Application of Reliability Analysis in Preliminary Design Stage of Digital I&C System

Presentation for PSAM 14

Wenjie Qin, **Xuhong He**, Xiufeng Tian, Dejun Du

September 2018, Los Angeles

Lloyd's Register

Contents

Introduction – I&C reliability analysis

As the digital I&C systems play a critical role in plant safety and availability, there is a need to quantitatively assess the reliability of such systems.

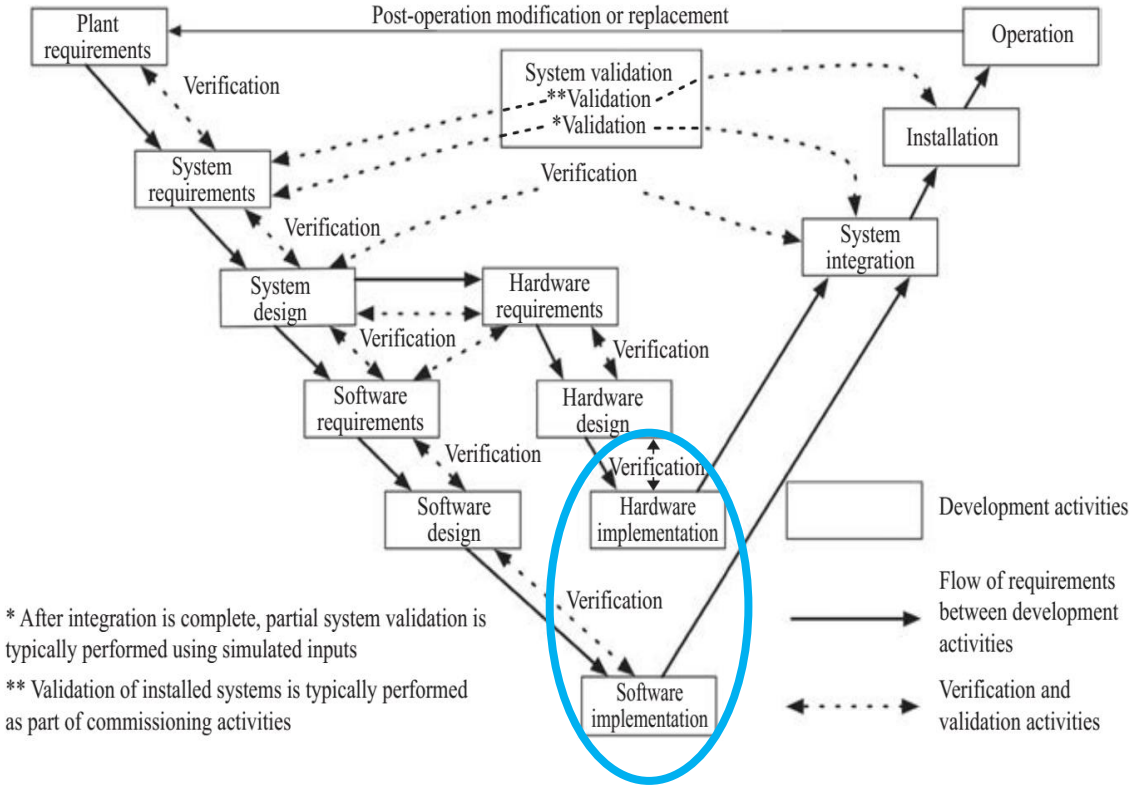
The reliability analysis of digital I&C systems are often performed in two contexts:

- To validate the fulfillment of reliability and availability requirements.
- Or, in Probabilistic Safety Assessment (PSA) for the modeling of I&C systems.

Introduction – Reliability analysis with detailed I&C design

- The I&C reliability analysis is often performed after hardware and software implementation stage, when the detailed I&C design information is available.
- However, in case of major design issue identified, it is very costly to make significant design change of the I&C systems at the stage.

