Rolls-Royce

VVER 2013: Experience and Perspectives after Fukushima

ADDRESSING I&C POST-FUKUSHIMA REQUIREMENTS:

From regulatory requirements analysis to systems design and hardened instrumentation.

Authors:

Arnaud DUTHOU, Rolls-Royce Civil Nuclear I&C, France

Silvain IKAZAKI, Rolls-Royce Civil Nuclear I&C, France

Jana KUBINOVA, Rolls-Royce Civil Nuclear I&C, Czech Republic

© Rolls-Royce plc 2013

The information in this document is the property of Rolls-Royce plc and may not be copied, or communicated to a third party, or used, for any purpose other than that for which it is supplied without the express written consent of Rolls-Royce plc.
Whilst this information is given in good faith based upon the latest information available to Rolls-Royce plc, no warranty or representation is given concerning such information, which must not be taken as establishing any contractual or other commitment binding upon Rolls-Royce plc or any of its subsidiary or associated companies.

Rolls-Royce Holdings plc
Registered Office:
65 Buckingham Gate
London
SW1E 6AT

T +44 (0)20 7222 9020
rolls-royce.com

Company number 7524813

ABSTRACT

Following Fukushima events, regulatory authorities have issued new recommendations and requirements for post and severe accident systems. From specification work to implementation, each phase of the process to integrate these new Instrumentation and Control (I&C) functionalities requires specific expertise:

i) Methodology to link regulatory requirements to functionalities and systems definition
ii) Implementing these specifications at system level
iii) Qualified hardened instrumentation and equipment

Considering plant specificities (seismic/flooding…), interpreting the regulatory requirements to produce the functionalities and description of the post-accident systems is a complex process.
Moreover, Defence-in-Depth principles and installed equipment impose additional constraints such as more stringent seismic and EMC requirements or separate PAMS and SAMS.

Once these specifications are established, the design of the post and severe accident systems must be adapted to each situation. For example, Rolls-Royce offers a step-by-step approach to tailor a solution adjusted to the plant specific constraints and severe environmental conditions: Digital or Hardwired systems (up to 1E/Cat A qualified) that can also contribute to diversity requirements, seismic-resistant equipment and hardened instrumentation.

To complete these systems, qualified ruggedized sensors able to withstand the extreme accident conditions must be used.

Rolls-Royce provides complete and modular solutions to address post-Fukushima I&C requirements for both newbuilds and upgrades, notably for VVER: regulatory guidelines analysis, specification and design of corresponding systems, hardened instrumentation and equipment supply.

TABLE OF CONTENTS

1. Context

Following the Fukushima events, international and local regulatory authorities have issued new recommendations and requirements to better cope with severe accidents.

These new guidelines call for a stricter implementation of the Defence-in-Depth concept at all levels, but in particular with new or improved post and severe accident systems and more resistant equipment from instrumentation to the complete systems.

Several factors complicate the implementation of these requirements:

- As the analysis of the Fukushima events is not yet complete, the recommendations and requirements are not precise and their interpretation is often ambiguous
- For new builds, it is easier to add new systems or modify the ones planned, but the risk remains to see new regulations appear and have to change these again
- For existing plants, the addition of new systems, or upgrade of existing ones, can be quite problematic as the technology used, the need of compatibility with other equipment in place and the lack of room leaves very little freedom to design the new system
- The resistance of the equipment used must be increased to face severe environment

This is why, from specification work to implementation, each phase of the process to integrate these new Instrumentation and Control (I&C) functionalities requires specific expertise:

- Methodology to link regulatory requirements to functionalities and systems definition
- Implementing these specifications at system level
- Qualified hardened instrumentation and equipment

Considering plant specificities (seismic/flooding…), interpreting the regulatory requirements to produce the functionalities and description of the post-accident systems is a complex process.

Moreover, Defence-in-Depth principles and installed equipment impose additional constraints such as Diversity requirements or separate PAMS and SAMS.

Therefore, a deep understanding of local and international regulations and the reactor design are needed to create the new specifications.

