Analysis of, and Defense Against, Spurious Actuations and Other Incorrect Behaviors of Digital Control Systems

Thuy NGUYEN
EDF
n.thuy@edf.fr

ABSTRACT

Modern digital instrumentation and control (I&C) systems offer nearly unlimited functional capability. However, the complexity of their design (including their system software and application software) is significantly higher than that of conventional, hardwired systems, to the point that it is generally impossible to demonstrate that there are no residual design errors, even when the best development and verification techniques have been applied. When activated by specific conditions, design errors could result in systematic failures, i.e., failures that occur deterministically each time and wherever an activating condition is present. Redundancy could be defeated when the same design error affects multiple channels or systems, and the activating condition affects several of these channels or systems.

In the case of safety I&C systems, most of the functions are poised protection functions that must be actuated when and only when a demand situation occurs in the plant. In nuclear power plants, the most dangerous failure mode for such functions generally is failure to actuate, and many measures are taken to protect from such failure mode.

This paper considers the other failure modes of safety I&C functions, and also the failure modes of the other I&C functions that are less important to safety. It is not limited to poised functions, and considers other types of functions such as regulation functions or human interface functions. It proposes a framework for analyzing and providing defense against spurious actuations and other incorrect behaviors from digital I&C systems directly interacting with the plant process or with operators: these might be useful for example to justify that design bases for reactor protection are adequate, or to ensure plant performance and availability.

Key Words: Spurious Actuation, Digital Control Systems, Digital Control Room Systems, Failure Analysis

1 INTRODUCTION

Instrumentation and control (I&C) is often considered as the central nervous system of a nuclear power plant (NPP): it concentrates and processes, if not all, then a significant part of the information regarding the plant and its operation. As digital I&C technologies are now offering quasi unlimited functional capabilities, new, recent or recently modernized plants often have advanced I&C functions, e.g., for reactor protection (allowing improved plant performance), process automation, equipment monitoring, diagnostics, prognostics, information display and operator interface, alarms processing and filtering, etc. To provide such high level services, the I&C functions tend to be more interconnected and interdependent, the outputs of one being fed as inputs to others. Besides functional capabilities, modern digital I&C equipment also offer high input-output and processing capabilities, meaning that more I&C functions can be hosted in the same processing unit, sometimes as high as many hundreds or thousands. Thus, the failure of a processing unit can affect large numbers of functions, and the combinations of the individual functions failure modes can be very difficult to predict if no appropriate measures are taken. Also, the more numerous and more complex I&C functions often come together with more complex and interconnected I&C systems architectures and overall I&C architectures, where the failure of one I&C function or one processing unit

could propagate to affect others, again in ways that could be difficult to predict if no appropriate measures are taken.

2 GENERAL APPROACH

The approach presented here is an extension and generalization of the failure modes taxonomy approach proposed in [1] for the purposes of probabilistic risk analysis (PRA) by the Working Group on Risk Assessment (WGRISK) of the OECD-NEA Committee on the Safety of Nuclear Installations (CSNI). The WGRISK taxonomy identifies the possible failure mechanisms that could affect a reactor protection I&C system. The focus on such systems reduces the scope of failure modes and failure effects considerably, since most of the functions of such systems are poised, logical functions (with Boolean output signals) that must be actuated when and only when a demand situation occurs in the plant.

The extension of the WGRISK approach proposed here aims at covering I&C systems and equipment (hereafter called *functional units*) in layers 0 (instrumentation and field devices), 1 (automation systems) and 2 (control room systems) of all safety classes, including those that are not classified as important to safety. The functions of I&C systems other than reactor protection systems are not limited to poised logical functions, and considers regulation functions, human interface functions, etc.

It is based on an underlying failure model shown in Figure 1. After a short typology of defensive measures (Section 3), the paper presents the following taxonomies:

- Taxonomy of initial defects (Section 4).
- Taxonomy of activating conditions or events (Section 5).
- Taxonomy of immediate effects at the boundary of the functional unit concerned (Section 6).
- Taxonomy of effects propagation modes (Section 7).
- Taxonomy of effects induced on other functional units of the same I&C system, on other I&C systems and on the process, including final effects (Section 8).

