

---

## Instrumentation Needs and Capabilities for Severe Accident Management

B. De Boeck\*  
M. Vidard\*\*  
J. Royen\*\*\*

\* AVN 148 Rue Walcourt B-1070 Brussels BELGIUM

\*\* EdF 12/14 Avenue Dutriévoz F-69628 Villeurbanne CEDEX FRANCE

\*\*\* NEA 12 Boulevard des Iles F-92130 Issy-les-Moulineaux FRANCE

---

**ABSTRACT:** This paper summarises the work performed over the last 12 years within the OECD/NEA Committee on the Safety of Nuclear Installations (CSNI) in the area of the instrumentation to manage severe accidents. One approach to the identification of the accident management information needs begins with high level safety objectives, and develops a structured method to correlate these safety objectives with specific accident management strategies. A second approach starts from what exists, and develops guidelines to use existing equipment to diagnose and manage beyond design conditions. The capacity of the instrumentation to supply the needed information is discussed, starting from the accident conditions and the instrument qualification testing, in order to assess the instrument performance beyond the design basis. Analyses have shown that instrumentation environmentally qualified for design basis accidents in a conservative way, exhibits important capabilities to remain operational in severe accident conditions, especially given the reduced accuracy needs. Important progress was achieved in the last twelve years in the understanding of the role of instrumentation in severe accident management. The instrumentation needs have been found to be lower than thought ten years ago, and the capabilities of existing instrumentation have been found to be higher. These findings have made severe accident management implementation easier and have increased the confidence in their effectiveness.

### 1 INTRODUCTION

No currently operating nuclear unit has been explicitly designed to withstand the loads resulting from accident sequences resulting in melting of a very significant portion of the core. As a consequence, instrumentation needs were defined based on what was deemed necessary to control the unit during normal operation and contemplated accident sequences. Detailed requirements for instrumentation were then established based on environmental conditions anticipated during accident sequences addressed in the design, estimation of additional conservatism deemed reasonable for assessing sensor robustness and information reliability, and a realistic understanding of the influence of aging. Though instrument failures could not be excluded, consequences were necessarily limited as adequate redundancy was provided by design for all information needed to adequately control the unit and bring it back to safe shutdown in case of accident could be assumed available.

However, though current plant designs are generally very robust, one cannot exclude that accident sequences involving significant melting of the core can happen. First estimates through risk studies reported in WASH-1400 showed that the risk of core-melt could not be ignored, and the TMI-2 accident in a first step, then Chernobyl confirmed this conclusion. These events gave impetus to the development of Severe Accident Management (SAM) programs, and, depending on analyses factoring the specifics of local regulations and plant designs, these programs were implemented either through better use of the capability of components and instrumentation, or through plant modifications allowing to cope with perceived vulnerabilities of units as built, and thus provide better resistance in case of challenges resulting from very degraded situations.

An essential component of SAM is the capability to assess the status of the plant. Information for this assessment can be derived from a number of sources, including the installed instrumentation system, the status (e.g. operability) of systems and components, condition (including failure) of components, sampling of liquid and gas streams, portable instrumentation, and other ad hoc measures to assess plant conditions.

In order to facilitate successful implementation of SAM goals, it is necessary to ensure that an adequate diagnostic capability exists in a severe accident environment to identify and assess the information needs of the operating staff (for the purpose of this discussion, “operating staff” refers to the plant operator, on-site support personnel, as well as off-site assistance) during a severe accident. It is important that this identification of the likely information needs be performed in a systematic and structured manner to ensure sufficient information is available to assess the plant status and to implement the appropriate accident management strategies.

## **2 DESIGN BASIS AND SEVERE ACCIDENTS**

Design Basis Accidents (DBAs) can be characterized by the existence of a path to success, i.e. there exist systems having adequate capability to control core reactivity, guarantee long-term decay heat removal from the core and to the environment, and maintain containment integrity. System actuation is made automatically upon reaching preliminary defined setpoints, and the operator is relied upon when the timeframe and conditions for performing actions provide enough confidence that human factors are not likely to introduce unacceptable risks.

Instrumentation needed for DBAs must be qualified to the most severe environmental conditions they could be exposed to during such accidents.

On the contrary, severe accidents are sequences in which at least one system needed for a path to success has completely failed. In the absence of mitigative action, core degradation is progressing, fission product release from the core increases, and, ultimately, containment integrity could be threatened.

To derive strategies for mitigating the consequences of severe accidents, the following must be considered:

- even though at least one safety-grade system needs to be assumed inoperable, there is still a possibility to recover partial or full system capability at some time into the accident. If system actuation is contemplated after recovery, and depends on physical conditions inside containment, there should exist sensors with adequate capabilities to show that

- there is a reasonable chance they will still operate when needed.
- safety functions can also be fulfilled by non safety-grade systems. So, it is important to have adequate monitoring of the status of these systems in case of accident, their actual storage capability, and know how they can be used, even when such use seems unconventional (e.g., systems normally injecting into the RCS could be used to inject directly into the containment through system realignments, or fire water systems could be used to refill steam generators when needed).
  - most contemplated mitigative actions also have detrimental effects. For example, water injection could, in some cases result in increased hydrogen generation or very energetic metal-water interaction. So, it is essential to have a reasonable understanding of potential risks and benefits before making decisions on strategies and decide whether instrumentation is needed to accommodate these risks.
  - system recovery and actuation could also have, at least temporarily, consequences which could be confusing to operators. For example, water injection on a molten corium will result in steaming, at least in the short-term, and thus pressure increase in the RCS or the containment. If such effects can be detected in case of accident, assessing the need for operator awareness should be advised.
  - once the core has started to melt, assessment of core degradation is difficult, even if one assumes that instrumentation is still available. Determining real plant status through the sparse information available is not a trivial task, and trying to extrapolate plant evolution to calibrate sophisticated strategies could be misleading considering possible bifurcations.
  - at last, unconventional actions such as RCS depressurization in PWRs, containment venting or containment flooding could well be found appropriate either to stabilize accident progression, or buy time for system recovery.

