A Summary of Taxonomies of Digital System Failure Modes

PSAM11/ESREL2012, Helsinki

June 25-29, 2012

Tsong-Lun Chu
Nuclear Science and Technology Department
(631-344-2389, Chu@BNL.GOV)

BROOKHAVEN NATIONAL LABORATORY

a passion for discovery

Office of Science
U.S. DEPARTMENT OF ENERGY

Outline of Presentation

- Background
- Collection of failure mode information from the participants
- Levels of detail of digital systems
- Summary of failure modes from participants
- Conclusions and ongoing work

Background and Objective

- In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group to coordinate activities in digital system reliability.
- Task report NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris, 2009 http://www.oecd-nea.org/nsd/docs/2009/csni-r2009-18.pdf summarizes research activities of participating countries/organizations and recommendation of future research.
- One of the recommendations was to develop a taxonomy of failure modes of digital systems for the purposes of probabilistic safety assessment (PSA).
- A new task group (abbreviated as DIGREL) was started 2010 with failure mode taxonomy as the first project.
- This presentation summarizes the inputs provided by participants of the project. A few other presentations of DIGREL task group provide summaries of additional activities on development of failure mode taxonomy.

Collection Of Failure Modes Information

- A workshop was held on May 16-19 2011 in Bethesda, Maryland, U.S.A. During the workshop, participants presented information on their failure mode work and ideas on the development of a failure mode taxonomy.
- In addition, the participants provided some written information about their research in this area including hardware and software failure modes, FMEAs, and modelling methods.
- The failure mode inputs from the participants are summarized according to the different levels of detail agreed upon by the participants.

Hardware Levels of Detail

- **System level:** A collection of equipment that is configured and operated to serve some specific plant function as defined by terminology of each utility.
- **Division level:** A system can be carried out in redundant or diverse divisions. In this case, a division may consist of the pathway(s) from sensor(s) to generation of an actuation signal. The actuation signal can be sent to multiple actuators. A division can be decomposed further into I&C units.
- **I&C unit level:** A division consists of one or more I&C units that perform specific tasks or functions that are essential for a system in rendering its intended services. I&C units consist of one or more modules.
- **Module level:** An I&C unit can be decomposed into modules that carry out a specific part of the process. For example, input/output-cards, motherboard, and communication cards, etc. An I&C unit may contain only a subset of these modules.
- **Basic components level:** A module is composed of a set of basic components bounded together on a circuit board in order to interact. Consequently, the states of a module are the set of the combined (external) states of its basic components. Failure modes defined at the basic component level should be independent of design or vendor.

Software Levels of Detail

- **System level:** For a digital protection system, at the system level, the software consists of the collection of software running on various microprocessors of the system and failure modes can be defined at this highest level.
- **Division level:** For the redundant or diverse divisions of an RPS, the collection of software running on the microprocessors of a single division may also fail and cause the failure of that division. Failure modes of all software belonging to a single division can be defined at this level as division level failure modes.
- **Module level/microprocessor level:** For the software program running on a particular microprocessor, the software is treated as an individual component like the microprocessor of a module.
- **Sub-module level:** The software that runs on a microprocessor may be complicated enough such that it can be further decomposed, to a so-called sub-module level.

Hardware Failure Modes

- The failure modes are often defined in terms of the functions, e.g., failure to actuate and spurious actuation. Some failure modes are more descriptive (and like failure causes), e.g., round-off/truncation/sampling rate errors and setpoint corruptions.
- Some failure modes are defined as detectable and non-detectable.
- Some failure modes are in terms of the signals being processed, e.g., many of those at the basic component level.

Software Failure Modes

- At system level, the failure modes are the same as those of hardware functional failures, except that timing of load sequencer and specific actuation signals of ESFAS are also used in the definitions.
- Due to the common assumption that divisions running the same software would fail together and cause a system failure, no specific division level failure modes was defined.
- At module level, function specific failure modes were defined, e.g., incorrect voting. At microprocessor level, generic failure modes were defined, e.g., software stalls, software aborts.
- At sub-level, functional failure modes associated with signals to valves and pumps were defined.

Conclusions and Going Forward

- The taxonomy of failure modes summarized here represents preliminary results collected from participants. The working group is developing a consensus failure mode taxonomy for both hardware and software based on the input of the participant and the discussions during the workshops. Other papers of DIGREL provide information about the progress made so far.
- The taxonomy needs to be defined and maintained at various levels of detail to provide options to PRA analysts and/or I&C system designers such that the taxonomy at a particular level of detail can be selected based on their own FMEA and/or reliability modelling need.
- It is generally agreed that a modelling method needs to capture dependencies and fault tolerant features, use meaningful failure modes, and propagate failure effects.