http://dx.doi.org/10.5516/NET.03.2012.700

PRESENT DAY EOPS AND SAMG - WHERE DO WE GO FROM HERE?

GEORGE VAYSSIER
NSC Netherlands, Leiden, The Netherlands
E-mail : george.vayssier@nsc-nl.com

Received March 23, 2012

The Fukushima-Daiichi accident shook the world, as a well-known plant design, the General Electric BWR Mark I, was heavily damaged in the tsunami, which followed the Great Japanese Earthquake of 11 March 2011. Plant safety functions were lost and, as both AC and DC failed, manoeuvrability of the plants at the site virtually came to a full stop. The traditional system of Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMG) failed to protect core and containment, and severe core damage resulted, followed by devastating hydrogen explosions and, finally, considerable radioactive releases.

The root cause may not only have been that the design against tsunamis was incorrect, but that the defence against accidents in most power plants is based on traditional assumptions, such as Large Break LOCA as the limiting event, whereas there is no engineered design against severe accidents in most plants. Accidents beyond the licensed design basis have hardly been considered in the various designs, and if they were included, they often were not classified for their safety role, as most system safety classifications considered only design basis accidents.

It is, hence, time to again consider the Design Basis Accident, and ask ourselves whether the time has not come to consider engineered safety functions to mitigate core damage accidents. Associated is a proper classification of those systems that do the job. Also associated are safety criteria, which so far are only related to 'public health and safety'; in reality, nuclear accidents cause few casualties, but create immense economical and societal effects – for which there are no criteria to be met.

Severe accidents create an environment far surpassing the imagination of those who developed EOPs and SAMG, most of which was developed after Three Mile Island – an accident where all was still in place, except the insight in the event was lost.

It requires fundamental changes in our present safety approach and safety thinking and, hence, also in our EOPs and SAMG, in order to prevent future 'Fukushimas'.

KEYWORDS : Post-Fukushima, Extended Design Basis Accidents, Extended SAMG Technical Basis, BDBA Safety Classification, Outside Emergency Support.

1. INTRODUCTION

Present day EOPs and SAMG have been largely developed on the basis of the experience from the accidents at Three Mile Island (1979) and Chernobyl (1986). Before these events, EOPs had been written for accidents up to design basis accidents (DBAs). Safety functions were defined to cope with such accidents. The associated equipment, such as ECCS, was classified for safety and, hence, designed to high quality standards.

The basic lesson from TMI was that, although all provisions were in place, an accident could happen beyond the DBA, even developing into a core melt, because the control room staff lost insight in the ongoing scenario. And EOPs of those days departed from a successful diagnosis of the scenario.

The TMI accident led to the development of EOPs that were independent from such recognition; they were designed to preserve the fundamental safety functions: subcriticality, core cooling and containment integrity. They serve as a kind of umbrella if the operators lose insight in the actual scenario. EOPs were also developed for events beyond the DBA, such as Anticipated Transient Without Scram (ATWS) and Station Black-Out (SBO). The EOPs did not only use classified systems, but used everything available, irrespective of its qualification.

The accident in Chernobyl showed the consequences of non-mitigated severe accidents in full and led, inter alia, to the development of Severe Accident Management Guidance (SAMG). This guidance would be entered once core damage was imminent or had already taken place. The focus of the guidelines shifted from preservation of core integrity to protection of (remaining) fission product boundaries. Mechanisms that challenge the integrity of these boundaries were identified, usually by PSA level 2. Examples are SG tube creep rupture, high-pressure melt ejection (HPME), vessel failure, hydrogen explosion, basemat attack and containment overpressurisation.

Both EOPs and SAMG, however, assume that instrumentation and control (I&C) is available and cooling water is available or will be again available within short time. For example, the first Severe Accident Guideline (SAG) in the Westinghouse Owners Group approach tells the operator to fill the SG, to prevent SG tube creep rupture.

There is a remarkable *common weakness* in this combined EOP/SAMG structure: *both use the same systems*: instrumentation, power, pumps and valves, and cooling water. One could argue that if all this is available, a severe accident has such a low probability that plant safety is not really enhanced by adding SAMG to high-quality EOPs. The only exception to this common weakness is the set of Extensive Damage Mitigation Guidelines (EDMG) at US plants, but these have been designed to respond to terrorist attacks, not because of the described inherent weakness in the EOP/SAMG structure.

Another weakness is the continuous consideration of the LBLOCA as the limiting DBA. The consequence is that *only SSCs*[1] *to mitigate the consequences of DBAs have been formally classified for safety* in most regulatory systems. Systems needed to mitigate severe accidents are usually not formally classified for safety. Some designs, like the EPR and the AP1000, have developed classification systems that go beyond the DBA classification, but this is on a voluntary basis. The IAEA is developing a safety guide on safety classification, which contains also a classification beyond DBA (BDBA), but the examples mentioned mostly allocate only commercial quality to most SSCs which mitigate BDBA.

A related problem is that the nuclear safety regulation usually (with few exceptions) focuses on public health and safety; the large damage that may be inflicted from nuclear accidents on the environment, the economy and the society is mostly unregulated.

Another problem is that not all plants have installed SAMG, and the plants that have SAMG use widely scattered approaches. There are three US PWR Owners Group (OG) approaches and one BWROG approach, and there are different approaches in various other countries. There is *an urgent need* to review these different approaches by appropriate review teams, such as those from IAEA RAMP[2] missions.

Industry should start to harmonise the approaches, as they all have a common goal. A beginning of such harmonisation has been made in the US.

As we have learned from Fukushima, reality is different. It looks like nuclear safety is centred around accidents that do not happen (LBLOCA, and other DBA), but that it fails to cover accidents that do happen (severe accidents). There is a need to reconsider a number of items:

- DBAs should include a number of accidents now called BDBA, as well as accidents in which control over the core is lost;
- safety criteria should include environmental and economic effects of severe accidents, as well as possible societal disruption;
- safety classification should include SSCs to mitigate severe accidents; this includes consideration of classification for seismic events, environmental effects, pressure integrity and quality assurance;
- SSCs that mitigate severe accidents should be largely separate from SSCs that mitigate DBA;
- EOPs should be strengthened to include strategies now only available in SAMG;
- the Technical Basis of SAMG should include spent fuel pools, hydrogen in adjacent buildings, cooling by dirty water / seawater, and protection of groundwater in basemat melt-through;
- SAMG should not be fully dependent on availability of AC, DC and cooling water of the NPP; a possibility is the use of portable equipment and the development of EDMGs; this should cover a spectrum of 'Extreme Events';
- prolongation of SAMG mission time;
- multi-unit damage and disorder in the surroundings should be assumed, which limits outside support;
- extensive external support from competent organisations (plant vendor, TSO[3], scientific institutions, government agencies, etc.);
- in-depth training for all involved in a highly stressful environment.