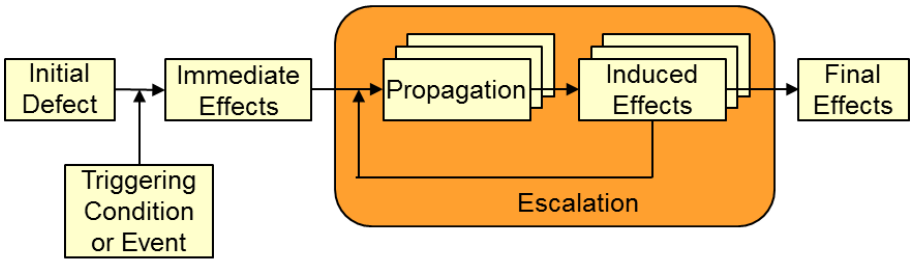

Figure 1. The underlying failure model

Section 9 proposes a modeling and simulation framework that can be used to provide tool support to help I&C designers and assessors understand the interactions of I&C functions and systems, first among themselves, and then with the various items of their environment (process, systems and humans). Tool-supported modeling and simulation is most useful to explore large numbers of situations and failure scenarios, and to understand complex interactions, particularly when large numbers of I&C functions are involved, as is generally the case of nuclear power plants digital control systems.

Ultimately, the collective purpose of these taxonomies and of the modeling and simulation framework is to provide a framework that helps I&C system designers identify suitable defensive measures, and that helps system assessors evaluate the effectiveness of the measures, also taking into account their possible side effects.

3 TYPOLOGY OF DEFENSIVE MEASURES

Defensive measure may be applied at each level of the failure model, and can be classified according to their basic principles:

- **Avoidance measures** eliminate altogether a cause or mechanism. E.g., one can eliminate the potential for software defects by having no software in the system. However, though very effective, such radical measures are not always possible or even desirable.
- **Preventive measures** do not completely eliminate a cause or mechanism, but aim at limiting its likelihood or potential. E.g., to continue on the preceding example, one can make sure that software is used only where necessary, and then that necessary software is kept as simple as possible.
- **Detection measures** aim at removing defects or at initiating actions to mitigate harmful effects or prevent further propagation.
- **Mitigation measures** aim at tolerating as best as possible the effects of failures, should they occur.

Some of these measures are applied during the development (including verification and validation) of the I&C system or when the I&C system is off-line and not in operation. Others are taken outside of the I&C system concerned.

Measures active during system operation are subject to failures of their own, and care needs to be taken to ensure that the cure is worthwhile and not worst than the initial problem.

4 TAXONOMY OF INITIAL DEFECTS

In digital systems, and in digital I&C systems in particular, initial defects can be divided into two main categories: defects that are present in the system right from the beginning (i.e., when the system is commissioned and put into operational use), and defects that appear or are created in the system during operational use.

The first category can be further subdivided into:

- Defects in functional requirements specification.
- Defects in system design, including in complex electronic logic, in generic system software (that is part of the I&C platform used), in application-specific software, in hardware or in system architecture.
- Defects in manufacturing or installation.

The second category can be further subdivided into:

- Random hardware defects.
- Human errors during operation or maintenance. These are not addressed in this paper.
- Malicious attacks. These are not addressed in this paper.

4.1 Defects in functional requirements specification

Operational experience in industrial sectors with high dependability requirements for digital systems shows that a significant residual cause of failure lies in inadequate specification of functional requirements (see [2], [3] and [4]), in part due to the fact that as digital technologies now offer nearly unlimited functional capability, plant, process and operations engineers tend to have increased, sometimes excessive, functional

ambitions. This often leads to high functional complexity and could result in functional requirements that are not adequate in particular situations. These situations could be internal to the I&C system (e.g., failures or particular normal states) or external to it.

There are different possible causes for such defects. Some may result from an incomplete understanding of the situations the I&C system may face or of the role of the I&C system in the plant or for operation. In such cases, the error is already in the mind of the specifier, and if the same person is also responsible for the specification of other functions or systems, then there is a potential for other related functions or systems to be affected by the same or similar defects.

In other cases, the specifier has an adequate understanding of what should be required of the I&C function or system, but does not translate it correctly into specification. This would be less likely to affect related functions or systems.

As elimination measures are not really possible, one can rely first on preventive and detection measures to limit the potential for such defects. That could include the use of adequate requirements analysis and specification methods, training, reviews, independent verification. They could (and should) also include close coordination with the other engineering disciples and teams involved in the environment of the I&C system, possibly with the co-modelling and co-simulation of I&C requirements and the environment of the I&C system (see Section 9).

Mitigation measures could include functional diversity, so that more than one function can deal with a given critical situation. Such measures are usually applied for safety functions. However, in the case of functions less important to safety but critical to plant performance, it might be worthwhile to identify, among the other functions that exist anyway, those that could act as backups or that could provide mitigation. When such functions do exist, measures should then be taken to limit the potential for common-cause failure.

