Requirements on Software Based Digital I&C in the Safety System of German Nuclear Power Plants

J. C. Stiller

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Schwertnergasse 1, D 50667 Cologne, Germany

www.grs.de jan.stiller@grs.de

20th Annual RIC, March 12th, 2008

Current situation in Germany

- In many German NPPs software-based digital I&C systems are used in:
  - operational (non-safety) systems
  - some safety related systems, e.g. systems required for beyond design basis accidents.
- In I&C systems of the **highest safety class** (RTS, ESFAS) currently **only conventional (hard-wired) technology** is used.
- Replacement of RTS and ESFAS with digital systems is planned for several plants.
- Two plants have applied for approval of backfitting RTS and ESFAS with software-based digital I&C.

German Rules and Regulations

- New regulations are under development (Module 5 of “Safety requirements for NPP”, KTA 3501).
- Discussions between operators, suppliers, regulatory bodies and expert organizations are still on-going.
- Main focus: Implementation of diversity as measure against common cause failures (CCF).
- Recently, consensus has been achieved among the German nuclear expert organizations supporting the German regulators (TÜV Nord, TÜV Süd and GRS organized in VdTÜV).

Opinion of German Expert Organizations (TSOs)

- (Software) CCFs of digital I&C Systems are
  - credible
  - **within design basis**.
- Therefore, the systematic failure has to be accounted for by design and has to be assumed in safety assessments for I&C systems of the highest safety class.

Opinion of German Expert Organizations (2)

- To account for systematic failures, sufficient diversity has to be implemented including
  - software diversity
  - hardware diversity.
- Criteria for diversity are e.g. different
  - hardware architectures,
  - hard- and software development tools,
  - development teams,
  - manufacture,
  - maintenance.

Opinion of German Expert Organizations (3)

- The **failure to actuate** as well as **spurious actuations** have to be considered.
- A simultaneous single failure in addition to a systematic failure need not be assumed.
- A systematic failure of I&C equipment shall not cause an accident.

Opinion of German Expert Organizations (4)

- Depending on the I&C function, either
  - no dissimilar equipment
  - two sets of dissimilar equipment
  - three sets of dissimilar equipment

  are necessary.
- Automatic voting shall be done by simple testable devices or directly at the final actuators (e.g. reactor trip breakers).

Opinion of German Expert Organizations (5)

- Manual actuations are also permissible, if they are
  - possible in the main control room
  - by means independent of the software based digital I&C system
  - and not necessary within 30 minutes.
- A detailed analysis has to be carried out to determine which measures are necessary and sufficient.
- In this analysis, it is assumed that all I&C equipment which is not sufficiently dissimilar fails simultaneously.

Opinion of German Expert Organizations (6)

- Examples:
  - If a protective action is definitely safety oriented and it is needed in design basis accidents earlier than after 30 minutes (e.g. reactor trip actuation), two diverse sets of I&C equipment are needed, such that a failure to actuate due to CCF is prevented.
  - If a protective action is **not** definitely safety oriented (i.e. it may be not safety oriented in some possible plant states) and it is needed in design basis accidents earlier than after 30 minutes (e.g. control of coolant level in reactor pressure vessel of BWR), three diverse sets of I&C equipment are needed, such that both a failure to actuate and a spurious actuation due to CCF are prevented.

Opinion of German Expert Organizations (7)

- If these requirements are met, no additional hard-wired backup system is necessary.
- Provisions must be made that planned emergency procedures can be carried out, independently of digital I&C systems.
- Emergency measures that are not pre-planned must also be possible.

For more details see the VdTÜV opinion paper, which will be publicly available soon, also as English translation.