### **3 CRITICAL DECISIONS IN SAM AND INSTRUMENTATION**

For SAM, decisions unconventional compared to that made for normal accident management are often contemplated either to reach a new plant state where safety functions can adequately be fulfilled, or limit the consequences of accident progression. These unconventional or critical decision SAM are:

- adding water to a degraded core,
- depressurizing the Reactor Coolant System (PWRs),
- spray or inject water into containment,
- actuation of hydrogen mitigative measures,
- actuate fan coolers for containment cooling,
- vent containment volume.

If one tries to analyse on which basis these critical decisions are made and which kind of information is needed for SAM, the following can be said.

#### **3.1 Adding water to a degraded core**

When the situation starts to degrade, but the core has not started to melt, priority is generally given to core-melt prevention. Water injection is then recommended in all cases, even when the situation is considered beyond design. For this phase, it is interesting to have information on core exit

temperatures or reactor vessel water inventory to evaluate whether cooling strategies are effective or if full system capabilities are needed. Instrumentation qualified for DBAs, such as core exit temperatures or the reactor vessel level instrumentation system is sufficient for this phase.

When the core starts melting, priority should be given to stopping or limiting accident progression. Injecting water is recommended. However, injecting water on a degraded core can have drawbacks, and these drawbacks need to be analyzed before making a decision. Injection of large quantities of water would result in steaming, but would not likely lead to RCS overpressure. At lower injection rates, quenching would be slower and more hydrogen would be produced, but scrubbing of volatile fission products would be increased. In both cases, water injection is beneficial. No additional information is needed for making decisions, though core exit temperatures and reactor water level are useful and redundant information to monitor plant degradation. There could be doubts, in BWRs, in case the reactor has not been scrammed or control rod materials have molten. Even in this case, no specific requirement would be needed as otherwise available instrumentation would allow to detect the problem before the core starts melting.

In case of more degraded conditions, water injection is the only way of stopping or limiting accident progression though satisfactory cooling cannot be guaranteed, and is beneficial for scrubbing fission products. Detrimental effects such as containment pressurization due to steaming or energetic interaction between water and corium cannot be excluded but it appears that potential benefits of injecting water exceed by far detrimental effects and is recommended in all cases.

### **3.2 Depressurizing the Reactor Coolant System**

RCS depressurization is contemplated to allow injection from system operating at intermediate or low pressure or prevent reactor vessel failure at high pressure. When direct depressurization is contemplated, the negative side is the increase of the rate at which fission products and hydrogen are released to the containment, or the increased potential for energetic fuel-coolant interaction. However, the former only affects release timing, and the latter is of sufficiently low likelihood to be neglected. Core outlet temperatures are generally used to decide RCS depressurization, and thresholds are generally below temperatures contemplated during DBAs. No additional constraint is identified.

When depressurization is contemplated through the steam generators, potential concerns are steam generator tube integrity or fission product release to the environment in case of primary to secondary leak. Steam generator parameters such as pressure, activity in secondary water, water level, or RCS pressure could be contemplated for decision making. Depending on the perspective adopted for SAM, information qualified for DBAs, or assessment of instrumentation survival under severe accident environmental conditions could be contemplated. The former would correspond to a situation where information, when lost, is frozen on a "fail-safe" basis, while the latter would be adopted in an approach where continuous monitoring is felt needed for the entire duration of the accident.

### **3.3 Spray or inject water into containment**

Spray system actuation has the potential for decreasing pressure inside containment through steam condensation and scrubbing fission products from the containment atmosphere. In some cases,

they could also provide, through redistribution of water inside containment, a very effective source for cooling the reactor vessel from outside and thus delay or prevent vessel failure. Negative effects could be containment de-inertization and increased flammability of combustible gases. It must be noted however that in large dry containment, containment atmosphere de-inertization is rather slow and that if igniters, when installed, are actuated together with spray, hydrogen burning should be smooth and pressure increase inside containment limited.

### **3.4 Operation of igniters or hydrogen recombiners**

Two types of problems can be considered depending on whether passive (e.g. autocatalytic recombiners) or active devices are used. For the former, the critical decision has been made at the design stage. Once installed, no operator action is possible, and hydrogen is eliminated depending on physical conditions in the vicinity of the PAR only. No instrumentation is actually needed. When monitoring hydrogen concentration for information purposes is found of interest, sensors should be qualified for severe accident environmental conditions. This, however, doesn't bring any additional information in term of risk during SAM (risk have necessarily be found negligible at the design level). For the latter, the problem could be system actuation under burnable or detonable conditions. If the risk is found non negligible, hydrogen concentration monitoring should be provided, and survivability under severe accident conditions assessed.

### **3.5 Actuate fan coolers for containment cooling**

Fan cooler operation will mix containment atmosphere and should prevent build-up of localized pockets of combustible gases. Detrimental effects could be containment de-inertization or providing ignition sources for combustible gases. Not all plants are equipped with safety-grade fan coolers. For those with no qualified fan coolers, operation in the course of severe accidents could provide a path to the environment, and actuation is generally not recommended. For those with safety-grade components, actuation happens upon reaching a containment pressure setpoint well before reaching the onset of core melt. If for some reason, actuation were contemplated after significant core degradation, pressure sensor survivability should be assessed for severe accident environment. If consideration of risk resulting from combustible gas flammability were raised, a similar conclusion would apply.

