Statement on the Separation of Safety I&C and Operational I&C

Expanded Version

Dr. Helmut Hirsch, Scientific Consultant for Nuclear Safety

Neustadt, November 05, 2009

Defence in depth

There is a fundamental concept which is applied world-wide to keep nuclear hazards as low as possible – the concept of defence in depth. The central feature of this concept is the idea to have multiple levels of protection.

In brief, the following levels are defined [INSAG 1999]:

Level 1 – prevention of abnormal operation

Level 2 – control of abnormal operation, detection of failures

Level 3 – control of accidents within design basis

Level 4 – prevention and mitigation of severe accidents

Level 5 – mitigation of radiological consequences of releases

For new reactors, the design basis (level 3) is generally broader than for reactors currently in operation, and level 4 is taken into account already in the design phase and not retroactively as in current reactors.

Independence of the levels of defence is an essential feature of the concept. Only a high degree of independence can guarantee that if one level fails, the subsequent level will be available.

The IAEA's "Fundamental Safety Principles" [IAEA 2006] discuss defence in depth and state, inter alia:

"When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. ***The independent effectiveness of the***

different levels of defence is a necessary element of defence in depth.” (emphasis added)

Digital I&C - classification

The distinction of different levels of protection is mirrored by the distinction of different safety classes or categories for structures, systems and components. This also applies to instrumentation and control systems.

For example, the recently published final version of the new German Safety Criteria for Nuclear Power Plants [BMU 2009] distinguishes three categories for instrumentation and control:

Category A – For all functions necessary to control events assigned to level of defence 3

Category B – For all functions necessary to control events assigned to level of defence 2, and to prevent occurrence of events assigned to level 3

Category C – All other safety-related functions

In Finnish regulations, safety classes from 1 (highest safety significance) to 4 (plus class EYT for anything not belonging to the other safety classes) are defined for all systems, structures and components [STUK 2000]. There is no explicit reference to the levels of the defence in depth concept as described above, but this concept is implicit in the definition of the classes.

UK regulations are similar in this respect, with safety classes 1 (highest safety significance) to 3 plus a safety class S (concerning possible safety relevance in case of a seismic event) [NSD 2003].

The Finnish regulations require separation between I&C systems of different levels, as do the German regulations. Exceptions are not completely excluded by both regulations as long as safety is not endangered. However, any exception is, in principle, a violation of the defence in depth concept. Also, it can be very difficult to prove that plant safety is not reduced, particularly regarding interconnections between digital I&C systems.

The “Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors” demands, inter alia, that the principle of separation between safety and non-safety functions shall be

applied to the design both of computer system architecture and the software [EC 2000].

Problems of digital I&C

In general, flexibility and complexity of digital I&C are considerably higher, compared to hardwired systems. Software offers much more possibilities regarding conception, parametrization and also later adaptations.

There is a strong pressure – mainly for economic reasons – towards interlinking of systems of different safety classes. This leads to complex interactions. Experience shows that complex networks without a history of safety problems are the absolute exception.

There is also the constant temptation to make extensive use of the flexibility of the software by building in more and more functionality and automatisms. Thus, appropriate testing of software can get increasingly difficult.

Regarding the case of the EPR, it has been reported that this reactor's I&C architecture is at present being reviewed by Finnish, French and UK regulatory authorities. According to the magazine "Nuclear Engineering International", the UK Nuclear Installations Inspectorate (NII) stated in a letter to AREVA and EDF in April 2009 that the EPR's digital I&C system architecture "appears overly complex". An NII spokesperson later explained that the Inspectorate is not convinced that software used to control the plant and software used to protect the plant in case the control system stops working are sufficiently separate. Also, there are concerns that safety systems (level of defence 3 and higher) might be compromised by too many connections with less safety-critical systems (levels of defence 1 and 2). The NII letter pointed out that "[t]he usual UK practice of only allowing one-way online communication from a safety system to systems of lower safety class is not applied in the UK EPR design" [NEI 2009].

At the beginning of October, the Finnish STUK and the UK NII have expressed reservations because of possible interference between safety-class and non-safety-class I&C. STUK required a hardwired backup from the beginning [NW 2009].

And most recently, at November 03, 2009, the nuclear regulatory authorities of Finland, France and the UK took the unusual step to publish a joint statement demanding amendments to the EPR's I&C. The regulators stated

that the operational controls for EPRs are too closely connected to the safety systems and hence, the design doesn't comply with the independence principle [F24 2009; WNN 2009].

It seems clear that there is an unacceptable degree of interconnectivity between systems belonging to different levels of defence, in the EPR's digital I&C. As pointed out above, such a far-reaching interdependence is contradictory to the foundation of nuclear safety philosophy world-wide – the concept of defence in depth.

This interdependence opens up the possibility that the functioning of safety I&C is impaired by interaction with lower-level I&C. In the worst case, this can lead to a minor incident developing into a severe accident.

STUK is well advised not to accept the digital I&C system of the EPR in its present form. It appears that fundamental and very far-reaching modifications of this system are urgently required.

For a more detailed assessment of the importance and possible consequences of the interdependencies of various automation systems, information on the sub-systems involved and on the connections between sub-systems would be required, in particular concerning the parts of I&C which are at present subject of the concerns of the regulatory authorities in Finland, France and UK.

Also, a presentation of the problem in terms of levels of defence (i. e. a classification of the sub-systems involved according to their role in the defence in depth concept) would be necessary.

References:

BMU 2009

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Sicherheitskriterien für Kernkraftwerke, Revision D; Juni 2009

EC 2000

European Commission: Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors; European Commission's Advisory Experts Group, The Nuclear Regulators' Working Group, Task Force on Safety Critical Software, Version 11, EUR 19265, May 2000

F24 2009

FRANCE 24: Regulators call for redesign of France's latest reactor; http://www.france24.com/en/20091103-nuclear-energy-epr-reactors-france-finland-areva-safety-concern?autoplay=, November 03, 2009

IAEA 2006

International Atomic Energy Agency: Fundamental Safety Principles; Safety Fundamentals No. SF-1, Vienna 2006

INSAG 1999

International Nuclear Safety Advisory Group: Basic Safety Principles for Nuclear Power Plants, Rev. 1; INSAG-12, International Atomic Energy Agency, Vienna 1999

NEI 2009

Nuclear Engineering International August 2009 (pp. 8/9)

NSD 2003

Nuclear Safety Directorate: Safety Categorisation and Equipment Qualification; Technical Assessment Guide T/AST/008, Issue Date 2/10/2000, Review Date 1/10/2003

NW 2009

Nucleonics Week Vol. 50, Number 39, October 1, 2009 (p. 4)

STUK 2000

Finnish Radiation and Nuclear Safety Authority (STUK): Nuclear power plant systems, structures and components and their safety classification; Regulatory Guide YVL 2.1, 26 June 2000

WNN 2009

World Nuclear News: Focus on EPR's systems; http://www.world-nuclear-news.org/RS_Focus_on_EPRs_systems_0311091.html, November 03, 2009