Once these specifications established, the design of the post and severe accident systems must be adapted to each situation. To answer all these needs, Rolls-Royce offers a step-by-step approach to create a solution adapted to the plant specific constraints and severe environmental conditions: Digital or Hardwired systems (up to 1E/Cat A qualified) for diversity, seismic-resistant equipment and hardened instrumentation.

To complete these systems, qualified ruggedized sensors able to withstand the extreme accident conditions must be used.

2. Methodology to analyze requirements and link them to functionalities and Post-Accident systems definition

2.1. Approach to I&C requirements

The Fukushima accident resulted in unprecedented efforts to review the safety of nuclear installations in the world. Initiatives were taken at national, regional and international level.

These efforts have led to the definition of new sets of requirements. These requirements are based on 3 main sources of requirements: IAEA, WENRA and US NRC.

- **IAEA**: Strengthening Nuclear Regulatory Effectiveness in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant – September 2013
- **WENRA**: Safety of new NPP designs, study by WENRA Reactor Harmonization Working Group, October 2012 (draft submitted to designers and operators)
- **US NRC**:
  - ISG-2012-01 Compliance with Order EA-12-049, Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events
  - ISG 2012-03 Compliance with Order EA-12-051, Reliable Spent Fuel Pool Instrumentation

These requirements must then be completed to comply with local regulations issued by the national authorities.

In order to ensure the compliance with all these requirements a system designer must follow a complete process to guarantee that all have been taken into account in the design of the post and severe accident systems.

The Figure 1: Process to define severe & Post-Accident I&C" summarizes the path that connects the regulation to the requirements applicable to I&C dealing with post and severe accident.

This process can be divided into 3 main steps:

First Step: defining the Post-Fukushima design basis

The regulatory requirements (which may vary depending on the country) and the VVER Plant Design will guide the definition of the set of internal events to be deterministically or probabilistically considered. Generally, the following internal events are considered:

- Total Loss of AC power source: this corresponds to a situation where the offsite power source is lost, in conjunction with all the Safety Diesel Generator Sets.
- Total Loss of Ultimate Heat Sink: this corresponds to a situation where the ultimate heat sink (pumping station of the sea, or river) is lost.
- Combination of Total loss of AC power source and ultimate heat sink.

In parallel, the regulatory framework and the site specificities allow to define the set of Beyond Design Basis External Hazards. In a plant design basis, the design basis external hazards are listed, and their mitigation is described. Fukushima Daiichi accident leads to broaden the search for external hazards and define "Beyond Design Basis External Hazards". These are usually the same as the Design Basis External Hazards, but with higher magnitude. For example, if the SSE (Safe Shutdown Earthquake) is define at 0.3g acceleration (at infinite frequency at ground level), then the extended magnitude could be defined at 0.5g.

The loading conditions corresponding to each Beyond Design Basis External Hazard are then assessed (vibration, water level, temperature …).

Second Step: defining the functional response to Post-Fukushima internal events

Based on the list of internal events to be considered, the minimal set of functional need is defined. This step is separated into two parts:

- The first part consists in avoiding the core melt. This approach is reinforced in the US NRC and is more deeply described in the NEI 12-06 FLEX strategy. It is also required in the WENRA and IAEA approach, which describes that the basic safety features must be reinforced in order to mitigate the event to avoid core melt.
- The second part consists in mitigating a core melt, should it occur. This corresponds to the so called Severe Accident Features. Although US NRC does not strictly require to consider this as part of Beyond Design Basis External Hazard mitigation strategy, WENRA and IAEA explicitly recommends to include them in the overall strategy.

Third Step: identify the SSC fulfilling the functional response to Post-Fukushima internal events and demonstrate their robustness to the Beyond Design Basis External Hazard loading conditions

Based on the list of functional needs, a minimal set of SSC allowing to prevent core melt and mitigating core melt are identified. This set of limited SSC, among which I&C equipment is included, is subjected to stringent loading conditions, defined in the first Step.

