these lessons and the priority setting for their timely implementation at each NPP.

In addition to the IRS based investigation, the WGRISK was asked to identify important precursor events based on risk significance. These precursors have also been analysed regarding their initiators, their effective barriers and their main lessons learned. Among these precursors, there were the initiators earthquake, loss of ultimate heat sink and loss of offsite power that are directly connected to the Fukushima Daiichi NPP accident. The two other precursor events selected by WGRISK are related to the loss of coolant accident. In addition to the major events and initiators directly related to the Fukushima Daiichi NPP accident, there are further important initiators or event sequences that could result in core melt accidents. Therefore, the focus of plant improvements should also consider risk significance in addition to operating experience feedback.

The question related to the effective barriers in significant events can be answered with respect to the different event sequences and the specific NPP designs. There is no generic lesson to be learned from these events that has not already been addressed in the national and international operating experience networks.

Regarding the question related to the potential improvements for the international systems on operating experiences, it can be stated that significant efforts have been made – nationally and internationally – to derive specific and generic recommendations for further improvement of NPPs. The challenge is the assessment of the applicability to specific NPPs, and whether the proposed actions have to be prioritised or not. Technical measures may be assessed and implemented quite easily, but lessons related to human and organisational factors as well as to the safety culture represent constant challenges. While the implementation of lessons learned is mainly the task for the utilities, the regulatory bodies should be aware of the applicability of the lessons learned disseminated by the international systems.

The WGOE and the IRS – and the related task groups - have, for more than 30 years, provided insights on important single events and derive generic lessons to be learned from individual events or event groups. The competence of the WGOE ends with the dissemination of its results. The implementation is clearly the task of the national regulatory authorities and the NPP owners.

The final question “Can we prevent the next severe accident?” is difficult to answer. The operating experience feedback is one important tool to prevent events but there exist other approaches to maintain or improve the required level of safety of NPPs. The lessons learned from the evaluation of operating experiences are capable preventing future accidents if implemented in a timely manner. The challenge for utilities and regulators is to prioritise the numerous lessons learned depending on the individual plant designs and conditions.

The conclusion of this report is that the existing operating experience feedback systems provide a good tool to prevent recurrence of events. Operating experiences considering also the risk significance provide a great source of potential improvements that have demonstrated their usefulness in the course of real events. There have been major works done on new event features, e.g. after the Barsebäck event and the Forsmark-1 event. After the TMI-2 accident and the Chernobyl accident – as well as after the Fukushima Daiichi NPP accident – further international approaches have been started far beyond the continuous work of WGOE.

The implementation of foreign or international operating experience is a continuous challenge. The challenge is to timely implement related actions on plant level based on the generic lessons learned. This is an on-going challenge for utilities and regulators. The further development of methodologies to correctly prioritise the lessons to be learned should be a focus of future work. First approaches have already been published by CNRA in their series of NEA Regulatory Guidance Booklets. For example the booklet "Regulatory Challenges in Using Nuclear Operating Experience (2006)" [30] provides valuable recommendations to improve the use of operating experiences.

REFERENCES

[1] Nuclear Energy Agency (2012), Summary record of the 26th CNRA meeting NEA/SEN/NRA(2012)1_SR_26th CNRA.

[2] International Atomic Energy Agency (2010), IRS Guidelines, IAEA, Vienna, Austria.

[3] Special Report on the Nuclear Accident at the Fukushima Daiichi NPP Nuclear Power Station, INPO 11-005, 2011.

[4] IRS No. 19, Partial Melting of Fuel Cladding due to Abnormal Temperature Rise during a Rise in Power, St. Laurent-1, France.

[5] IRS No. 7632, Damage Of Fuel Assemblies Inside A Cleaning Tank, Paks-2, Hungary.

[6] IRS No. 8220, Accident at Three Mile Island Unit 2 (March 28, 1979): NRC Backgrounder, TMI-2, USA.