### **3.6 Vent containment volume**

Venting is considered when containment pressure is increasing to the point where containment integrity could be challenged. Such challenge is resulting from combustible gases generated by steam-metal or molten core concrete interaction as well as decay heat release to the containment. Venting actuation is made well into the accident, when containment conditions are beyond that contemplated for a DBA (i.e. with the safety injection available). As venting is generally decided based on containment pressure, pressure sensors should be shown reliable for conditions prevailing at system actuation. Depending on qualification profiles, further investigation allowing to assess survivability could be needed. If other parameters need to be controlled to prevent system deterioration in case of actuation, similar conclusions would apply.

## 4 ACCIDENT MANAGEMENT INFORMATION NEEDS

A systematic assessment of accident management information needs can be approached in a number of ways. Two different approaches have been suggested in the past. One is a “top down” approach of beginning with high level safety objectives, and developing a structured method to correlate these safety objectives with specific accident management strategies, thereby providing a systematic check on the plant staff’s information needs. A second systematic approach is more like a “bottom up” method, starting from what is existing, and devising guidelines to use existing equipment to diagnose and manage beyond design conditions.

Within the subject area of instrumentation, a systematic approach to assess the adequacy of instrumentation for accident management requires: (1) the specification of the information needs of the plant personnel during a wide range of accident conditions; (2) the compilation of the existing plant measurements capable of supplying these information needs; (3) knowledge of the limitations of hardware under the conditions of a wide range of accidents (in particular the harsh environment associated with severe accidents), or areas in which the information systems could mislead plant personnel; and (4) what, if any, additions to instrument and display systems would be necessary to facilitate effective accident management.

The following sections briefly describe the application of two of the above-mentioned systematic approaches to information needs and instrumentation for accident management.

### 4.1 Top down approach

This methodology was developed by the Idaho National Engineering Laboratory [5]. The first step of this approach identifies the relationships between the high level safety objectives, that have been identified for severe accident management, and the potential strategies for fulfilling these objectives. The second step uses these relationships to identify the information needed by the operating personnel to understand what objectives are not being met and what strategies may be effective in mitigating any challenges to these objectives. The final step examines the capability of existing or proposed measurements to supply these information needs.

This approach is based on the observation of a hierarchical structure between safety objectives and accident management strategies. In order to maintain the safety objectives, certain critical plant safety functions must be upheld. An accident will present challenges to these safety functions. These challenges may be caused by different physical and chemical mechanisms which, if unattended, have the potential to defeat the safety function. The technical support and plant operations staffs then identify and implement various strategies for dealing with the mechanisms which present challenges to the safety functions.

The operating staff thus fulfils its role to maintain the safety objectives by:

1. monitoring the status of the safety functions;
2. detecting challenges to the safety functions;
3. identifying, if possible, the symptoms of the mechanisms which could be causing the safety function challenges;
4. selecting and implementing strategies for maintaining or restoring challenged safety functions;
5. monitoring the performance of the strategies to determine if they are having the desired effects in maintaining or restoring the safety functions.

The application of this methodology for the evaluation of information needs and the corresponding instrumentation requirements must consider the severe accident environment experienced during various specific accident sequences. During the accident sequence, this environment will undergo significant changes. To obtain an accurate assessment of the instrumentation needs and challenges during the sequence, it is necessary to consider the full range of environmental conditions. This is facilitated by the consideration of distinct accident phases. For example, the conditions of a severe accident initiated by a Loss-of-Coolant Accident (LOCA) could be characterized as a blowdown phase, a fuel heat-up and degradation phase, a core-concrete interaction phase following vessel melt-through, and finally a release phase following containment failure. Although it is recognized that the objective of accident management during each phase is the interdiction of further degradation, and hence termination of the accident before it degrades to the next phase, accident management capabilities must be assessed for each physically possible stage of the accident.

The application of a systematic examination of information needs and sources for severe accident management will result in a comprehensive assessment of plant instrumentation (and other sources of information) availability. Independent of the method employed, this assessment is made by matching the information needs developed from a systematic, structured method with the inventory of available information sources during the various phases of a severe accident sequence.

## **4.2 Bottom up approach**

This methodology, developed by EPRI for NUMARC, starts with the compilation of all available accident management capabilities. This inventory is not restricted to hardware, in recognition that accident management involves information resources and personnel resources, as well as systems and hardware. The capabilities compiled in this manner are then tested against the major phases of representative accident sequences. This approach envisions the availability of plant-specific compilations of severe accident sequences, usually resulting from the PSA. Any gaps identified in the process of matching capabilities to the challenges identified by plant-specific risk-dominant accident sequences identify specific opportunities for improvements in the plant's accident management capabilities.

### *4.2.1 Compiling accident management capabilities*

A major element of this systematic approach to accident management is the assessment of existing accident management capabilities. The methodology suggests that this step be accomplished through a structured series of questions. In recognition that accident management should not focus exclusively on hardware, the questions address personnel resources (e.g. organisation, training, communication) and information resources (procedures, technical guidance, process information), as well as systems and equipment (e.g. available instrumentation, repair and restoration capabilities, use of alternatives).

In the consideration of available instrumentation, the evaluation process includes the consideration of the severe accident environment, and its effect on the functioning of the instrumentation. Enhancements to existing capabilities considered in this step would include identification of measures to interpret readings outside the range of the instrument, or the use of process signals not intended by their design, which could provide information on the progress of a severe accident.

#### 4.2.2 Defining and grouping accident sequences

The primary source for the definition of accident sequences is the PSA. For the purpose of this evaluation process, the set of plant-specific accident sequences can be simplified by grouping of accident sequences by:

1. a general category for the initiating event,
2. the system level function(s) whose failures lead to core damage,
3. the status of the systems for containment heat removal,
4. the status of containment integrity prior to onset of core melt,
5. the timing of the accident, including the timing of failures.