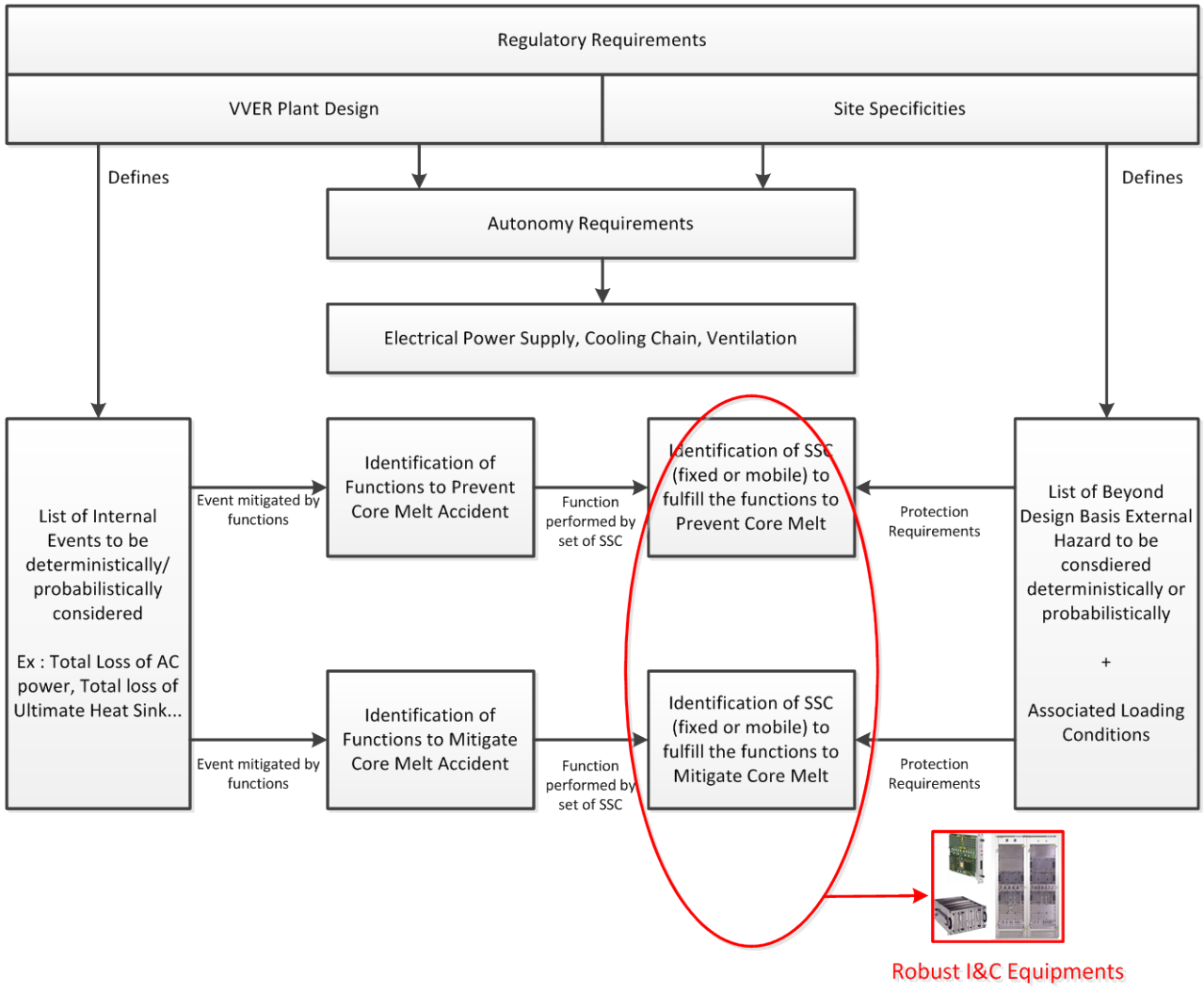


Figure 1: Process to define post & severe Accident I&C

2.2. Examples of Requirements applicable to post-Fukushima related I&C

Although the recommendations are different depending on the above listed texts, and subject to evolution, the following main aspects can be considered as general tendencies:

- Consideration of beyond design basis external hazards whose magnitude goes beyond what has been considered in the design. The ASN proposes to consider a level of earthquake 1.5 times higher than the SSE and NRC recommends to demonstrate the robustness to an earthquake 1.67 times higher than the SSE, but authorizes to use statistical methods such as “Seismic Margin Assessment”

- Demonstration that a certain autonomy in terms of support functions (electrical power supply, cooling chain, ventilation) is available on site, even when offsite sources are unavailable for a long period. To comply with such requirements, having simple and low consumption I&C is an asset.