[7] IRS No. 8175, Tohoku-Taiheiyou-Oki Earthquake Effects on Japanese Nuclear Power Plants: NRC Information Notice 2011-05.

[8] IRS No. 7342, Partial Loss of Safeguard Systems as a Result of External Flooding, Blayais-1, France.

[9] IRS Topical Study, Operating Experience Feedback (OEF) External Flooding, prepared by IRSN for the IAEA, Vienna, Austria, 2010.

[10] IRS No. 1025, Fire in one Turbine Generator Group and Subsequent Failure of Safety Systems, Vandellos-1, Spain.

[11] IAEA, ASSET-Mission to Vandellos-1, Chapter 2, Analysis of the Event: Degradation of Operability of the Safety Function “Cooling Of Fuel” due to Fire on one Turbo Generator, 1990.

[12] IRS No. 1008, Loss of Vital AC Power and the Residual Heat Removal System during Mid-Loop Operation at Vogtle Unit 1, Vogtle-1, USA.

[13] IRS No. 6350, Deenergization of DC Switchboard due to Damage to a Reversible Motor Generator and Battery Tripping, Kola-1, former USSR.

[14] IRS No. 6341, Complete Station Blackout due to Fire in Turbine Building at NAPS-1, Narora-1, India.

[15] Gawande, D., Fire in the Turbine Hall Resulting in Complete Failure of all Classes of Power Supplies, Presentation on the 11th WGOE-Meeting, March 2012.

[16] Final DIDELSYS Task Group Report, Defence in Depth of Electrical Systems and Grid Interaction, NEA/CSNI/R (2009)10.

[17] IRS No. 7596, Pipe Rupture inside Containment due to Radiolysis Gases Explosion, Brunsbuettel, Germany.

[18] IRS No. 7788, Loss of 400 kV and Subsequent Failure to Start Emergency Diesel Generators in Sub A and Sub B, Forsmark-1, Sweden.

[19] Edward D. Blandford and Michael M. May, Lessons Learned from “Lessons Learned”: The Evolution of Nuclear Power Safety after Accidents and Near-Accidents, ISBN: 0-87724-094-9, 2012.

[20] Nuclear Energy Agency (2013), Fukushima Daiichi NPP Nuclear Power Plant Accident: OECD/NEA Nuclear Safety Response and Lessons Learnt, NEA No. 7161, OECD, Paris, France.

[21] IRS No. 401, Power Grid Outage, 27 December 1983, Sweden.

[22] IRS No. 8068, Total Loss of the Heat Sink further to Clogging of the Rotating Drum Screens by a Very Significant Arrival of Vegetable Materials, Cruas-4, France.

[23] LER 3382011003R00, Dual Unit Reactor Trip and ESF Actuations during Seismic Event with a Loss of Offsite Power, North Anna-1, USA.

[24] IRS 8335, Performance Issues with Seismic Instrumentation and Associated Systems for Operating Reactors, generic report, USA.

[25] IRS No. 1294, Clogged Pump Suction Strainers in the Wet Well Pool, Barsebäck-2, Sweden.

[26] LER 3462002002R00, Reactor Coolant System Pressure Boundary Leakage Due to Primary Water Stress Corrosion Cracking of Control Rod Drive Mechanism Nozzles and Reactor Pressure Vessel Head Degradation, Davis Besse-1, USA.

[27] International Atomic Energy Agency (2008), IRS Topical Study Analysis of Events Related to Interaction between Grid and NPPs, SSA J1020261, IAEA, Vienna, Austria.

[28] Nuclear Energy Agency (2006), IRS Blue Book 2002-2005, Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System, NEA No. 6150, OECD, Paris, France.

[29] IRS No. 8164, Non-compliance of rod big end bearings in emergency diesel generator engines, generic, France.

[30] Nuclear Energy Agency (2006), CNRA, Regulatory Challenges in Using Nuclear Operating Experience, NEA No. 6159, OECD, Paris, France.