4.2 Defects in system design

The design complexity of digital systems is most of the time significantly higher than that of conventional, hardwired systems, to the point that is is generally impossible to demonstrate that there are no residual design errors, even when the best and most rigorous development and verification techniques have been applied. Regarding design defects, one often thinks of defects in software or complex electronic logic. However, there could also be defects in hardware design and also in system design (where a defects does not lie in a specific hardware or software component, but in inadequate interactions or interconnections between otherwise perfect components).

Possible measures to limit the potential for such defects include the use of adequate design methods, training, elimination of unnecessary complexity, reviews and inspections, rigorous verification and validation, independent verification. Such measures have been very effective in the case of safety I&C systems, as shown by [2], due to very rigorous application. However, in the case of systems less important to safety, they are difficult to apply with the same level of rigor. One possible set of measures is to identify and segregate the functions critical to plant performance, and to subject them to adequately rigorous development.

4.3 Defects in manufacturing or installation

These include defects such as manufacturing defects in particular types of components, wiring errors, errors made when configuring the parameters of smart components, etc. Though rigorous suppliers selection and products inspections & testing aim at limiting the potential for such defects, operational experience shows again that they cannot be neglected (see [2]).

4.4 Random hardware defects

These are defects that affect all systems including conventional hardwired systems. One can distinguish:

- Transient or permanent defects.
- Single or correlated defects. Correlated random defects may occur for example when a "shock" concurrently affects multiple hardware components.

Each type of component or functional unit has its specific set of possible failure modes, and the effects and propagation of a component failure will depend on the place and role of the component or functional unit in the system (sensors, signal conditioning modules, actuator controls, priority logic modules, controllers, point-to-point or network communication links, gateways, data communication switches, human-system interface devices, ...).

Possible defenses include components qualification (preventive), redundancy (mitigation), self or external monitoring for diagnostics or prognostics (detection), periodic testing (detection).

5 TAXONOMY OF ACTIVATING CONDITIONS

A defect in a system state that does not necessarily translate immediately into a failure, i.e., an incorrect system behavior: for this, it needs to be activated by a specific condition (or event) which depends on the defect. For a given defect, the activating condition or event can be:

- Immediate or delayed. It is immediate when the defect is activated into a failure by the normal operation of the system. It is delayed when only a specific condition not occurring routinely, is necessary.
- Local or spread out in space. A local condition is likely to affect only one or a limited number of components and systems. A condition that is spread out in space could affect multiple components and systems.
- Instantaneous or spread out in time.
- Internal to the I&C system, related to the process being controlled, related to operators actions, or related to other technical systems.

Defensive measures concerning activating conditions generally aim at prevention and detection. Preventive measures often aim at ensuring stable or well-bounded conditions: this could concern ambient conditions as well as processing conditions (e.g., computing, input-output or communication loads, or use of computing resources such as memory). They can also aim at limiting inputs to the strict necessary. Detection measures may be used to provide early warning when approaching or reaching abnormal conditions, so that automatic or manual mitigation measures can be taken.

6 TAXONOMY OF IMMEDIATE EFFECTS

At the boundary of a functional unit, the immediate effects of the activation of a defect can be one of, or a combination of:

- No effects.
- Absence of action and / or communication: the functional unit does not perform what it should.
- Spurious action and / or communication (including communication storm): the functional unit performs what it should not.

- Untimely (i.e., to early or too late) action and / or communication, to various degrees.
- Action and / or communication with detectable incorrect values: then, upon detection, appropriate measures can be taken to mitigate the consequences and / or limit propagation.
- Action and / or communication with incorrect but plausible values. Such effects are difficult to defend against. When they affect functions important to safety or plant performance, one could determine by analysis whether the end effects are acceptable. If not, then one could for example try to make the incorrect values detectable (e.g., by having redundant or diverse information).

The immediate effects can also be:

- Limited to an individual functional unit, or on the contrary, affect a group of functional units in an I&C system, or a complete I&C system.
- Limited in scope (i.e., affecting only a limited number of actions), or to the contrary, extensive and affecting a large number of actions. As input-output and processing capabilities have improved considerably, event effects limited to an individual controller can have an extensive scope.
- Intermittent or permanent. Intermittent effects are often the more problematic, since they are more difficult to detect and characterize, and their initial defects more difficult to identify and correct. Continuous monitoring
- Predetermined (where they are known and determined by specification of design), or on the contrary, haphazard (where one cannot predict what the effects will be). For I&C functions critical to plant performance, as is already the case for safety I&C functions, it is generally preferable to avoid haphazard effects.