- Possibility to upgrade I&C systems mitigating Post-Fukushima events to Class A. This can be required when some parameters need to be shared between safety I&C systems and I&C system credited to mitigate Post-Fukushima type events, where a common conditioning cabinet is necessary for both systems. This conditioning would then need to be Class A.

3. Implementing these specifications at system level

Once the functionalities and general characteristics of the new or upgraded post-accident systems have been established according to regulations, the plant specificities must be taken into account to produce the detailed specifications.

For existing plants, the constraints created by the existing systems: technologies used, qualification standards dating from original install and often lack of spare room make it quite difficult to add new systems or upgrade existing ones.

For new builds this process is less complex as there are no constraints due to equipment already in place, nevertheless the compatibility with the plant design (layout, sensors, actuators..) and needs of diversity must also be ensured regarding other systems, and the new requirements will have to be totally implemented and demonstrated.

To be able to adapt to these various constraints, Rolls-Royce provides flexible and modular solutions to address post-Fukushima I&C requirements for both newbuilds and upgrades, notably for VVER.

The choice of measurements, architecture and technologies must be carefully studied to guarantee the correct implementation of the functionalities, compatibility with other systems and acceptation by licensing authorities.

The first step is to identify all the parameters to monitor and actuators that may be requested in severe and post-accident systems. This is done on the base of the regulations requirements but must be completed by simulation tools (for example: MAAP, APROS, RELAP, Melcor..) to determine the number and location of sensors needed.

Figure 2: Example of Measurements/Actuation needed in post-accident systems" shows a list of such parameters and actuators.