Grouping accident sequences by these characteristics will result in a reduction of the large number of accident sequences typically resulting from probabilistic safety assessments into a relatively small group of categories of sequences.

For each group, a representative sequence, and the major phases of the representative accident sequence are then identified. The phases are selected such that specific interventions (e.g. restoration of a safety function) can be identified for each phase. For a station blackout sequence (loss of off-site and on-site AC power with failure to restore power prior to battery depletion), for example, the accident phases could be defined by the opportunities to interrupt the sequence as follows:

1. Avoiding interruption of core cooling, or restoring core cooling prior to core damage
2. Restoring core cooling prior to vessel breach
3. Establishing cooling of the core debris after vessel breach
4. Restoring systems to prevent containment failure
5. Taking measures to limit fission product release

At this point the methodology provides a sufficiently defined structure for comparing the accident management capabilities to the challenges presented in each of the progressively more severe phases of the representative sequences. At each step, the objective of the process is to find ways to use the identified accident management capabilities to prevent further degradation of the sequence. This process affords the opportunity to evaluate the information needs, as well as the anticipated performance of available instrumentation in the environment characteristic of each phase of the sequence.

#### 4.3 Results of information need assessments

The results of the application of a systematic assessment of the information needs and instrumentation availability, discussed above, will differ from one plant type to another, as well as for the various accident management approaches used in different countries. The development of strategies to deal with various severe accident conditions alone is not sufficient if there is inadequate information to indicate the need for, the appropriate timing, and the observation of success of the strategy. A systematic evaluation process can identify specific information needs for accident management. Such a structured approach will permit the necessary prior planning to ensure alternate methods for obtaining the requisite information to ensure successful implementation of mitigation strategies.

## 5 INSTRUMENTATION CAPABILITIES

### 5.1 Accidental conditions

Beyond the information which is needed for automatic actuation of safety systems, instrumentation which is needed for accident management includes parameters [1]:

- needed by control room operators to perform manual actions allowing safety systems to accomplish their intended function;
- providing information on whether safety functions are fulfilled;
- allowing to evaluate whether fission product barriers are breached or likely to be breached;
- providing information on operation of safety systems or systems important to safety;
- which could be used for evaluating the magnitude of fission product release.

Some of these parameters are design specific, while others can be considered as more generic. Examples of such more generic parameters can be found in [1] for BWRs as well as PWRs, together with the ranges in which they are expected to operate. For example, maximum RCS pressure and temperature in PWRs are expected to be 209 bars and 370°C respectively, while maximum core exit temperature could be as high as 1260°C.

For primary systems parameters, it seems that, though there could be minor differences in expected ranges, the approach is basically the same in most countries and considers DBAs, in particular LOCA, for defining maximum anticipated values.

For containment or system parameters, however, there could be differences based on whether the limiting accident is a LOCA with satisfactory operation of the safety injection system, or a LOCA leading to a core melt situation due to the failure of the safety injection system. For the former, fission product release to the containment is considered moderate (generally part or whole of the gap inventory), and hydrogen generation is a slow process resulting in limited concentration in the containment atmosphere. For the latter, on the contrary, fission product release to the containment is much higher, sometimes tens of percent of total core inventory for some isotopes, and hydrogen generation can be fast and significant, potentially leading to detonable concentrations. This obviously affects environmental radiation conditions inside containment and for systems recirculating contaminated water outside the containment building, and the range of values the instrumentation is expected to measure.

It seems that there could be significant differences when considering instrumentation capabilities in case of severe accident. In fact, one could argue that there is virtually no difference, except for hydrogen monitoring, because most instrumentation needed for severe accident management is used early into the accident considering the timeframe needed for having very high integrated doses. Similarly, when it comes to pressure or temperature conditions, they are not likely to significantly differ from DBA conditions except when hydrogen burning is considered. The case could be different for components having to continuously operate in a post-accident situation.

## 5.2 Instrument qualification testing

Most instrumentation trip functions occur early enough in the accident sequence so that the harsh environments associated with the conditions calling for accident management in the containment have not yet developed. Thus the qualification of existing plant instrumentation should be sufficient, i.e. bounded by the design basis. In contrast, instrumentation required for accident management is likely to experience conditions more severe than those corresponding to design basis accidents.

Equipment qualification (EQ) testing is needed to demonstrate that safety equipment will remain functional in the environment caused by the design basis event which requires its functioning. Post-accident monitoring equipment (which includes instrumentation useful for accident management in the containment), typically is qualified, by testing, to the design basis loss-of-coolant accident conditions. While each plant has its own accident profile, typical conditions for a PWR are:

Peak Temperature	-	150 °C
Peak Pressure	-	5 bar
Radiation dose	-	70 - 200 Mrad

The conditions for EQ testing are typically assumed to arise very quickly, and to remain for extended periods of time (up to one year). This extended time period may provide some of the margin which may be useful in severe accident situations. In particular, it has been shown that the containment environment for the first hour of a severe accident is not likely to exceed the EQ test levels [12]. Moreover, a best estimate judgement shows that an adequate margin of instrument performance exists for at least 24 hours for the less severe accidents and 2 to 3 hours into even the most severe accident (TMLB for a generic PWR).