Typical I&C development process

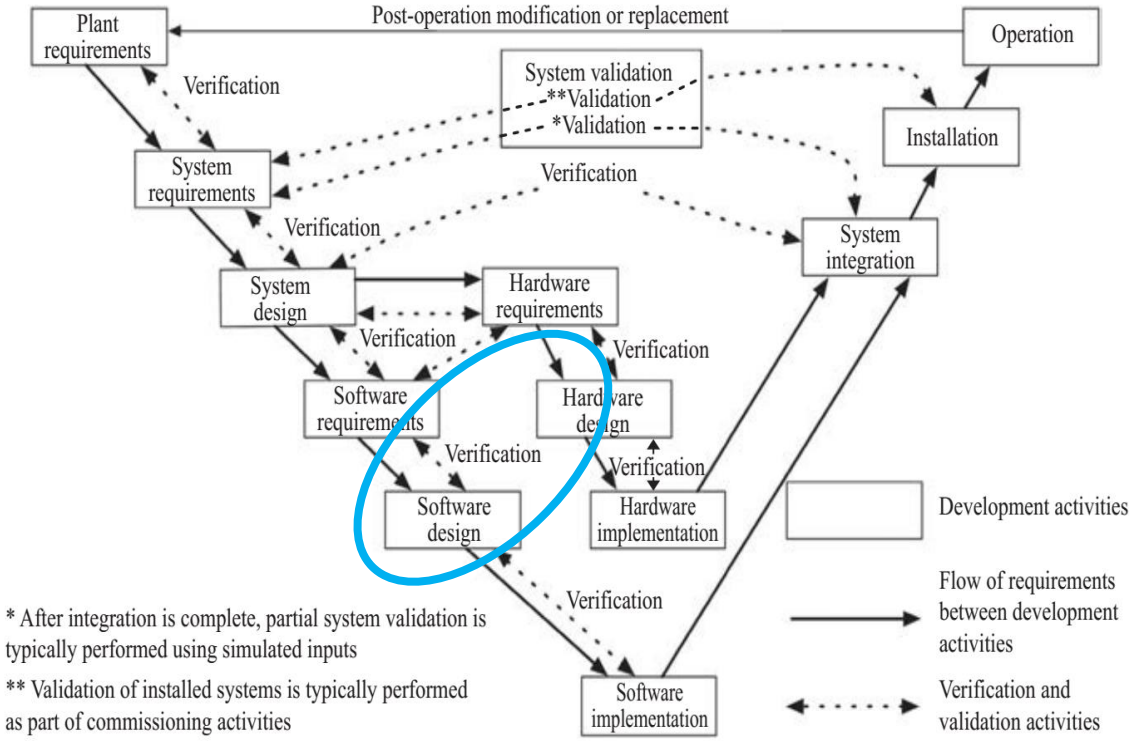


Introduction – Reliability analysis with preliminary I&C design

To perform reliability analysis of I&C systems in early I&C design stage (beginning of hardware and software design) when design changes can still be easily incorporated, is beneficial in the aspects such as:

- To guarantee the fulfillment of the reliability objective
- To provide recommendations and requirements to the I&C and system designers
- To optimize the maintainability of the I&C systems

Typical I&C development process



Analysis method

For digital I&C systems, there are mainly 2 types of reliability analysis methods:

- the classical FMEA - FTA method
- the dynamic reliability methods, such as Dynamic Flowgraph Methodology (DFM) and Markov/CCMT (Cell-to-Cell mapping technique)

The FMEA – FTA method is used for this analysis, because:

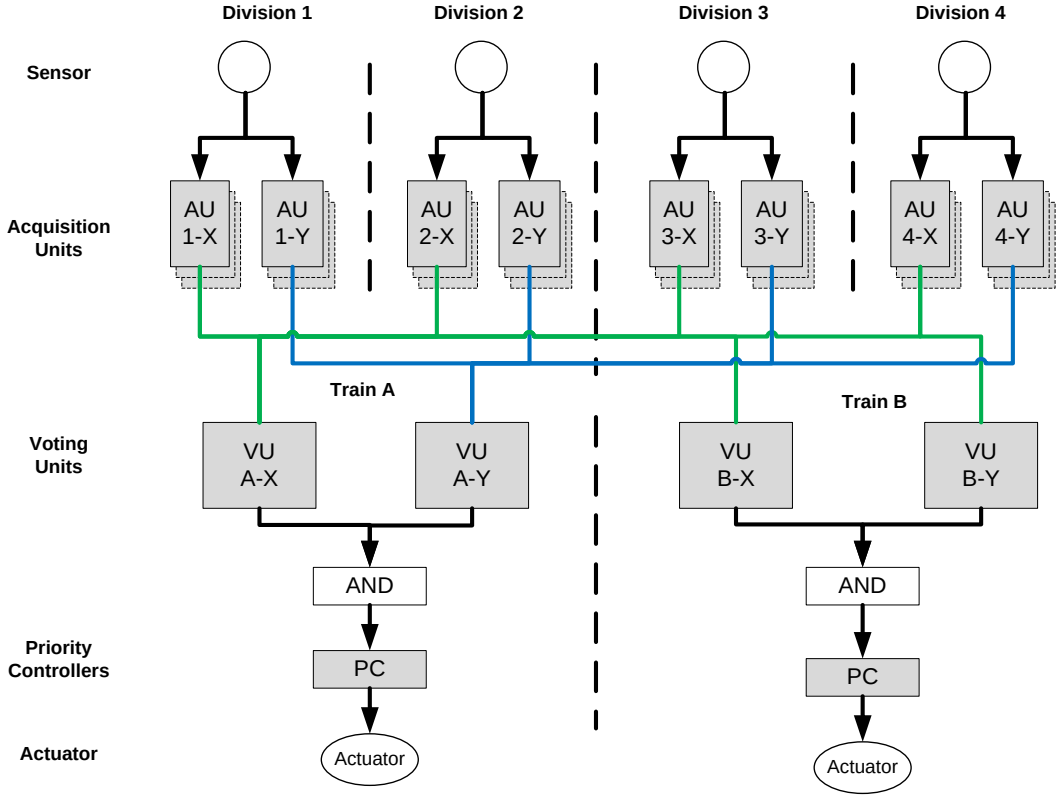
- dynamic methods require large amount of knowledge and detailed input data of the system being studies, which are not available in the preliminary design stage.
- FTA mothed is considered sufficient for protection system (without control loop)

Application case and insights

The reliability analysis is performed in the preliminary design stage of the Reactor Protection System (RPS) in a new build NPP project.