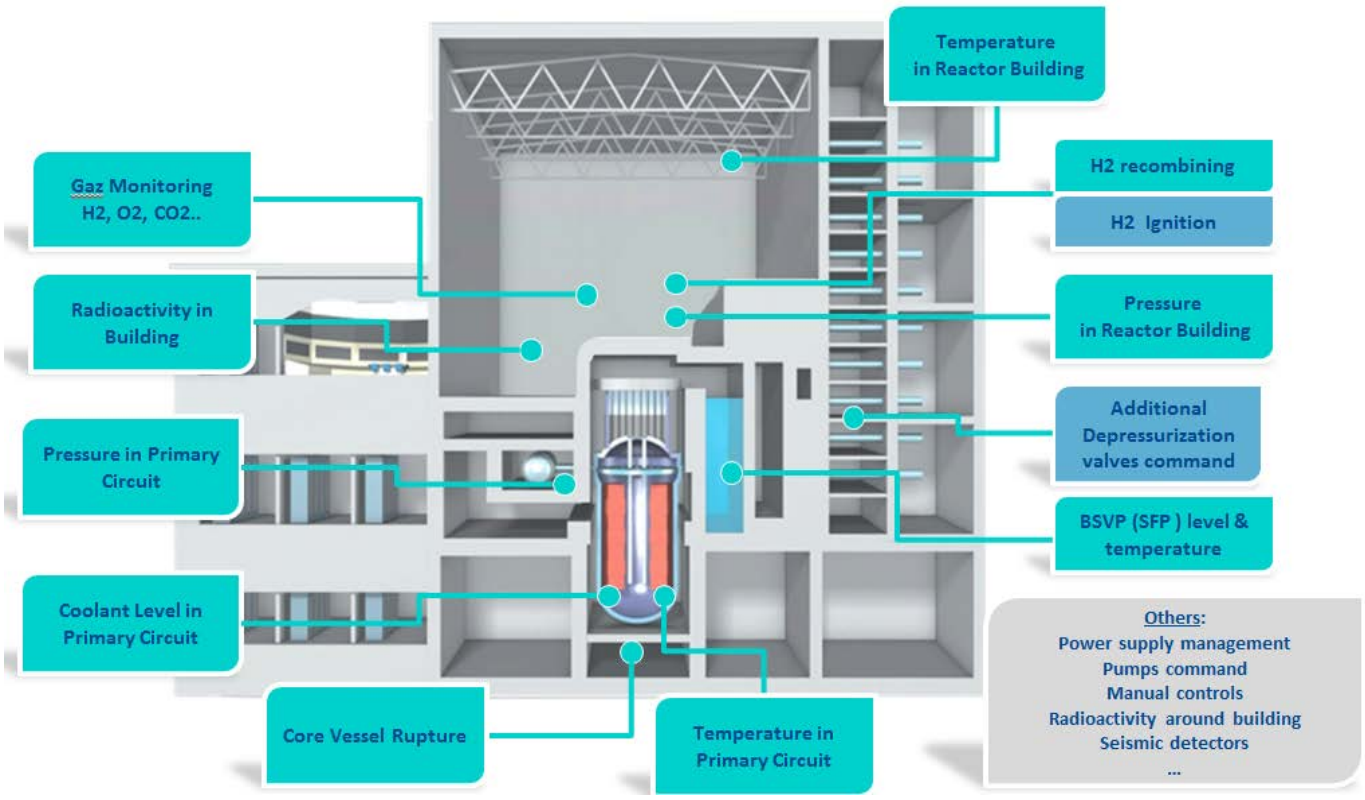


Figure 2: Example of Measurements/Actuation needed in post and sever accident systems

In section 4: “Qualified hardened instrumentation and equipment” we will describe in detail how to find the physical characteristics that must be satisfied by these sensors and the rest of the equipment.

Once the exact scope of the measurements and actuators has been defined, the corresponding conditioning equipment is established: the number of cabinets, their seismic resistance and location will depend on the technology chosen (this is often dictated by the sensors used), local regulations and availability of spare room to fit them.

Notice that the use of existing sensors and conditioning is possible, but only if they have been qualified according to the new post and severe accident regulation standards

Then, for the processing of the data, Rolls-Royce offers several technologies: Digital, Analogue or Hybrid. This allows for optimal treatment compatibility with technologies in place (for upgrades) or planned (new builds) and diversity needs:

Rolls-Royce has implemented numerous Cat A & B Hardwired and Digital systems on Nuclear Power Plants all over the world.

Spinline^{TM} is Rolls-Royce digital platform, Safety qualified (1E/Cat. A) and installed in France, Czech republic, China, and soon 1E qualified in the US.

Similarly, Hardwired Cat A & B systems total up more than 2000 reactor years on the French fleet and are also present in China, South Korea and South Africa. These are built using the following technologies/elements:

- Failsafe Dynamic logic modules
- “Modumat” modules
- Spinline racks and cubicles that contain these systems.

This variety of technologies provides more flexibility to the plant owner or designer to implement the new functionalities required.

Moreover, the architecture design can take advantage of these platforms modularity as it provides more choices to implement each functionality that may have strict constraints (parts of the system/instrumentation already installed, regulations requirements for diversity, etc..).

In the control room the signal and actuation commands are located on specific panels, also designed to fulfill post and severe accident requirements.

Finally, as thought by some safety authorities, the signals may be sent to a remote crisis center, in parallel to the main control room, to guarantee the continuity of the functionality in case of unavailability of the main control room caused by the accident.

Figure 3: Example of a complete Post-Accident system” shows the possible architecture resulting from this process for a complete severe and post-accident system.