## 5.3 Instrument performance beyond the design basis

The significance of design basis equipment qualification with respect to risk significance in severe accident conditions has been investigated by Sandia National Laboratories (SNL) [4]. This study investigated the potential for extrapolating equipment reliabilities for severe accident environments from environmental qualification testing for severe accident conditions, as well as the degree to which such information might affect the results of PSAs. With respect to the typical assumptions made for design basis equipment qualification the study found that:

- PSAs typically model equipment performance for the first 24 to 48 hours, while some safety-related equipment is qualified for a month to one year following the accident. Manufacturers of cables, for example, have exposed their cables to accident conditions for time periods of 180 days to one year.
- EQ research suggests that performing simultaneous (versus sequential) accident simulations of radiation, steam, and chemical spray environments is not important.
- Oxygen within the test chamber has been demonstrated to accelerate accident degradation of polymer materials; however EQ research has not demonstrated an early accident functional performance impact from this issue.
- Beta radiation dose can be simulated by gamma irradiations. Using gamma emitters to simulate exposure to beta radiation levels defined in NUREG/CR-5175 [3] is conservative; moreover, accident sequences of PSA interest do not produce a need to demonstrate long term radiation survivability.

The study examined the operator's reliance on instrumentation for a few severe accident sequences

with sufficient detail to develop some bounding risk importance estimates. For steam generator level transmitters, for example, SNL noted that PSAs typically do not model the transmitter's harsh environment in determining the auxiliary feedwater system reliability. Moreover, auxiliary feedwater is usually calculated to have quite high reliability. While there is substantial redundancy for the steam generator level transmitters, poor moisture sealing, use of terminal blocks, degraded electrical penetration seals, or presence of degraded transmitter o-rings may produce a common-cause susceptibility to moisture degradation.

Examination of the severe accident utility of the high range radiation monitors suggest that this instrument is an important indication to the operator that core melt is occurring. Hence, reliable operation may be important for accident management in containment. The performance of this instrument has been established by EQ tests [2]. SNL noted that at the time of core melting containment pressure, temperature, and radiation level are within typical qualification parameters. However, within this design basis it was found important (as confirmed by the TMI-2 experience) to maintain proper sealing against moisture intrusion to ensure meaningful output from this sensor.

With respect to consideration of the harsh severe accident environment in the evaluation of equipment reliability in probabilistic safety studies, SNL notes that PSAs rarely account for equipment reliabilities during accidents that differ from normal operation reliabilities. In some cases, however, EQ research has provided evidence to the contrary. PSAs typically provide only limited modelling of post core melt accident management strategies, and generally do not model plant status instrumentation. The development of post core damage accident management strategies may necessitate changes in PRAs and equipment qualification or survivability programs.

## **5.4 Signal validation**

Signal validation techniques are one way to ascertain the availability of specific instrumentation [12]. The basis of signal validation for accident management is the use of redundant measurements or the creation of analytical redundancy. In severe accidents, time is important, thus suitable validation methods must detect developing incipient faults and reveal which measurement is faulty, to avoid initiation of incorrect measures to handle the accident. The methods must be robust to signal noise and to abnormal dynamics due to the accident.

Advanced validation methods make use of mathematical models of the system. The system is defined by its parameters, the initial state, and the actual inputs and outputs of interest, which also exist as measured values. Model-based methods require some kind of evaluation of the nominal input-output relations of the system which causes the residuals to deviate from the initial value (normally zero) in case of a fault. Using appropriate functions, decision logic is created which monitors the time of occurrence and identifies the faulty signal or measurement.

Even more advanced validation methods have been proposed. The Halden Reactor Project for example has been studying the use of artificial neural networks and of fuzzy logic to this aim [13]. Such techniques look very promising, but important problems remain to be solved like their qualification and the formal proof of their reliability [14].

## 5.5 Other approaches to information needs

Qualifying instruments to survive the severe accident environment is by no means the only method to satisfy the information needs for successful accident management. Useful information can be extracted from instruments and other equipment in a degraded, or even failed condition, from the collective status of systems (e.g. the observation of which systems have failed and which are still functioning, from temporary or portable equipment, and from direct observations).

An example of such unusual sources of information is the behaviour of ex-vessel neutron detectors at TMI-2. These detectors showed large fluctuations in neutron flux during the core damage phase of the accident. Although unexplained at the time of the accident, later analysis indicated that the measured fluctuations could be correlated with the back-calculated water level in the reactor vessel. The increased neutron flux recorded by the instruments indicated that water level had fallen below the level of the instrument's field of view.

For accident management information concerning the containment, several parameters which could be measured, perhaps with portable instrumentation systems are radiation levels, radioisotope mix, containment structural strain, continuity and strain of reinforcing steel, and temperatures of penetrations. During the TMI-2 accident, an estimate of the dose rate on the containment dome was obtained from a volunteer who scaled the exterior of the containment and obtained a "contact" dose rate on the outside of the containment dome. This information confirmed that the radiation monitor installed on the inside was in fact saturated. (The saturation characteristics of the installed instrument had resulted in a return of the needle to the "O" position following an off-scale reading). The concept of external gamma spectroscopy has been discussed as a potentially valuable source of information concerning the radionuclide mix, which, in turn, could provide an indication of the temperatures reached by the fuel.

Such unorthodox sources of information are not useful in accident management, of course, if they cannot be explained at the time of their occurrence, as was the case with the TMI-2 neutron monitors. If this type of information is to be useful in accident management, it is necessary to examine such "creative" sources of information beforehand, and to develop the necessary aids to their interpretation.

## 5.6 Research needs

The information needs and capabilities during a severe accident, as discussed here above, suggest that the information sources available to the operating crew could be enhanced by research in the areas of:

- assessment of instrument response beyond their design bases (including signal validation);
- computational aids to provide the needed information which is unavailable during a severe accident sequence due to support system failures, instrument inaccuracy, or unavailability;
- investigation of alternative sources of information to provide sources of information not currently tapped for accident management purposes.