7 TAXONOMY OF PROPAGATION MODES

Failure effects can propagate according to various modes:

- Propagation along functional dependencies: when a function displays an incorrect behavior, other functions that depend on it may also be affected and behave incorrectly, and then affect other functions.
- Propagation due to partial or complete hardware failure. This can be illustrated by two examples. Example 1: due to a software error, a controller performs a division by zero; this causes an exception that freezes the controller; all I&C functions of this controller are lost. Example 2: a defect in a hardware communication component causes a data communication storm; the corresponding data communication link is overloaded; communication through this link is slowed down or stopped; the I&C functions that depend on the link are affected.
- Propagation by invasion. Example: due to a software error, an incorrect pointer value is computed; the pointer is used to write data in memory; other functions of the computing unit may be affected.
- Indirect propagation, through the environment of the functional unit or of the I&C system, e.g., via the process, human operators or other technical systems.

8 TAXOMONY OF INDUCED EFFECTS AND FINAL EFFECTS

The induced and final effects may be classified according to the importance of their consequences for the plant:

- The induced effects (and consequently the final effects) may remain completely internal to the I&C system, which can still performs its missions as required, e.g., due to redundancy, fault-tolerance, repair in operation.
- The induced effects may prevent the I&C system to perform all its missions as required, but the downgraded behavior has no or limited impacts at plant level: e.g., the required safety actuations have been performed, or normal plant operation is not interrupted.
- The induced effects may be impossible to determine in advance with certainty (e.g., due to haphazard immediate effects, or haphazard propagation), and one cannot guarantee that the downgraded behavior will have no or limited impacts at plant level.
- The induced effects may result in behavior that is unacceptable at plant level: e.g., the required safety actuations have not been performed, or normal plant operation is interrupted.

9 METHOD

9.1 Process analysis

When addressing digital I&C systems of low or no importance to safety, one is often confronted with a very large number of functions, often in the hundreds and sometimes in the thousands. Thus, a failure analysis based primarily on the I&C functions could, and generally will, rapidly be overwhelmed by combinatorial explosion. A more practical approach could be based on a process analysis identifying the actuations by the I&C system being considered that would be most detrimental to safety and / or plant performance.

To facilitate this analysis, a simulable process model could be most useful, particularly when considering the very large number of scenarios to be considered, and the complexity of nuclear power plant processes. Particularly when aiming at plant performance, manual analysis is likely to be a lengthy and error-prone task. For tool-supported analysis however, there are a number of issues to be resolved:

- With conventional process modeling approaches, developing a comprehensive process simulator is a very significant undertaking, and such a simulator is often available only in the final stages of the plant development, too late for the purposes of I&C design.
- As the number of cases and scenarios to be analyzed could be extremely high, it is important to be able to automatize the exploration process. This would also facilitate the re-analysis and the re-exploration of the cases and scenarios when the plant process is modified and with different I&C design options.

9.2 Advanced modeling and simulation

A constraints-based modeling and simulation approach have been developed at EDF in the framework of the European collaborative project ITEA2 MODRIO (MOdel DRIven physical systems Operation). Models developed using conventional 3D physics modelling languages (e.g., based on finite elements) or 0D-1D multi-physics modelling languages (such as Modelica [5]) are essentially deterministic models: given precise initial and boundary conditions, they determine one and only one behavior and trajectory (see Figure 2). While extremely useful for the analysis of detailed designs, they cannot be used at early design stages when no precise physical equations are determined yet. Also, when dealing with complex problems where very high numbers of simulation runs are necessary to ensure a reasonable level of exploration, operational cases and simulation results need respectively to be produced and assessed one by one, which is costly, error-prone and impractical.

The FORM-L language (FOrmal Requirements Modelling Language [6] and [7]) developed by EDF within the MODRIO project proposes a very different approach to modeling that is better suited to complex and large systems, and also to upstream activities at early stages of systems lifecycles. It is based on *constraints* that do not define individual trajectories, but envelopes of acceptable trajectories (see Figure 2). Thus, the language can deal with uncertainties, provides a basis for automatic generation of operational cases (conforming envelopes formally specified as *assumptions*) and automatic simulation results assessment (against envelopes formally specified as *requirements*). It is applicable to all kinds of dynamic phenomena: not only physical phenomena or I&C functions, but also economic costs and revenue; not only in normal situations, but also in exceptional or failure situations.