These items and others will be discussed below in more detail.

2. SELECTION OF DESIGN BASIS ACCIDENTS.

Nuclear power plants have been designed in a robust way, i.e. there is a high quality of structures, systems and components (SSCs), so that there is a low probability of failure of these SSCs. Nevertheless, the designer assumes that deviations from normal operation can occur, and that failures happen that may endanger the fundamental safety functions: controlling the reactivity of the core, cooling the core and spent fuel pool, and confining any radioactivity that otherwise may be released. Systems and procedures are in place that prevent anticipated operational occurrences from developing into accident conditions.

In addition, the designer has selected a number of hypothetical accidents, i.e. accidents that are not assumed

[1] SSCs = structures, systems and components

[2] RAMP = 'Review of Accident Management Program', a service offered by the IAEA

[3] TSO = 'Technical Support Organisation', usually a scientific organisation supporting a regulatory body

to occur during plant life, but which are included in the design basis to generate a high level of safety. SSCs are developed that can mitigate such accidents and, therefore, are believed to generate large safety margins to accidents that may occur 'in real life'. These hypothetical accidents are called Design Basis Accidents (DBAs); examples are large break LOCA (LBLOCA) and control rod ejection. That this concept worked was shown in the TMI-accident: the containment remained intact, despite the fact that an accident occurred for which it had not been designed.

This concept of layers of safety is known under the name 'Defence in Depth' (DiD), of which we just have described the first three levels. Good quality of SSCs is the first level, tolerance against disturbances and failures is the second level, and protection against hypothetical accidents (design basis accidents) is the third level.

Releases that go with these accidents must be below prescribed limits.

The concept of DiD, well described in [1], includes even further levels. Should accidents happen that are beyond the DBA (the BDBA), then provisions should still be in place to limit the consequences. These consequences, however, need not be demonstrated to stay below prescribed limits, as is the case with DBAs. Typical examples are Anticipated Transient Without Scram (ATWS), loss of the ultimate heat sink (UHS), and Station Black-Out (SBO). Also accidents that involve core damage are in this category. All measures that are in place to mitigate such accidents are in level 4 of the DiD.

Ultimately, it should be recognized that limitations of radioactive releases may not be achieved and that substantial amounts of radioactivity may be set free. Then protection measures of plant staff and general public are initiated, which can mean sheltering against radioactivity, taking iodine pills or evacuation. These measures are the fifth level of the DiD.

This concept of Defence in Depth, with designing NPPs against a set of DBAs and taking measures beyond DBAs, is a 'corner stone' of nuclear safety and has been confirmed and strengthened by the results of PSAs. Many PSAs showed core damage accidents to be in the range of 1.0E-4 to 1.0E-6 / reactor-year, with release frequencies being one or two orders of magnitude smaller. In practice, this means they are not expected to happen.

Even core damage frequencies of 1.0E-07 have been reported. The actual meaning of such a value is that a core melt accident only happens *once in the entire life time of the human race* (which so far has lived for about 5 million years). Note that this result has been obtained in a technology which *has hardly existed for 60 years*. With computing technologies which only have existed for *half that time*. PSAs have enjoyed and still enjoy a remarkable degree of belief, despite the short time they exist and the remarkable results which they report. The question may arise whether we are not over-confident about a technology which has existed only a few decades, but claims results valid for a time span of thousands, or even millions of years.

This concept of DBAs, thought out in the sixties/ seventies of the last century and strengthened by the PSA-results as described, apparently does not match the reality. The three major accidents which we have seen in the last several decades, TMI, Chernobyl and Fukushima-Daiichi were core damage accidents, two of which resulted also in large radioactive releases. There were also a number of near-misses, such as the Maanshan SBO in 2001, where operators only through hard work and sheer luck were able to survive an SBO. The grace time for such an event was set by designers, with approval by their regulatory bodies, at 2 hours. In a core melt event, regulators often set 24 hours as the time where they require defined counter-measures, and decreased requirements, if any, after that.

Those responsible for such values probably have no idea about the turmoil that goes with such drastic and dramatic events which beyond design basis accidents and notably severe accidents are. Losing all AC is not just bad luck, to be handled by a smart mechanic for whom 2 hours for repair of a diesel engine is plenty of time. Losing core cooling and facing large releases is not just a job for 24 hours; it is a struggle of life and death - maybe even literally - and may last days, weeks, or even months.

The consequence must be that we should rethink the concept of DBA. And that we should rethink the grace time that goes with events beyond the (present) DBA. Let us state this fairly: design basis accidents should be - as a minimum - those that actually occur. Grace times are those times which - with realism - are needed to 'fix the problem'. This may be repairing a diesel engine in an SBO scenario, or establishing a controlled release path in a severe accident. Restoration actions in a severe accident may take many hours, maybe days, possibly a week or longer.

A possible solution is the following: define the accidents which are now part of the BDBAs but are not yet core melt accidents inside the design basis accidents. Examples are ATWS, loss of UHS, SBO. A basis could be the PSA - just 'condemned' for its optimistic results. If we take all accidents which have a calculated frequency of occurrence of, say, above 1.0E-8 / reactor-year, we have at least a series of common cause failures, which otherwise are beyond the scope of DBAs. Note that this cut-off frequency is also used as a cut-off frequency above which EOPs are defined in a number of EOP-approaches. Note also that the use of PSA here is not a measurement of plant risk - it serves as a tool to define improbable accidents which are candidate events for the set of design basis accidents. Whether such accidents are indeed then DBAs for a particular design, may still be the result of engineering judgement. The result is that mitigative systems have to be designed that cope with these events, and do so within prescribed regulatory limits. These may or may not be the same as those of the traditional DBA. As it concerns events with a low probability, higher release limits could be defined.