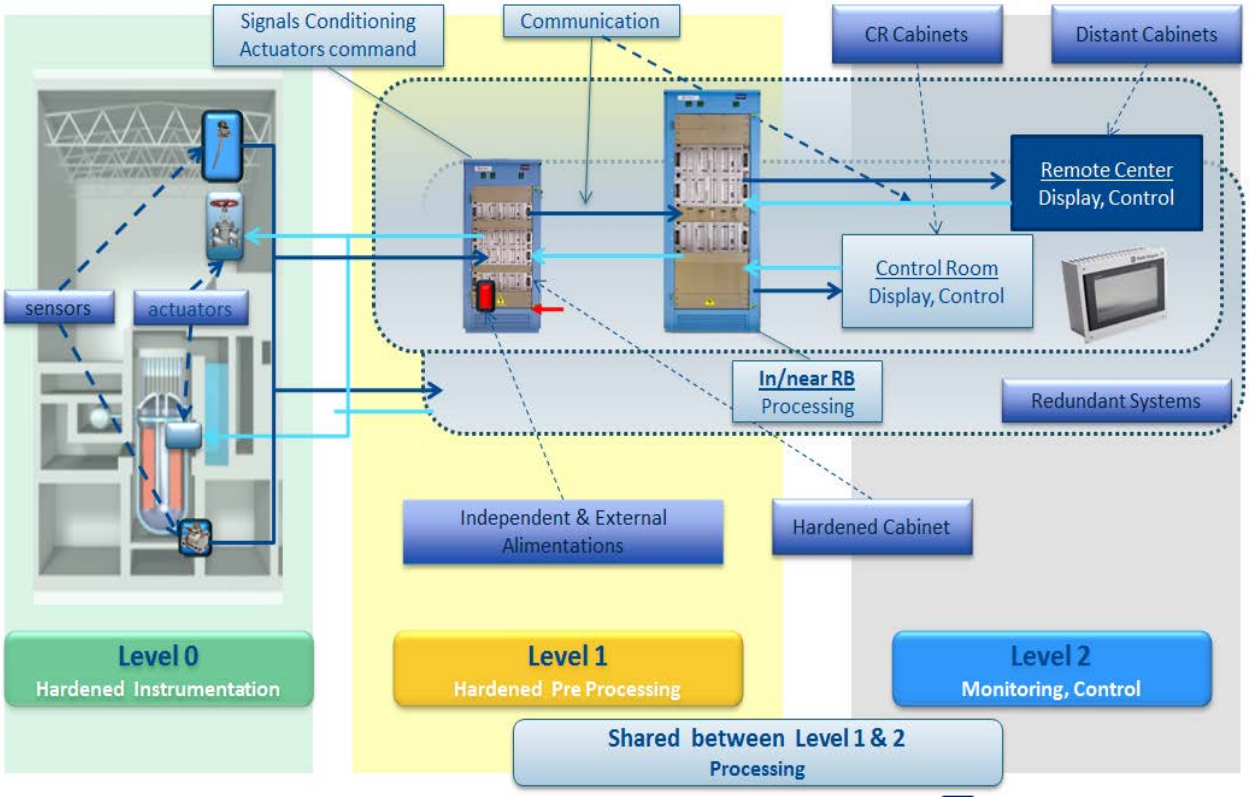


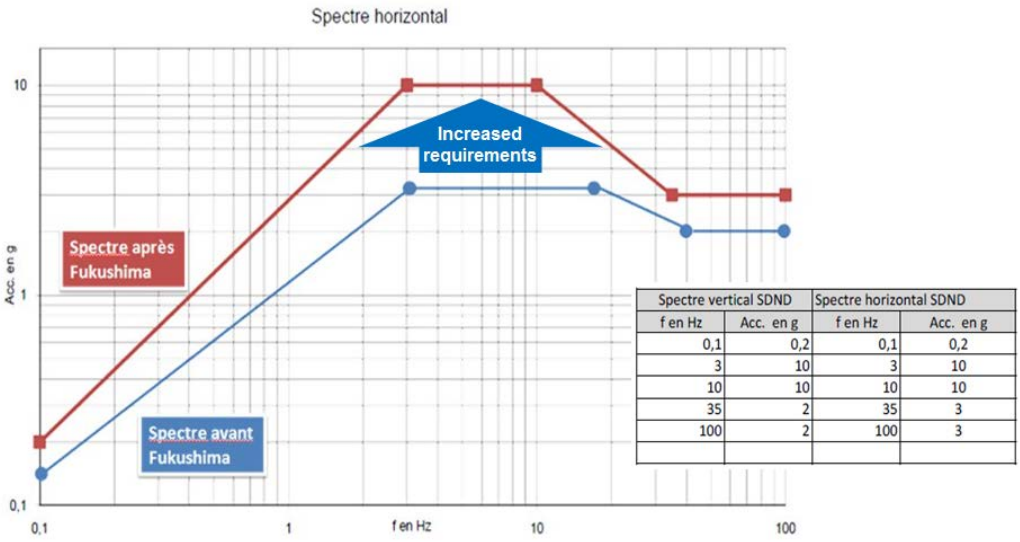
Figure 3: Example of a complete post and severe accident system

This transition from regulatory requirements and plant constraints to the system implementation necessitates both nuclear engineering capabilities and modularity and flexibility of the platforms and technologies used to minimize the impact on other systems, and therefore reduce implementation time and ease the acceptance by the safety authorities.