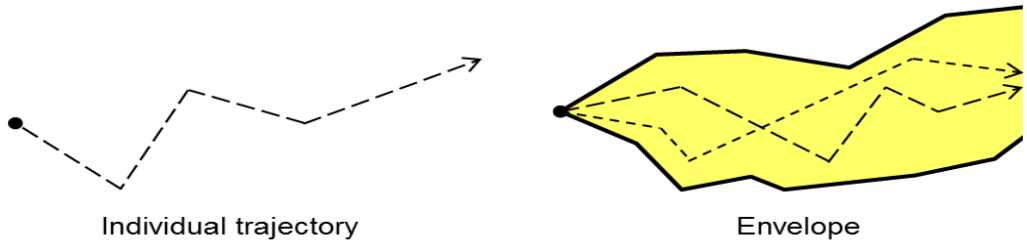

Figure 2. Individual trajectories versus envelopes allowing multiple trajectories.

For the particular case of failure analysis for I&C systems, FORM-L allows the modeling of I&C functional requirements (including accuracy and response times aspects) and of physical processes at different levels of abstraction, so that dynamic phenomena of importance are represented in detail, whereas the others are represented only by overall envelopes. It also allows the modeling of *events* representing the occurrence of defects of various types. Other events may be used to represent the occurrence of activating conditions, which could lead to *single* or *common-cause failures* and their effects. So-called *multi-mode modeling* may be used to model in a modular manner the effects and behavior associated with each failure mode.

9.3 Validation of I&C functional requirements specification

Section 4.1 introduces the notion of defects in I&C functional requirements specification. An approach for minimizing the potential for such defects was presented at the ANS NPIC-HMIT 2015 in Charlotte. It is based on a FORM-L based co-modeling and co-simulation of the power plant process and of the specified I&C functional requirements, in order to verify that under various situations (including abnormal and failure situations), the fundamental plant-level requirements are satisfied.

9.4 Constraints-based allocation of I&C functions to functional units

FORM-L also allows the modeling and the analysis of postulated failure effects propagation. However, a more analytic approach to this issue is often possible. One of the results of the previous analysis is the identification of I&C functions that should not fail concurrently. For plant performance purposes, defensive measures could be less drastic and more cost-conscious than when safety is at stakes. In many cases, segregation of concerned I&C functions or data communications into separate controllers or data communication links is sufficient.

EDF has developed a tool that allocates the specified I&C functions and their data communications to functional units, based on a number of specified constraints. Some of these constraints are related to response time requirements and to the computational and input-output needs of each function, considering the capabilities of the underlying I&C platform. Other constraints express segregation requirements: the tool allocates functions that must be segregated to different functional units or controllers, or even to different segments (i.e., groups of interconnected functional units and controllers).

10 CONCLUSIONS

The analysis of I&C failures and their consequences is a complex issue, particularly when aiming at minimizing adverse effects on plant performance. This is in a large part due to the high number of I&C functions and to the size and complexity of nuclear power plant processes. Also, as I&C and the plant process have numerous and complex interactions, appropriate solutions are usually not all on the I&C side or the process side, but are based on adaptations of both.

The approach proposed relies in a large part on constraints-based co-modeling and co-simulation: this allows tool-supported analyses at early stages of plant development, when the plant design is not cast in concrete yet. Also, this form of modeling provides powerful means to manage the immense complexity of nuclear power plants.

Currently, tools supporting FORM-L are under development at EDF R&D. Their use will not be limited to the I&C and processes of nuclear power plants: they are also at the heart of other EDF R&D projects, such as the SIMSE project which aims at providing methods and tools for the modeling and simulation of power grids of all sizes, from small local smart grids to national or even continental power grids.

11 REFERENCES

1. NEA/CSNI/R(2014)16 “Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis” https://www.oecd-nea.org/nsd/docs/2014/csni-r2014-16.pdf (February 2015).
2. EPRI TR-1016731 "Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems" (December 2008)
3. EPRI TR-1002835 "Guideline for performing Defense-in-Depth and Diversity Assessments for Digital Upgrades" (December 2004)
4. N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, The MIT Press (2011).
5. P. Fritzson, *Principles of Object-Oriented Modeling and Simulation with Modelica 3.3*, IEEE Press (2015)
6. Thuy Nguyen, *FORM-L specifications*, EDF R&D report No. H-P1A-2014-00535-EN (2016)
7. Thuy Nguyen, *FORM-L: A Modelica Extension for Properties Modelling, Illustrated on a Practical Example*, Proc. 2014 10th Int. Modelica Conf. https://www.modelica.org/events/modelica2014/proceedings/html/submissions/ECP140961227_Nguyen.pdf