The above receipt may still go without severe accidents inside the envelope of DBAs. For this set of accidents, it seems prudent to just assume and postulate that they will occur during plant life. That means core cooling gets lost and the whole series of phenomena associated with a core melt accident are assumed to occur. Hence, we assume the core melts down to a pool in the lower plenum and threatens the vessel integrity by a melt-through. Hydrogen will be generated and its combustion may threaten the containment integrity. Corium may interact with the basemat concrete and generate large masses of CO_2, which also may threaten containment integrity. As the containment is a pressure vessel, designed to contain radioactive material, it should have overpressure protection and, as such devices upon activation will release radioactive material, also appropriate filtration, to limit the consequences for the environment.

For all these phenomena, engineering countermeasures have been developed. By declaring the core melt accident as an accident inside the design basis, these counter-measures get 'status', i.e. their mitigative devices must be properly designed, inspected, tested and operated. And they fall within the regulatory oversight.

An example of a useful extension of the design basis to severe accidents is the protection of the containment against subatmospheric pressure. In a severe accident, we may wish to vent the containment. However, as much air will also then be ejected from the containment, the containment may reach subatmospheric pressure once the steam has condensed later in the accident. Similarly, if we burn or recombine the hydrogen, we also 'eat away' the oxygen from the atmosphere, and may create subatmospheric pressure. The vacuum protection system, however, has not been designed against such subatmospheric pressure, and the containment may collapse.

Note that this does not mean the core melt accident will become a formal 'design basis accident'. The consequences of a DBA fall with predefined margins within regulatory release limits. Techniques to control severe accidents have not yet progressed so far that this can be achieved for those accidents. As a regulatory limit, one could propose just ALARA: let the designer demonstrate that he has achieved this prime objective of nuclear safety. Hence, the severe accident falls within the design basis, yet is not formally a design basis accident.

Of course, the above suggestions for redefining the DBA are not unique solutions - other approaches can be developed as well.

So far, we note two regulatory actions where accidents beyond the design have obtained additional weight. One is in the IAEA Requirements "Safety of Nuclear Power Plants: Design", SSR 2/1, which is a revision of IAEA NS-R-1, in the 'design extension conditions', [1]. The other is included in the statement of former USNRC Chairman dr. Nils Diaz, in his recent speech before the 19th International Conference on Nuclear Engineering (ICONE19), Osaka, Japan, in October 2011, [2]: "We should be mindful of striking a proper balance between confirming the correctness of the design basis and expanding the design basis of U.S. plants"- USNRC.

The industry has included protection against severe accidents in some of its newest reactor designs, such as the EPR, the AP1000, the ESBWR and the VVER-TOI.

3. SELECTION OF SAFETY CRITERIA.

So far, in most countries, the criteria to measure the consequences of reactor accidents are formulated in radiological limits. This is an appropriate set of limits for the traditional DBAs, as other consequences of these DBAs, i.e. socio-economic and environmental consequences, are practically negligible.

This situation, however, does not hold for severe accidents. The severe accidents which we have seen in Chernobyl and Fukushima had enormous consequences for the society, the economy and the environment. Societal consequences were very visible: people had to be relocated, and there is the threat that they will not be allowed to return to their homes for a long time - if not forever. Also, the environmental damage is visible: large areas are contaminated, control of vegetation and animals in these areas has become difficult, if not practically impossible. Finally, also the economical damage can be very large. If, for example, the radioactive release from a severe nuclear accident will hit a big harbour, all traffic from and to that harbour may be paralysed. Even if the radiological limits on goods and products are in an 'acceptable range', customers may not want to buy goods shipped via that harbour.

However, in most countries there are no criteria for societal, environmental and/or economic damage caused by nuclear accidents. Hence, design of SSCs is not directed to satisfy such criteria, and regulators have no means to set such requirements on NPPs.

There are some exceptions: for example, in Sweden and Finland there are criteria for land contamination, i.e. there are environmental criteria, [3], [4]. And the common position on severe accidents by the French GPR[4] and the German RSK for the EPR requires that the need for measures outside the plant should be 'practically eliminated', which thereby includes a societal criterion [5].

There is, to the knowledge of this author, no criterion to limit economic damage. What will, for example, be the impact of a severe accident at the Doel station, Belgium, on the operations of Antwerp harbour? Even if ships are contaminated below acceptable safety levels, it may occur

[4] GPR = Permanent Group of Experts of Nuclear Reactors, RSK = Reactor Safety Committee

that their owners and/or business partners will suspend any business with those ships. This may bring economic damage to unprecedented levels. Where tolerable radiation levels for the protection of the people near the site and of the environment can be defined more or less on quantifiable parameters, economical damage cannot, as it depends on the mindset of people and companies doing business - which cannot be quantified.

The only possible solution seems to be that countries set in advance what they believe is a tolerable level of contamination for vessels and industrial equipment to continue doing business in case of a large nuclear accident. Not in terms of causing harm to people involved - for that purpose, there are sufficient regulations - but for the incentive of companies to continue doing business with the stricken harbour and/or industrial area. Even then, it is not sure that business will go on 'as usual' after a severe nuclear reactor accident in the surroundings.

4. SAFETY CLASSIFICATION

With few exceptions, safety classification is only defined for SSCs that mitigate accidents up to and including equipment designed to mitigate DBAs. A well-known safety classification is [6]. A special class is available for SSCs with separate licensing commitments, which could be used for SSCs designed to mitigate BDBA. This, however, is not further detailed in the standard.

The IAEA works on a safety standard that classifies SSCs to mitigate BDBAs and severe accidents, [7]. This (draft) standard then gives a practical example in its Appendix II, where such SSCs are in safety class 3, which is one class lower than the SSCs for mitigation of DBAs. It is remarkable that SSCs which are used or even designed to mitigate BDBAs, including severe accidents, have such a moderate classification. The reason, of course, is that these accidents are 'beyond design' and, in the traditional safety philosophy, do not need the stringent requirements for the SSCs mitigating DBAs.

By enlarging the spectrum of DBAs, this problem, of course, is already partially solved. Where this is not feasible, at least the classification of SSCs used and/or designed to mitigate BDBAs and severe accidents could be adapted.

As such, the methodology of [7] offers this 'upgrading'. However, the relation between these specific classes for SSCs, which mitigate BDBAs and severe accidents, and the design requirements for those SSCs should be better defined, possibly also upgraded.