## 6 INSTRUMENTATION ASPECTS OF SAM IMPLEMENTATION

Severe accident management programmes were developed and implemented in most countries during the late eighties and the nineties. In 1995, a CSNI Specialist Meeting reviewed the progress made [9]. From the presentations provided during that meeting, it was apparent that the development of SAM programmes in different countries is highly influenced by the general expectations set at the national level for such programmes [10].

In some countries, risk reduction through SAM programmes is pursued by simply applying existing equipment and instrumentation when developing SAM guidelines and procedures. Minor equipment modifications for SAM are made whenever they are cost-effective in facilitating the plant staff to apply procedures. Major plant modifications have been implemented over the past several years but were generally focused on prevention of core damage, rather than management of a damaged core in vessel or in containment.

In other countries instead, SAM is considered a basis of design by requiring that certain severe accident safety goals and release limits have to be met. This approach can lead to major plant modifications that are needed for ensuring a SAM safety goal. Some other countries have chosen to combine features of both these approaches.

The progress made in this field was again reviewed and discussed during a CSNI workshop in 2001 [18]. The overall picture is that SAM implementation made remarkable progress since the 1995 meeting. SAM has been implemented in various ways in many plants, but not yet in all plants. A systematic approach, which is based upon a clearly defined decision-making process, is one of the features implemented in many cases. Available means are determined and priorities are set. This approach is made up of strategies intended to become an optimum approach to prevent or mitigate the consequences of beyond-design basis accidents. It is based upon a prepared information package about plant-specific behaviour to be expected in beyond-design scenarios [19].

The approaches followed in the different countries do not fit one single pattern. Harmonisation, to the extent it is desirable, does not seem feasible at this stage. As a rule, the responsibility of the plant owner for the safety of his plant remains untouched. Also, safety goals may vary between countries.

The prevention of severe accidents should normally receive the first priority. When this is done successfully, the probability of a core melt becomes very small. It is then difficult to justify costly additional measures. A pragmatic approach for existing plants is therefore to start from the plant "as is" and to give guidance to the operators in order to help them manage core melt accidents with existing equipment. This is for example the approach followed by the Westinghouse Owners Group (WOG) in developing Severe Accident Management Guidance (SAMG) that would be generically applicable to the majority of PWR plants employing a Westinghouse Nuclear Steam Supply System [9]. One of the ground rules was that no new equipment (or instrumentation) was to be considered.

Although some modifications to the plant make technical sense for severe accidents, a cost-benefit evaluation concludes that the costs far outweigh the benefits for these low probability core damage events. Thus, if equipment or instrumentation might not be available when needed, an alternate method was developed. In particular the issue of instrumentation survivability was addressed in the WOG SAMG by specifying that multiple means of measuring the key parameters should be used in the diagnosis process:

- several different instruments can provide key parameters,
- several different instruments can confirm primary instrument,
- graphical computation aids are provided for some parameters.

It is worthwhile to note that the equipment qualification envelope for pressure, temperature and radiation is not exceeded for most severe accident sequences. Thus, the available instrumentation should be useful in diagnosing severe accident conditions. However, verification of the indicated conditions using diverse instrumentation indications is strongly advised. Moreover, it may be necessary to assess, on a plant specific basis, the availability and capability of instrumentation for use beyond the design basis.

The WOG SAMGs were implemented at the Tihange nuclear power plant in Belgium [15]. The plant-specific implementation of the WOG SAMGs involves an extensive adaptation of the generic guidance, regarding both its form and its content, in order to obtain a set of guidelines which fully takes into account plant-specific features and which is easily integrated into the plant's operational practice. Since the Tihange NPP already features a limited vulnerability to severe accidents, due to a combination of conservative design, post-TMI measures and accident mitigation oriented plant back-fits (such as auto-catalytic hydrogen recombiners), the implementation of the SAMGs has been strictly limited to the use of existing equipment and instrumentation. In general, considerations of risk-relevance and implementation feasibility have led to several modifications to the strategies appearing in the WOG SAMGs. Nevertheless, the SAMG implementation at Tihange does fully maintain the structure and the key features of the WOG SAMGs, and thus constitutes a coherent and complete approach to accident management.

Of particular importance is the installation of passive auto-catalytic hydrogen recombiners, designed to limit the hydrogen concentration in containment under severe accident conditions to a maximum value of 5%. With properly designed and well-qualified hydrogen recombiners, the hydrogen issue becomes irrelevant to the overall risk. Moreover, since these hydrogen recombiners are entirely passive and do not require operator actions, a significant simplification of the hydrogen management strategies could be achieved, as well as a simplification in the strategies requiring the use of containment sprays, which in the absence of recombiners, induces the potential for containment de-inertisation.

As a result, it was found that the remaining instrumentation needs were rather limited. Only the following key parameters were found to be necessary to drive the application of the SAMGs at Tihange:

- core exit temperature
- pressure in the primary circuit
- water level in the steam generators
- containment pressure
- water level in the containment sumps
- radiation level at various locations

The available redundancies and alternate ways to obtain those key parameters were identified. It was also verified that the ultimate limits for the use of the available instrumentation (accident environmental conditions, measuring range and precision, risk of being flooded) were compatible with their use within the SAM strategy.

The experience obtained at Tihange confirms a general observation made while developing and implementing severe accident management plans: although severe accidents involve complex phenomena, severe accident management can be formulated in terms of a small number of critical decisions, relying on a small number of key parameters. For instance, it is generally agreed that, when it is available, water ought to be added to a degrading core since the advantages outweigh potential disadvantages [11]. The onset of core degradation can be detected by a small number of instruments.

