System and software safety viewpoints

Inga-Lill Bratteby-Ribbing
Defence Materiel Administration
P.O. Box 228, SE-751 04 Uppsala Sweden
ilbra@fmv.se

Abstract

For the stakeholder procuring safety-critical systems there is a need for architectural viewpoints and views addressing system safety to further a coherent description of how system safety is to be achieved on different levels in the structure, on which level(s) a specific safety threat is to be met, by which means the contributions to the overall system criticality from different parts are to be reduced etc.

1. Subject of discussion

Some interesting topics for the workshop within this area could be:

- Which models, architectural patterns etc. have been successful in supporting system safety for different applications?
- Are there differencies between the software safety views of an architecture defined for an information system compared to those for a real-time system (e.g. for monitor and control)?
- Should separate safety views be defined or should safety aspects be incorporated in the basic views used for the system (safety-critical parts and safety-critical information flows identified in the traditional views, hazard-accident chains added as anti-scenarios)?

A number of common safety principles have been formulated and used in different applications, e.g. [1] - [7].

- How can these be transformed to a higher level as patterns for a safety-critical architecture?

An example might be the principle of separation between critical and none (or less) critical parts, where traditionally physical separation has been advocated. Lately logical and temporal partitioning have been in focus (e.g. in IMA: Integrated Modular Avionics). Supporting concepts such as safety-walls, safety-ports and safety-kernels have also been suggested, [8] - [10].

These are just a few examples from the intersection Software Architecture – System Safety, where it would be interesting to see a number of advancements.

2. References

[1] N.G. Leveson, Safeware: System Safety and Computers, Addison-Wesley Publishing Company Inc., ISBN 0-201-11972-2, 1995.

[2] Standard Practice for System Safety, MIL-STD-882D, 2000.

[3] Requirements for Safety Related Software in Defence Equipment, Part 1 : Requirements, Part 2: Guidance, MOD Defence Standard 00-55, 1 aug 1997.

[4] Software Considerations in Airborne Systems and Equipment Certification, DO 178-B, dec 1992.

[5] IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Part 1-7, 1998-2000.

[6] IEC 60880, Software for Computers in the Safety Systems of Nuclear Power Stations, 1986.

[7] H ProgSäk, Handbok för Programvara i säkerhetskritiska tillämpningar (Handbook för Software in Safety-critical Applications), Armed Forces book and form store, M7762-000531, 2001.

[8] B.L. Di Vito, A Model of Cooperative Noninterference for Integrated Modular Avionics, 7th Intern. Working Conf on Dependable Computing for Critical Applications, pp. 251-268, 1999.

[9] John Rusby, Partitioning in Avionics Architecures: Requirements, Mechanisms, and Assurance, NASA/CR-1999-209347, 1999.

[10] G.T. Watt, Firewalls in Safety-Critical Systems, Proc. of the 18th Intern System Safety Conf, pp. 22-29, 2000.