As an example, consider the containment vent line. As this is a line in this safety class 3, it may not need to satisfy seismic requirements for safety class 2 equipment. If we then have a severe accident initiated from a seismic event, this line may fail and, in the moment one wishes to vent the containment, one will vent the gases to other rooms and compartments, possibly causing damaging hydrogen explosions and large releases.

Some new NPP designs have recognized the importance of a safety classification for systems designed to mitigate BDBAs and severe accidents. Examples are the EPR and the AP1000. Typically, however, some other new designs did not.

5. SSCS THAT MITIGATE SEVERE ACCIDENTS SHOULD BE LARGELY SEPARATE FROM SSCS THAT MITIGATE DBAS

A severe accident does not start from 'scratch' - there is probably a prehistory. It may start from a relatively small event, which gradually deteriorates into a larger event, and from there into a severe accident. This means that usually

Table 1. Proposed Classification According to IAEA DS 367, [7]

Requirements	Mitigatory Safety Functions		
	Safety Class-1	Safety Class-2	Safety Class-3
Quality Assurance	Nuclear Grade	Nuclear Grade	Commercial Grade or Specific Requirements
Environmental qualification	Harsh or Mild	Harsh or Mild	Harsh or Mild
Pressure Retaining Components (example codes)	High Pressure: C2 Low Pressure: C3	C3	C4
Electrical (IEEE)	1E	1E	Non-1E
I&C (IEC 61226 Category)	A	B	C
Seismic	Seismic Category 1	Seismic Category 1	Specific Requirements
Civil Structures (External Events)	Class 1	Class 1	Class 1

the operator and the Technical Support Centre (TSC) have started a number of systems to mitigate the event before it has degraded to a severe accident. In this time frame, they use the various plant systems, as is indicated in the EOPs.

Once core damage is imminent or actually occurs, most accident management approaches transit to SAMG. An example is the generic Westinghouse Owners Group (WOG) SAMG, where, upon core damage, the first priority is to fill the steam generator (Severe Accident Guideline #1, SAG-1). The second and third priorities are to depressurise the RCS and to fill the RCS.

Such measures have been defined and make sense in situations where the operator has lost insight in the ongoing events, but still has necessary equipment, power and water available. This was the situation at Three Mile Island - all was there, except insight into what happened and what needed to be done. After TMI, however, highly sophisticated EOPs have been developed, which have proper answers to operator needs, even if he/she has lost insight into what actually is going on. The WOG EOPs define critical safety functions (other approaches have equivalent names), which are the only safety functions the operator needs to care about to bring his/her plant back to a safe condition.

The consequence is that, if the operator nevertheless must face a core melt accident, this is practically only possible because the systems which he/she needs to properly execute the EOPs, fail to operate. Hence, if there is no water for the core for hours, there probably is also no water in the few minutes which pass after the transition to SAMG and SAG-1 needs to be executed. Similarly, there will also be no water to fill the RPV (SAG-3). This will practically exclude the possibility to execute the SAMG as they have been designed.

Consequently, systems that are able to support SAMG should be different from those designed or used to execute EOPs. A corollary is that the same systems indeed may be used, provided that also separate systems are available for SAMG.

The ideal case would be if the systems are not only different, but also use different power (both AC and DC) and systems to provide cooling water. This has been largely realised in a number of German reactors, where separate bunkered systems are capable of providing separate AC and separate cooling water. American reactors (and some others) provide portable systems, located elsewhere on site, which can be hooked up to the plant in case of an unavailability of the plant systems, e.g. caused by extreme external events.

6. EOPS SHOULD BE STRENGTHENED TO INCLUDE STRATEGIES NOW ONLY AVAILABLE IN SAMG.

Further to #5, a logical question then is to consider why the systems that are designed to support SAMG can also not support EOPs.

A problem here is that the execution of SAMG usually requires a different organisation and a different decision making model. In EOP-domain, operators are responsible and take most/all decisions, whereas in SAMG-domain, usually the TSC and the Site Emergency Director (SED) are the responsible organs. In EOP-domain, operators try primarily to save the core; in SAMG-domain the priority is with protection of the fission product boundaries - if needed, even at the cost of core integrity. Some of the SAMG-techniques, hence, may not be suitable for execution inside the EOPs.

In principle, however, all that is available in SAMG-domain, should be made also available in EOP-domain. Application should be done carefully, as SAMG has other objectives, may have negative consequences and can even work out detrimental for some SSCs relevant for safety in EOP domain (e.g., pumping sea water in the reactor or steam generator).

7. THE TECHNICAL BASIS OF SAMG SHOULD INCLUDE SPENT FUEL POOLS, HYDROGEN IN ADJACENT BUILDINGS, PROTECTION OF GROUND WATER IN BASEMAT MELT-THROUGH.

SAMG has originally been set up for the core at power states, as this obviously was the most challenging condition for a reactor in distress. Risk studies showed, however, that for many plants a considerable risk was also present in shutdown states, which warrants a separate type of SAMG, so-called Shutdown SAMG, usual acronym SSAMG.

Only few plants, so far, have developed such SSAMG. This type of SAMG includes plant states where the containment is open and/or the RPV is open, as occurs during refuelling / maintenance periods. SSAMG includes also the spent fuel pool.

The development of SSAMG require an extension of the Technical Basis of at-power SAMG. This work has started e.g. in the US, for the generic Owners Groups SAMG-approaches.

Generally, SAMG should also be developed for areas outside the containment, where leakage or venting of the containment may bring radioactive gases to adjacent compartments. If, for example, such leakage will contain hydrogen, hydrogen combustion is possible in those compartments. This will also load the containment by pressure loads from outside, for which it has a limited design value - which value is not linked to any hydrogen combustion in those compartments.

Other areas where the present Technical Basis of many SAMG approaches can be improved are:

- air ingress into the RPV
  - this becomes an issue after RPV melt-through
- cooling by untreated water (including dirty water, sea water)

  - where available stocks of borated water, demineralised water, etc. are exhausted
- measures to cope with loss of I&C
  - where loss of DC has occurred - but SAMG measures requires insights in the plant damage states
- better insight in potential negative consequences of proposed SAMG actions

The last issue stems from the fact that no action under SAMG should be initiated before the potential negative consequences have been balanced against the expected benefits. However, few TSCs, if any, have appropriate tools to do this, and on-the-spot calculations seem hardly feasible.