## **7 ARE THERE OTHER NEEDS?**

From a technical standpoint, it seems possible to deal with all credible severe accident sequences based on very limited information and a system action matrix. However, adequate crisis management needs at least rough information on system status (e.g. inventory in storage tanks) to decide whether contemplated actions have a reasonable chance to be successful, and, when operator intervention is needed, on environmental conditions in buildings (e.g. radiation monitoring) to make sure these interventions wouldn't be harmful for operators. Sensors which would be needed for assessing such conditions should also exhibit adequate reliability for the kind of environment they would be exposed to.

At last, utilities and safety authorities are not the only players in case of emergency, as there is a need to feed information to civil authorities, the media and the public. The last two are of significant importance as, confronted to a technology they don't know, the risks of which they cannot actually evaluate, they could well want to have confirmation of real plant status in addition to prognosis on plant evolution however accurate this information could be. For this purpose, information of interest could be, for example:

- rough estimate of core degradation (is the core still inside vessel?);
- is there a risk of catastrophic containment failure?

The former could be addressed partly through using temperature detectors in the reactor cavity, while the latter, which is essentially related to hydrogen flammability, measuring hydrogen concentration, or indicating that mitigative systems have been actuated could provide adequate answers.

## **8 SUMMARY AND RECOMMENDATIONS OF THE 1992 SPECIALIST MEETING**

The First CSNI Specialist Meeting on Instrumentation to Manage Severe Accidents was held at Cologne, Germany on 16th and 17th March 1992 [7]. It was hosted by GRS. The Specialist Meeting concentrated on existing instrumentation and its possible use under severe accident conditions; it also examined developments underway and planned. Desirable new instrumentation was discussed briefly. The interactions and discussions during the sessions were helpful to bring different perspectives to bear, thus sharpening the thinking of all. Questions were raised concerning the long-term viability of current (or added) instrumentation.

It must be realized that the subject of instrumentation to manage severe accidents was very new in the early nineties, and that no international meeting on this topic was held previously. One of the objectives was to bring this important issue to the attention of both safety authorities and experts. It could be seen from several of the presentations and from the discussions that this kind of work was still in a planning phase.

The following conclusions and recommendations [8] were therefore seen as preliminary:

1. To make decisions which are appropriate and effective to control and mitigate an accident, it is essential to have the clearest picture possible of the accident and its progress. This can be obtained by accumulating information from as many sources as is practical.
2. It is important to use a systematic approach to evaluate accident sequences, information needs and instrument capabilities in severe accident conditions.
3. It should be confirmed that instrument performance will be sufficient to give the information needed to manage a severe accident. In some cases the instruments may function beyond their specification range.
4. Important lessons can be learned from the TMI-2 and LOFT-FP-2 measurements, in particular for instruments giving new information (e.g. source range monitor information about vessel water level).
5. All participants agreed on using the full instrumentation and accident management capacity of the plants. All were focusing on making full use of post-TMI-2 safety enhancements and instrumentation additions already in place.
6. Most participants agreed on the types of measurements which will prove useful. Various means are being pursued to think ahead and interpret plant status, such as computer codes and calculational tools.
7. An important conclusion is that there is a need for additional work on unconventional use of existing instrumentation under severe accident conditions.
8. This work should identify areas where existing instrumentation can indirectly contribute to the information needs in severe accident situations and areas where it cannot, thereby giving indications on desirable new developments.
9. The question of new accident management instrumentation was raised. The current perspectives were based on national objectives, and depended on the optimism or pessimism of the participants over the longer term viability of instruments. It was clear that efforts to ensure the long-term viability of instruments were being pursued by all (with a reasonable "common sense" attitude). In fact, the pessimistic view is "conservative" and leads planners to make prudent provisions to manage the accident with any instruments that may be available.
10. Some new instruments are being developed; their possible usefulness under severe accident conditions needs to be further qualified.
11. In spite of differences in purpose, some instruments used in experiments can be evaluated and qualified also for current nuclear power plants.
12. The papers presented at this meeting clearly showed that most approaches to expert systems were still in a conceptual phase. Some applications transferred from other fields were under development for use in the severe accident domain. Only those system that offer a set of less sophisticated tools could be said to be readily available for limited purposes.
13. Expert systems may be of help to plant staff and external experts, but cannot substitute for them.
14. There will not be a single expert system for severe accidents (i.e. a general problem solver) but rather a set of simpler systems devoted to specific goals in situations that can be clearly identified.
15. Expert systems should have the capability to verify plant conditions and assumptions made by the operating personnel.
16. Expert systems used in this domain must be even more explanatory and transparent to permit verification of their conclusions by the personnel.
17. Expert system should, if possible, also be used during normal plant situations to increase operating personnel confidence.

## **9 SUMMARY AND CONCLUSIONS OF THE 2001 WORKSHOP**

The CSNI Workshop on Severe Accident Management - Operator Training and Instrumentation Capabilities to was held in Lyon on 12th to 14th March 2001 [16]. It was hosted by EDF. Basically, the workshop was a follow-up to the 1997 Second Specialist Meeting on Operator Aids for Severe Accident Management (SAMOA-2) [13] and [14] and to the 1992 Specialist Meeting on Instrumentation to Manage Severe Accidents [7] and [8].

The meeting confirmed [17] that only limited information is needed for making required decisions for SAM. In most cases existing instrumentation should be able to provide usable information. Additional instrumentation requirements may arise from particular accident management measures implemented in some plants. In any case, depending on the time frame where the instrumentation should be relied upon, it should be assessed whether it is likely to survive the harsh environmental conditions it will be exposed to.