The analysis focuses on the typical automatic Emergency Safeguard Features (ESF) actuation functions, such as the automatic actuation of Safety Injection.

Preliminary I&C architecture of automatic ESF actuation function



Application case and insights

Example of insight on I&C function allocation:

Sensitivity cases are created to compare the following allocation choices:

- Case 3A: Automatic ESF actuation function implemented in both sub-systems
- Case 3B: Automatic ESF actuation function implemented in one sub-system

The result of a typical I&C function shows that comparing to case 3A, the PFD with allocation choice in case 3B has a significant increase of 201%.

Recommendation: As it is impossible to implement all functions in both sub-systems due to the I&C sizing limit, it is recommended to identify critical I&C functions by PSA, and implement when it is applicable such functions in both sub-systems.

Application case and insights

Example of insight on diversification requirement:

Sensitivity cases are created to compare the diversification set-up at Priority Controller (PC) level:

- Case 4A: PC in Train A diversified from the PC in Train B
- Case 4B: No Diversification of PC

The result shows that comparing to case 4A, the absence of PC diversification in case 4B leads to a significant increase of PFD of 1085%. And such result could question the fulfillment of reliability objective. The reason is that at the level of I&C output to actuators, there is no possibility to implement additional redundancy, the failure of a PC module leads directly to the non-actuation of the corresponding actuator.

Recommendation: it is strongly recommended to implement diversification in PC. And if the diversification is not feasible, simple modules (e.g. electronic modules without software application) shall be used so as to lower the possibility of CCF, and detailed analysis shall be performed to evaluate the CCF mechanism and risk.

Application case and insights

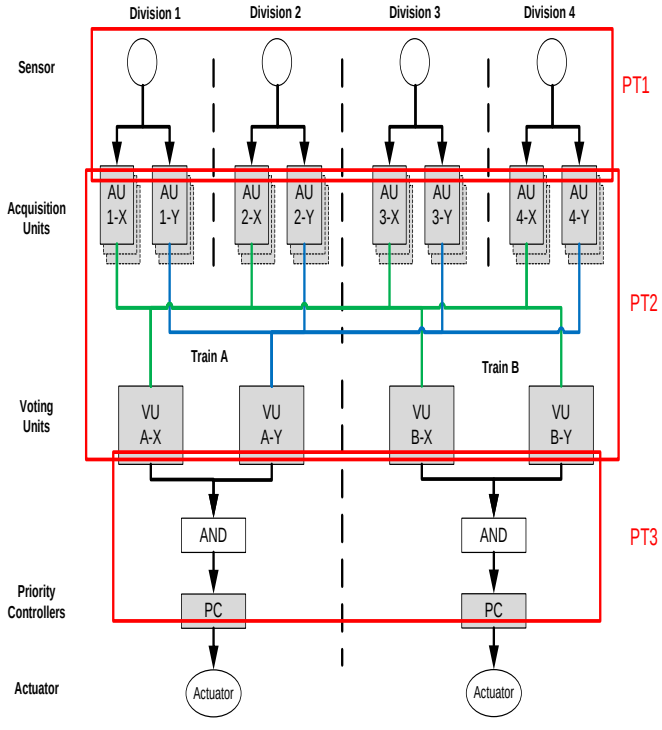
Example of insight on Periodic Test design:

In the preliminary design of Periodic Test (PT) of the RPS, 3 PT are planned with overlapping (see figure on the right):

- PT1: Instrumentation channel test.
- PT2: Processing channel test.
- PT3: Actuator control channel test.

Reliability calculation cases show that the most important PT is the PT3, and the least important one is the PT2. The reason is that the self-test coverage factor is much higher in the upper part of I&C architecture than that in the lower part.

<u>Recommendation:</u> it is recommended to keep as far as possible the PT interval design target (e.g. one PT per division/train per cycle), and in case the reliability objective is exceeded, one choice is that when decreasing the interval of PT3, one can increase the interval of PT1 or PT2 to balance the workload in plant operation.



Conclusion

- It is beneficial to perform reliability analysis in the early I&C design stage.
- Such analysis can reduce the risk of non-fulfillment of reliability design objective, it can also provide useful insights to improve various design aspects.
- One of the most important things to make this analysis successful is to have deep involvement of upstream teams (such as process/safety and fluid system designers) and I&C designer in the analysis.

Thank you

Please contact:

Xuhong He
+46 70 377 1447

xuhong.he@lr.org

Wenjie Qin
+86 21 5157 5759

wenjie.qin@lr.org