4. Qualified hardened instrumentation and equipment

To be able to continue operating after the accident, all the equipment used in the severe and post-accident systems must be able to withstand harsher environmental conditions than normal operation systems. This is particularly true for all the sensors inside the reactor building.

After the stress tests, most countries have decided to reevaluate their seismic requirements to be able to resist stronger events.



Spectre vertical SDND		Spectre horizontal SDND	
f en Hz	Acc. en g	f en Hz	Acc. en g
0,1	0,2	0,1	0,2
3	10	3	10
10	10	10	10
35	2	35	3
100	2	100	3

Figure 4: Planned increase of seismic requirements for French post-Accident "noyau dur"

Therefore, Cabinets, racks and boards must be designed to withstand tougher qualification tests.

This is also the case for sensors & actuators that will be included in the post-accident I&C functions. In addition to the seismic requirements they must also be able to resist to a stronger and longer exposure to Thermal-Hydraulic harsh conditions, EMC and radiation (in particular for those installed in the reactor building).

These new requirements can be problematic for all the equipment that contains electronic components that are very sensitive to radiations.

To alleviate this risk, in Rolls-Royce Bibloc pressure transmitters, the electronic parts are separate from the actual mechanical sensors, so all the electronics are placed outside of the reactor building (and therefore away from the harsher environmental post-accident conditions) while only the mechanical part (very resistant to harsh environment) are located within the reactor building.

Similarly, the other sensors, probes and actuators must be designed to withstand these more stringent requirements and it is quite complex to strengthen existing ones enough to become compliant.

5. Conclusion

The new guidelines following the Fukushima events call for a stricter implementation of the Defence-in-Depth concept at all levels, but in particular with new or improved post and severe accident systems, a greater diversity and more resistant equipment from instrumentation to the complete systems.

Several factors complicate the implementation of these requirements:

- As the analysis of the Fukushima events is not complete yet, the recommendations and requirements are not precise and their interpretation is often ambiguous
- For new builds, it is easier to add new systems or modify the ones planned, but the risk remains to see new regulations appear and have to modify these
- For existing plants, the addition of new systems, or upgrade of existing ones, can be quite problematic as the technology used, the need of compatibility with other equipment in place and the lack of room leaves very little freedom to design the new system
- The resistance of the equipment used must be increased to face severe environment

This is why, from specification work to implementation, each phase of the process to integrate these new Instrumentation and Control (I&C) functionalities requires specific expertise:

- Methodology to link regulatory requirements to functionalities and systems definition
- Implementing these specifications at system level
- Qualified hardened instrumentation and equipment

Considering plant specificities (seismic/flooding…), interpreting the regulatory requirements to produce the functionalities and description of the post-accident systems is a complex process.

Moreover, Defence-in-Depth principles and installed equipment impose additional constraints such as Diversity requirements or separate PAMS and SAMS.

Therefore, a deep understanding of local and international regulations and the reactor design are needed to create the new specifications.

Once these specifications are established, the design of the post and severe accident systems must be adapted to each situation. For example, Rolls-Royce offers a step-by-step approach to tailor a solution adapted to the plant specific constraints and severe environmental conditions: Digital or Hardwired systems (up to 1E/Cat A qualified) for diversity, seismic-resistant equipment and hardened instrumentation.

To complete these systems, qualified ruggedized sensors able to withstand the extreme accident conditions must be used.

Rolls-Royce provides complete and modular solutions to address post-Fukushima I&C requirements for both newbuilds and upgrades, notably for VVER: regulatory guidelines analysis, specification and design of corresponding systems, hardened instrumentation and equipment supply.