There was general agreement that instrumentation for SAM should be as simple and straightforward as possible, due to limitations on power availability under severe accident conditions and ability of operators to assimilate and use information. Some SAMGs rely on adaptation of existing design basis instrumentation to meet SAM needs. Other SAMGs introduce new instrumentation for SAM needs for particular plants. There is a conflicting view in the industry that certain aspects of the plant condition should be monitored, irrespective of whether the information is used in SAM.

There is an Equipment Qualification issue in the use of DBA instrumentation for SAM: operating margins must be carefully considered and may require additional Equipment Qualification tests to verify needed operating range, particularly for temperature and mission time.

The question was raised about the value of new techniques such as neural networks or fuzzy logic as operator aids for SAM. The prevailing view was that such systems are not mature nor sufficiently simple at this time and are topics for research. Not much progress in this field had been noted since a few years.

## **10 CONCLUSIONS**

The specialist meetings organised and the work performed during the last twelve years within CSNI in the area of the instrumentation to manage severe accidents, have allowed the sharing of important information, the exchange of views and cross-fertilisation of ideas, the fostering of international collaboration, the mutual understanding of national strategies and positions. They were therefore instrumental in the progress made in the field.

In line with the defence-in-depth concept, the prevention of severe accidents normally receives the first priority. When this is done successfully, the probability of a core melt remains very small for any given plant. It is then difficult to justify costly additional measures. Most countries have therefore adopted a pragmatic approach, i.e. to start from the plant “as is” and to give guidance to the operators in order to help them manage core melt accidents with existing equipment. Concerning the instrumentation needs and capabilities, the experience has shown this strategy to be workable for the following reasons:

1. Analyses have shown that instrumentation environmentally qualified for design basis accidents in a conservative way, exhibits important capabilities to remain operational in severe accident conditions (analysed in a best estimate way), especially given the reduced accuracy needs.
2. The identification of redundancies and alternate means to obtain information on key parameters can increase the confidence in the capabilities of existing instrumentation in severe accident conditions. When several sensors measure the same parameter, it is easier to identify failed instruments. It is also often possible to obtain indirect information on a given parameter (e.g. the safety injection flow rate is an indication of the primary pressure). Graphical aids can be prepared to help interpret some indications (e.g. to obtain the level of water in the reactor building sumps from the level of water remaining in the reactor water storage tanks).
3. In order to obtain an accurate picture of the accident and its progress, it is necessary to measure a large number of parameters. However, it has been shown that such a detailed picture was not needed to derive an effective severe accident management plan, and that only a few key parameters were sufficient for this purpose, thereby reducing the instrumentation needs.

Most severe accident mitigation and management strategies can be effectively implemented using available instrumentation qualified for DBAs. However, further assessment could be required for some sensors needed for actuating containment atmosphere mitigative devices, and assessing system status or radiation conditions in some buildings. Moreover, there could be a need for rough evaluation of plant status for public communication.

Important progress was achieved in the last twelve years in the understanding of the role of instrumentation in severe accident management. The instrumentation needs have been found to be lower than thought ten years ago, and the capabilities of existing instrumentation have been found to be higher. These findings have made severe accident management implementation easier and more robust. They have increased the confidence in the effectiveness of accident management strategies and procedures.

## 11 REFERENCES

- [1] "Instrumentation for light-water-cooled nuclear power plants to assess plant and environs conditions during and following an accident", USNRC Regulatory Guide 1.97
- [2] "Equipment Qualification Test of a High Range Radiation Monitor", NUREG/CR-4728, Sandia National Laboratory, 1988
- [3] "Beta and Gamma Dose Calculation for BWR and PWR Containments", NUREG/CR-5175, Sandia National Lab., 1989
- [4] "Equipment Qualification Risk Scoping Study", NUREG/CR-5313, Sandia National Lab., 1989
- [5] "Accident Management Information Needs", NUREG/CR-5513, Vol. 1 and 2, April 1990
- [6] "Instrumentation for accident management in containment", NEA/CSNI/R(92)4, January 1992
- [7] "Proceedings of the first OECD (NEA) CSNI specialist meeting on instrumentation to manage severe accidents (Cologne 16-17 March 1992)", NEA/CSNI/R(92)11
- [8] "Specialist meeting on instrumentation to manage severe accidents - Summary and recommendations", NEA/CSNI/R(93)3
- [9] "Proceedings of the specialist meeting on severe accident management implementation (Niantic 12-14 June 1995)", NEA/CSNI/R(95)5
- [10] "Specialist meeting on severe accident management implementation - Summary and conclusions", NEA/CSNI/R(95)16
- [11] "Severe accident management implementation", OECD/NEA, 1996
- [12] "Instrumentation and signal validation under extreme conditions", Proceedings of the FISA 95 symposium on EU research on severe accidents, EUR 16896, 1996
- [13] "Proceedings of the second specialist meeting on operator aids for severe accident management (Lyon 8-10 September 1997)", NEA/CSNI/R(97)10
- [14] "Second specialist meeting on operator aids for severe accident management - Summary and conclusions", NEA/CSNI/R(97)27
- [15] "Implementation of severe accident management guidelines at the Tihange power plant", Proceedings of the TOPSAFE'98 conference, Valencia, April 1998
- [16] "Proceedings of the OECD (NEA) CSNI workshop on severe accident management - operator training and instrumentation capabilities (Lyon 12-14 March 2001)", NEA/CSNI/R(2001)7
- [17] "Workshop on severe accident management - operator training and instrumentation capabilities - Summary and conclusions", NEA/CSNI/R(2002)11
- [18] "Proceedings of the OECD (NEA) CSNI workshop on implementation of severe accident management measures (Villigen 10-13 September 2001)", NEA/CSNI/R(2001)20
- [19] "Workshop on implementation of severe accident management measures - Summary and conclusions", NEA/CSNI/R(2002)12