Measures to prevent or halt the core-concrete interaction ('core catchers') have been developed for a number of new reactor designs. In the absence of such designs, or where the proposed measures lack a convincing demonstration, basemat attack and melt-through may occur. The consequence has, so far, been considered to be low in terms of risk profile: the containment leak deep in the foundation does not lead to harmful radiation levels outside.

However, ground water may be polluted and, by the spread of this ground water, contaminate a large area. Where such ground water also is used for preparing drinking water or used for agricultural or industrial purposes, a serious long-term environmental problem may occur. Plants should, therefore, enhance their basemat protection or, where this is not possible, consider to erect large steel dams around the plant (after the accident), so as to minimise the spread of contaminated water.

Enhanced basemat protection can be done, for example, by preparing for filling cavities below the RPV, if any, with concrete, or to prepare for injection of further concrete under the plant basemat, where this is feasible.

As the probability of this accident is low and there will be, for most plants, ample time to build the dam or pour the concrete once the threat is there, it would be sufficient for most plants to just *prepare for* building the dam, or pouring the concrete. This means material is in place or can be brought in quickly, and plant layout indeed allows the building of the dam, without cutting important pipe lines or electric cables.

8. SAMG UNDER LIMITED OR NO AVAILABILITY OF AC, DC AND COOLING WATER OF THE NPP.

In the case of large damage to the site and/or complex internal events, there may be a total loss of AC, DC and normal or emergency cooling water supply. This may not only affect the reactor, but also the communication network on the plant: telephones, loudspeakers are dead, etc.

This situation may lead to a total loss of EOP and SAMG capability. Many plants have, therefore, created stocks of portable equipment, which can be brought to the plant and hooked up to pre-installed connections. Where DC cannot be restored, instrument calibrators can be used to read instruments. Also valves cannot be operated by power and, hence, must be operated manually. This may require special provisions at the various valves.

Note that for manual operation one must consider the local environmental conditions, which may induce the need to design tools for remotely operated manual control. For example, the manual operation of a containment ventilation valve may require special provisions, in view of the local radiation fields.

Such complications lengthen the time that is needed to initiate proper actions - which should also be reflected in the EOPs and SAMG.

In the most severe cases, there is also a loss of command and control. For example, if there is no answer from the control room upon the occurrence of site damage. Procedures then must be in place to start the Emergency Plan at the site, possibly even by a neighbouring plant, so that there again is a line of command and control.

Major actions under such circumstances are to shutdown the reactor, to initiate core cooling (e.g., by the turbine driven auxiliary feed water for the PWR and the Reactor Core Isolation Coolant system {RCIC} or Isolation Condenser {IC} for the BWR) and to isolate and protect the containment. A description of needed functions and the associated equipment can be found in [8]. In this example, the associated procedures are called Extensive Damage Mitigation Guidelines (EDMGs). The various safety functions and mitigation strategies of [8] are presented in Table 2.

Safety functions:

Table 2. Safety Functions and Mitigation Strategies under Large Site Damage (largely from [8]).

BWR Safety Functions	PWR Safety Functions
RPV level control	RCS inventory control
RCS heat removal	RCS heat removal
Containment isolation	Containment isolation
Containment integrity	Containment integrity
Release mitigation	Release mitigation

Mitigation strategies:

BWR mitigation strategies	PWR mitigation strategies
Manual operation of Reactor Core Isolation Coolant (RCIC) or isolation condenser (IC)	Makeup to Reactor Water Storage Tank (RWST)
DC power supplies to allow depressurisation of RPV & injection with portable pump	Manually depressurize SGs to reduce inventory loss
Utilise feedwater and condensate	Manual operation of turbine (or Diesel-) driven Auxiliary Feedwater (AFW) pump
Make up to hotwell	Manually depressurise SGs and use portable pump
Make up to Condensate Storage Tank (CST)	Make up to CST or alternate feed source
Make up to Control Rod Drive (CRD)	Containment flooding with portable pump
Procedure to isolate the Reactor Water Clean-Up (RWCU)	Portable sprays
Manually open containment vent lines	
Inject water into the drywell	
Portable sprays	

9. PROLONGATION OF SAMG MISSION TIME.

A number of EOP and SAMG actions assume a remarkably short time to initiate and complete restorative actions. Often, a time span of 2 hours is defined to restore AC, as this is the amount of time an NPP considers to be sufficient to hook up to alternate AC sources. This, however, assumes an intact site area and no large disturbances from outside or at the grid.

For actions with a damaged core, the mission time is often 24 hours: after this time, it is apparently assumed that plant staff and off-site support have taken sufficient measures to deal with the consequences.

The reality here probably looks much different. A severe accident does not occur unless there is a large disruption of normal operating conditions. What that in fact is, is difficult to predict. A severe accident from outside events, as we have seen in Fukushima, totally disrupts possibilities to restore power in 2 hours or, once core damage occurs, to limit the consequences in 24 hours. Similar conditions may apply if there is a large fire, or other limiting circumstances.

It seems prudent to enlarge mission times: having a diesel back on line may take a whole day, or even longer. And consequences of severe accidents may require a week, or a month, or even longer, to establish stable conditions, for which long term measures can be defined.

A number of plants (and regulatory bodies) have already taken action and lengthened the SBO allowable time to 8 hours, 24 hours; even 72 hours is considered.

The long operation time of emergency equipment and cooling with various water sources for a long time, may produce large quantities of radioactive water, for which at present there are no provisions on site. Run-off of such water to the sea, river or other environment, may cause widespread contamination. There is a need to design facilities to capture such run-off and treat the associated radioactive waste. This is a complex matter, as the mass of run-off water can be very large.

10. MULTI-UNIT DAMAGE AND DISORDER IN THE SURROUNDINGS SHOULD BE ASSUMED, WHICH LIMITS OUTSIDE SUPPORT.

A clear lesson from the Fukushima accident is that, on a multi-unit site, more than one NPP can get into distress. Often, at multi-unit sites, it is assumed that only one unit is stricken at a time, and then help (e.g. additional AC, cooling water) can be obtained from the other unit(s). This, apparently, is too optimistic a view.

The disorder that causes or goes along with the severe accident at one unit, may affect other units as well. For example, a large release from one unit may hamper rescuing efforts from other units. Site disorder, as we have seen, even may inflict severe accidents on various units at the same time. Site disorder also limits possibilities to change shifts, to bring in additional equipment and/or staff and to orderly execute the site Emergency Plan, which then may affect health and safety of the public.

Multi-unit sites may have only one set of portable

emergency equipment, as only one unit at a time is assumed to be in need for such equipment. Apparently, the volume of portable equipment should match the need of more than one unit (possibly: all units) on the site. In addition, care should be exercised that the storage of such additional equipment is not itself at risk under the event causing the site damage. For example, in case of possible flooding, the elevation of the warehouse(s) that store(s) this equipment should be well above any real or even at a hypothetical maximum water level. Off-site storage is also feasible - and alleviates site concerns - but this may require heavy-lifting helicopters, as surface transport may not be well possible. Can we expect helicopter pilots to fly through a cloud of radioactive material?

For use of off-site equipment, proper agreements / contracts with the third parties which are involved (army, foreign nations) should be put in place - one may *expect* but not always *count* on good will under these circumstances: third parties may have other obligations and/or priorities. Successive use of installed equipment on-site, use of portable equipment on-site and off-site equipment is under development in the US under the name 'FLEX' [9] and in France under the name 'Hardened Safety Core' [10].

11. EXTENSIVE EXTERNAL SUPPORT FROM COMPETENT ORGANISATIONS (PLANT VENDOR, TSO, SCIENTIFIC INSTITUTIONS, GOVERNMENT AGENCIES).

As stated various times above, severe accidents may be extremely complex events, for which no easy answers may be available, despite well-developed EOPs, SAMG, possibly EDMG, and a well-designed TSC and Emergency Response Organisation. It cannot be expected that plant staff can develop new EOP-SAMG-EDMG strategies on the spot - in most plants, plant staff does not have the knowledge or in-depth experience that the EOP-SAMG-EDMG developers have. And they do not have the time, should they have that knowledge and experience. On the other side, plant staff can be expected 'to know their plant', i.e. they will have knowledge about possible exotic line-ups, power connections, etc. which knowledge may not be available at the plant designer and/or EOP-SAMG-EDMG developer. Certain complex physical phenomena, e.g. solvability of hydrogen in water, fuel clad oxidation in air, may only be well known at scientific institutions, Technical Support Organisations (TSOs), or other bodies with in-depth knowledge about the physical phenomena of beyond design basis and severe accidents. Exotic solutions, e.g. helicopter transport of heavy equipment, may require army involvement, as discussed under #10. Also any predictive capability – when will the reactor vessel fail, when do we need to vent the containment? – may also only be available at high-level institutes. Note: one could argue to also create such a possibility at the NPP, but extreme care should be exercised in executing such calculations in the distress of the severe accident at the site (see also # 13, ad 2).

Hence, off-site support should be organised that is available to any plant that is struck by a complex accident which may evolve into a severe accident. This support should be institutionalised, i.e. its organisation does not need to be set up on the spot - it is available and functional on demand.

It goes without saying that all parts of such an organisation must be trained well to make sure that it will function as required in a plant emergency, which includes that it will be timely available and functional.

12. IN-DEPTH TRAINING FOR ALL INVOLVED IN A HIGHLY STRESSFUL ENVIRONMENT.

Ultimately, all accident management is handled by people, in the organisational form designed for that purpose. People, however, are no machines: they may be subject to stress, fatigue, emotions, hope and despair. For example, plant operators that anticipate a large release will care primarily about their loved-ones, yet must operate according to their duties. Even the transition from EOPs to SAMG requires a major change in the mindset, as now it is no longer relevant to save the core but to save people, possibly at the cost of the plant.

I sometimes explain the transition from EOP to SAMG as the decision making on board of the RMS Titanic, on that cold night of 14-15 April 1912, now 100 years back.

The Titanic had compartments, which were isolated from each other (in the figure visible as the vertical lines up from the keel). Should a leakage in the hull occur, only one such compartment would be flooded, and the ship would stay afloat. The designer had gone far: even if four compartments would be flooded, the ship would still stay afloat.

Now when the ship approached the iceberg, the captain ordered to change direction: he wished to avoid a collision. This was his 'EOP' for such an event. However, the ship was already too close: collision was unavoidable. By still following his 'EOP', the captain hit the iceberg on the side of the hull and ripped open five of the ship's compartments. Hence, the ship was damaged beyond her design basis; she could not be saved and sank.

The proper action would have been to stay on navigation course, and *hit the iceberg head-on*. With decreased speed - as far as a ship of that size can decrease speed at such a short distance. This operation would have damaged the front compartment, possibly also the second compartment, but under such damage the ship would have stayed afloat. Of course, she would have been heavily damaged, possibly beyond repair.

Captain Smith should have realised that he already had left EOP-space, that he had entered SAMG-space,

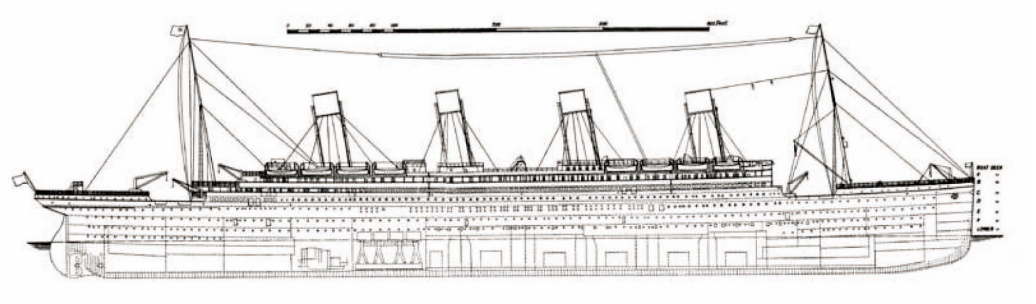

Fig. 1. RMS Titanic with Her Watertight Compartments

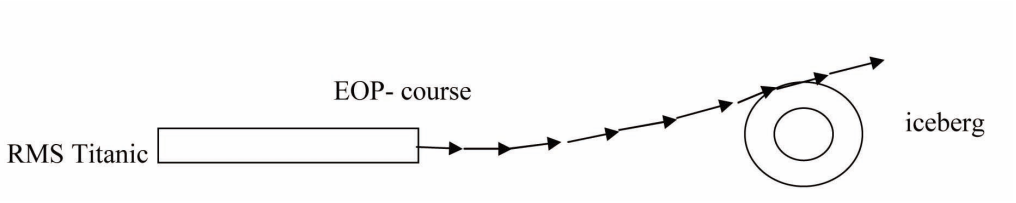

Fig. 2a. RMS Titanic on EOP Course, Trying to Avoid Collision, but Failing;
Ship will Sink Due to Large Opening in the Side

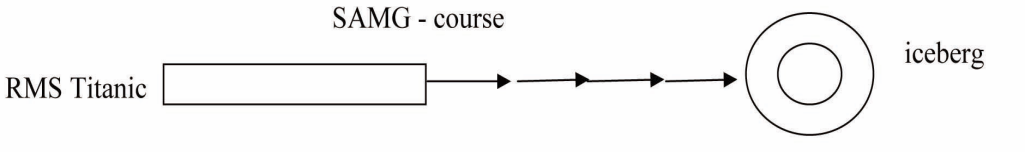

Fig. 2b. RMS Titanic on SAMG Course, Hitting Iceberg, but Limited Damage;
Ship Front Compartments Damaged, but She will Stay Afloat

and that his only duty now was to save people, possibly at the cost of his ship. Unfortunately, such thinking did not exist at that time, and the Titanic went down, at the cost of 1500 lives.

It is questionable whether the lessons of the Titanic have been learned at all: the Costa Concordia recently went down for exact the same reason: her captain Schettino should not have tried to avoid the rock, but to hit it head-on.

Neither the captain of the Titanic, Edward Smith, nor his successor at the Costa Concordia, Francesco Schettino, understood the difference between EOPs and SAMG, and the complex transition between the two. The consequences were tragic, in both cases.

I do not believe the captains should be blamed for this misunderstanding. The transition between EOPs and SAMG is a complex, dramatic, stressful event, a jump into the dark - at least, so it may look to many - to master a pending catastrophe. Such a transition is only possible if its meaning is well understood by those involved, and well trained, frequently, and in all earnest. Many plants, unfortunately, train their SAMG only occasionally, e.g. once in two, four, even six years. One cannot expect that such training is useful to master a catastrophe.

As was discussed in # 11, the proper handling of a severe accident may require a large organisation, with many people operating, in different settings. And this organisation should be in place and functional in a short time. Here also it should be understood that only appropriate training at appropriate intervals can make such an organisation work in a real event. If not, people may totally fail to perform their duties or even run away under the stressful environment, causing the organisation to collapse: only trained soldiers are able to fight.

13. FUTURE WORK IN EOP, SAMG, EDMG.

A number of items for future work in EOPs, SAMG and EDMG have been discussed in the previous sections. Major work on strengthening the safety of NPPs in extreme events has been initiated e.g. in the US,[11], in France, [12]. Work by these and other countries have been reported, for example, at the IAEA conference on Fukushima at the ministerial conference in Vienna, in June 2011, [13], and the workshop on lessons learned in Daejeon, Korea, November 2011, [14].

All plants in the EU have been subject to a 'stress test', as defined by ENSREG, [15]. The final report by the EU is expected in June 2012.

The IAEA has developed methods to test a plant's robustness for extreme events [16], [17], which are close to finalisation. As discussed, a 'stress test' is designed to investigate the robustness of a plant for events beyond its licensed design basis.

A number of items may warrant further attention in the matter of accident management, in arbitrary sequence:

1. Implementing SAMGs / EDMGs into the Probabilistic Safety Analysis (PSA); this will indicate whether indeed risk is reduced by applying the various accident management strategies. Part of this work will be the investigation of potential negative consequences of SAMG strategies. For example, considering bringing water onto the debris in the cavity floor may result in large pressure spikes in the containment, [18]. This may result in challenges to the containment integrity and, hence, to the consideration not to do this, or change the basic strategy to, for example, inject very gradually. It is important to consider the human actions, as the decision making can be quite complex. Overall, the inclusion of SAMG into the PSA may be a complex matter, for which industry standards at present do not give proper guidance.
2. As authorities in charge of measures to protect the public need insights on what is going on but even more, what is going to happen, notably in terms of releases, some form of predictive capability may be useful. Questions, for example, could be: how much time will elapse before there is a vessel melt-through, how will the pressure build-up in the containment evolve and in how much time can we expect a venting of the containment or a containment failure, if such venting does not exist or does not work? Tools to follow and predict upcoming events exist [19], [20], but probably need further predictive power and practical exercise.
3. Consideration of extreme events of all natures, both internal as well as external events, as a major lesson from Fukushima is that, despite a voluminous design basis, accidents can happen which were not foreseen. One could argue that the tsunami that had occurred was outside the design basis because of errors (which may be true), but the overall lesson is that events can occur, for whatever reason, that are outside the plant design basis. A corollary is that it is needed for all plants to again check the design basis - are events left out that, with present insights, should have been considered? This is a major check, as it should be done by all plants worldwide.
4. In conjunction with the preceding statement, all plants in the world should perform a 'stress test' to find their robustness against events exceeding the licensed design basis. By this check, we can obtain already quite some insights on how much safety margin is available, should an accident beyond the design basis at one of the plants or sites occur.
5. At present, there is a large scatter in EOPs, SAMG, EDMG. As the goals of plants' accident management tools are almost identical, it is amazing that so many different approaches exist. Hence, harmonisation and integration seem useful. Peer review of the approaches will be much more easy, as will be support by third parties in a real event. A worldwide harmonisation may be difficult to achieve, yet this is no reason not to start. Each method probably has its weak points and its strong points. By combining the strong points and avoiding the weak points, substantial progress may already be achieved. Key points may be:
   a. in EOP-domain: EOP-strategies should include all strategies available, including those in SAMG and EDMG;
   b. in SAMG-domain: a full and total priority for challenges to fission product boundaries should be defined, where possible including the chronology of such challenges, as plant operators and the TSC cannot do everything at the same time, neither are there resources for meeting all challenges at the same time.

Efforts of this type are already underway in the USA - more countries may follow.

14. CONCLUSIONS.

PSAs have made us believe that severe accidents are remote events, which one should not really expect to occur. However, within a time frame of 30 years, we have seen already three major accidents, two of which have resulted in large releases. In addition, there were a number of 'near misses'. We probably must reconsider some of our principal thinking on nuclear safety.

Accidents which involve melting of the core are no longer hypothetical accidents and, hence, must be considered in the design of NPPs. Either through a redefinition of the 'design basis accident', [2], or through new definitions, such as 'design extension conditions', [1]. The design features to cope with such accidents should be brought within regulatory oversight.

Safety classification should be extended so as to include equipment designed to mitigate beyond design and severe accident conditions. First steps have been made, in a draft IAEA guideline and some advanced NPP designs.

Severe accidents have the capability to disrupt societies, cause large-spread environmental damage and cause severe economic consequences. Hence, nuclear safety criteria should be extended to include criteria for such consequences. This should be an international effort, as damage to the environment and the economy crosses borders.

EOPs and SAMG must be extended considerably. The time frames available now in these procedures/ guidelines do not reflect the high stress condition and the large plant and/or area destruction that can go with these accidents. In many cases, EOPs and SAMG use the same equipment, which effectively decreases the possibilities of the operators, once they find their EOPs unable to control the event. Portable equipment should be available, stored elsewhere, and appropriate guidelines be made to use it. Loss of DC includes finding ways to read instruments without DC, and to operate valves manually, also from remote locations. Off-site support should also be organised, to help on a longer term.

Approaches in EOPs and SAMG vary widely - whereas their goals are identical. Efforts should be made (are underway in some countries) to harmonise approaches, which also will benefit peer review and actual support in emergencies.

The Technical Basis of the SAMG needs considerable improvement. It should include the spent fuel pool, plant shutdown states, multi-unit damage, and long mission times. Potential negative consequences of SAMG actions are often badly known - this needs an urgent improvement.

One should prepare the site for effective isolation from the groundwater, where this is used for drinking water and/or agricultural or industrial purposes.

The organisation around the mitigation of a severe accident needs a considerable upgrade: large site damage should be assumed, support by third parties (companies, army, other countries) must be well organised and possibly contracted, so that help is not dependent on good will but on well-defined obligations of all parties involved. Part of this organisation is the plant vendor, the EOP/SAMG vendor (if not the same as the plant vendor), a well-informed TSO, scientific institutes that possess knowledge about severe accidents.

Training emergencies both on-site and off-site is of utmost importance. SAMG is a different world than EOPs: the plant is lost, the only thing that counts is the protection of human life, the environment, the country's economy. This is a task that is beyond the scale of ordinary emergency duties. Without proper and well-trained organisations, this task is impossible to execute.

Plants need to be checked for their robustness worldwide, which includes the review of the adequacy of the design basis. Tests could be similar to the ENSREG tests, but also newer developments, such as the Design Safety Margin Evaluation methods of the IAEA, are suitable (advanced) methods.

REFERENCES

[1] "Safety of Nuclear Power Plants: Design", SSR 2/1, IAEA, Vienna, 2012 (replacing NS-R-1).

[2] Dr. Nils J. Diaz (former chairman USNRC), "Reflections on Fukushima", *19th International Conference on Nuclear Engineering (ICONE19)*, Osaka, Japan, October 24-25, 2011

[3] Oddbjörn Sandervåg, Wiktor Frid, "Swedish regulatory aspects on severe accident management implementation", *OECD Specialist Meeting on Severe Accident Management Implementation*, Niantic, CT, USA, June 1995

[4] Harri Tuomisto, "In Pursuit of Consistency and Completeness in the Severe Accident Assessment and Management", *OECD Specialist Meeting on Severe Accident Management Implementation*, Niantic, CT, USA, June 1995

[5] "GPR/RSK Proposal for a Common Safety Approach for Future Pressurised Water Reactors", Federal Agency for Radiation Protection (German: Bundesamt für Strahlenschutz), Salzgitter, Germany, May 1993.

[6] "Safety and Pressure Integrity Classification Criteria for Light Water Reactors", American National Standard, ANSI/ANS 98.14, 2011.

[7] "Safety Classification of Structures, Systems and Components in Nuclear Power Plants", Draft Safety Guide DS367, IAEA, Vienna, 2009.

[8] "B.5.b Phase 2 & 3 Submittal Guideline, Rev. 2", ERIN Engineering & Research, NEI 06-12, December 2006.

[9] Bill Borchardt, "USNRC Fukushima Lessons-Learned Actions", *IAEA International Experts Meeting on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima-Daiichi NPP*, IAEA Vienna, 19 - 22 March 2012.

[10] Caroline Lavarenne, "Main Conclusions of the French NPP Stress Tests, 'A Need for a Hardened Safety Core' ", *IAEA International Experts Meeting on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima-Daiichi NPP*, IAEA Vienna, 19 - 22 March 2012.

[11] "Recommendations for Enhancement of Reactor Safety, The USNRC Near-Term Task Force (NTTF) Review of Insights from the Fukushima-Daiichi Accident", USNRC, July 2011.

[12] Michel Vidard, "EdF Nuclear Fleet, Post-Fukushima Safety Assessments," *EdF, presentation to the meeting mentioned in ref. [14]*.

[13] IAEA Ministerial Conference, 20-24 June 2011, Vienna, Austria.

[14] "IAEA Consultant's Meeting on Updating Accident Management Guides on Safety Aspects of Lessons Learnt from Fukushima Accidents: Embedded Workshop on Harmonization and Integration between SAMG and EOP", *IAEA, 14-16 November 2011, Hotel Intercity (Spapia)*, Daejeon, Korea, Working Material, November 2011.

[15] "ENSREG Stress Test", www.ensreg.eu, May 2011.

[16] "External Event Design Safety Margin Evaluation Program", IAEA International Seismic Safety Centre, September 2011.

[17] M. El-Shanawany, I. Kuzmina, A. Lyubarskyi, "Systematic Assessment of Robustness of Nuclear Power Plants against the Impact of Extreme Events", *TSO Forum*, Vienna, Austria, 18-20 January 2012.

[18] R. J. Lutz, Jr. and M. A. Lucci, "Modelling Post-Core Damage Operator Actions in the PRA", *PSA'08 Conference*, Knoxville, TN, USA, September 2008.

[19] Marcel Slootman, "Use of the Software Module SPRINT in the Netherlands for the Prediction of the Source Term", *OECD ISAMM 2009*, Böttstein, Switzerland, 2009.

[20] Yong Man Song, "The Demonstrative Assessment of Possible Candidates for Controlling Containment Hydrogen and Fission Product Release in Korean PHWR Plant", *at workshop ref. [14]*.