Spurious Actuations in Digital Instrumentation and Control Systems - Evaluation Framework

Mr. Ismael L. Garcia, P.E.
U.S. Nuclear Regulatory Commission
11545 Rockville Pike, Rockville, MD 20852-2738
Ismael.Garcia@nrc.gov

ABSTRACT

When a digital Instrumentation and Control (I&C) system or its associated components produce an unintended operation, it is known as a spurious actuation. Spurious actuations could lead to unnecessary challenges to safety equipment, challenge the ability of safety systems to provide their intended functions, or place the plant in an un-analyzed state. There is arguably a lack of clear and sufficient regulatory guidance for assessing spurious actuations. In an attempt to address this guidance gap, this paper provides a generic framework for evaluating spurious actuations in digital I&C systems, components, or supporting systems that are important to safety.

The framework provides a methodology for: (1) defining the scope of the evaluation including supporting assumptions; (2) providing options for excluding a spurious actuation from the evaluation; (3) assessing the potential consequences from the assessed spurious actuations; and, (4) defining a high-level acceptance criteria. The methodology discussed by this paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators; instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for assessing spurious actuations in digital I&C systems.

Key Words: actuation, control, digital, instrumentation, spurious

1 INTRODUCTION

There are two inherent safety functions that safety-related systems provide. The first function is to provide a trip or system actuation when plant conditions necessitate such action. The second function is to not trip or actuate when not required by plant conditions in order to avoid challenges to the safety systems and to the plant. When an I&C system or its associated components produce an unintended operation, it is known as a spurious actuation.

A spurious actuation can be caused by, but not limited to, single failures, common cause failures [1], maintenance testing errors, design errors, or missing requirements. Triggering events such as environmental effects and plant transients can also cause a spurious actuations. Design attributes such as independence and diversity would help mitigate the risk of a spurious actuation. Modern digital I&C systems can have interconnectivities, dependencies, and commonalities that can facilitate fault propagation thus leading to a potential spurious actuation of more than a single train of plant equipment. Therefore, a spurious actuation of multiple trains of plant equipment may be attributed to inadequate independence among redundant portions of I&C systems, lack of adequate diversity to address dependencies, or commonalities that result from functional or plant process configurations, which are not addressed during the design development or the equipment qualification phases.

Based on the potential adverse effects that spurious actuations could have on safety, their impact needs to be evaluated. Specifically, spurious actuations could lead to unnecessary challenges to safety equipment, challenge the ability of safety systems to provide their intended functions, or place the plant in

an un-analyzed state with respect to its safety analysis. Spurious actuations of concern would be those which are plausible and that have not been addressed in the I&C system design. For example, a potential spurious actuation may not be of concern if the cause was the result of multiple independent systems failing. As such, the potential for this spurious actuation may be considered implausible. However, a potential spurious actuation due to a single system failing may be considered plausible if it relies on the failed system to prevent itself from causing the spurious actuation.

Spurious actuations are a cross-cutting safety issue that can affect multiple disciplines. Adequate resolution to this issue may necessarily involve personnel with expertise in safety analysis, human factors, I&C, electrical, probabilistic analysis, etc. Therefore, evaluating spurious actuations necessitates a multi-disciplinary approach to ensure that the consequences of spurious actuations on plant safety are fully understood and accounted for.

Currently, there is arguably a lack of clear and sufficient regulatory guidance for assessing spurious actuations. Regulators abroad agree that guidance for evaluating spurious actuations is warranted given the increase use of digital I&C systems in new reactor designs and its safety implications. Such feedback is based on recent experience by domestic and international regulators with new reactor application reviews and operating plant issues as well as an examination of the regulatory requirements, relevant industry standards, and international documents.

1.1 Definition of Terms

The following definitions are specific to this paper:

- **Architecture:** Organizational structure of the I&C systems of the plant which are important to safety [2].
- **Common Cause Failure:** Failure of two or more structures, systems, or components due to a single event or cause [3].
- **Defect:** A problem which, if not corrected, could cause an I&C component or system to either fail or to produce incorrect results [4].
- **Diversity:** The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure [3].
- **Failure:** Loss of the ability of a structure, system, or component to function with acceptance criteria [3].
- **Fault:** Defect in a hardware, software or system component [2]. (Note: An error may lead to a fault, a fault may lead to a failure, and failure may lead to a hazard, and a hazard may lead to harm.)
- **Graded Approach:** A process or method in which the stringency of the control measures and conditions to be applied is commensurate, to the extent practicable, with the likelihood and possible consequences of, and the level of risk associated with, a loss of control [3].
- **Hazard:** Potential source of harm [5].
- **Independence:** [Property that is exhibited between two or more systems or components] that possess both of the following characteristics: (a) the ability to perform their required function is unaffected by the operation or failure of the other [systems or components]; and (b) the ability to perform their function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which they are required to function [3].

- **I&C system:** System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself [2].
- **Item important to safety:** An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or member of the public [3].
- **Plausible:** Not eliminated by justified and documented technical means. (Note: The term "plausibility" is used in reference [6]. In the context of reference [6], the term "plausibility" is used to characterize an example of a design feature (segmentation) that could be used to reduce the likelihood of a spurious actuation such that it can be justifiably eliminated from consideration.)
- **Postulated Initiating Event:** An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. (Note: The primary cause of a postulated initiating event may be credible equipment failures and operator errors (both within and external to the facility) or human induced or natural events [3]).
- **Spurious Action:** Unintended operation of an I&C system or component(s) that may result in a failure of some of the items important to safety to fulfil the actions required in response to a postulated initiating event [6].
- **Spurious Actuation:** Unintended operation by an I&C component or system.
- **Safety Analysis:** Evaluation of the potential hazards associated with the conduct of an activity. (Note: Safety analysis is often used interchangeably with safety assessment. However, when the distinction is important, safety analysis should be used for the study of safety, and safety assessment for the evaluation of safety — for example, evaluation of the magnitude of hazards, evaluation of the performance of safety measures and judgement of their adequacy, or quantification of the overall radiological impact or safety of a facility or activity [3]).
- **Safety Group:** The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded [3].
- **Safety System:** A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents [3].

1.2 Evaluation Framework

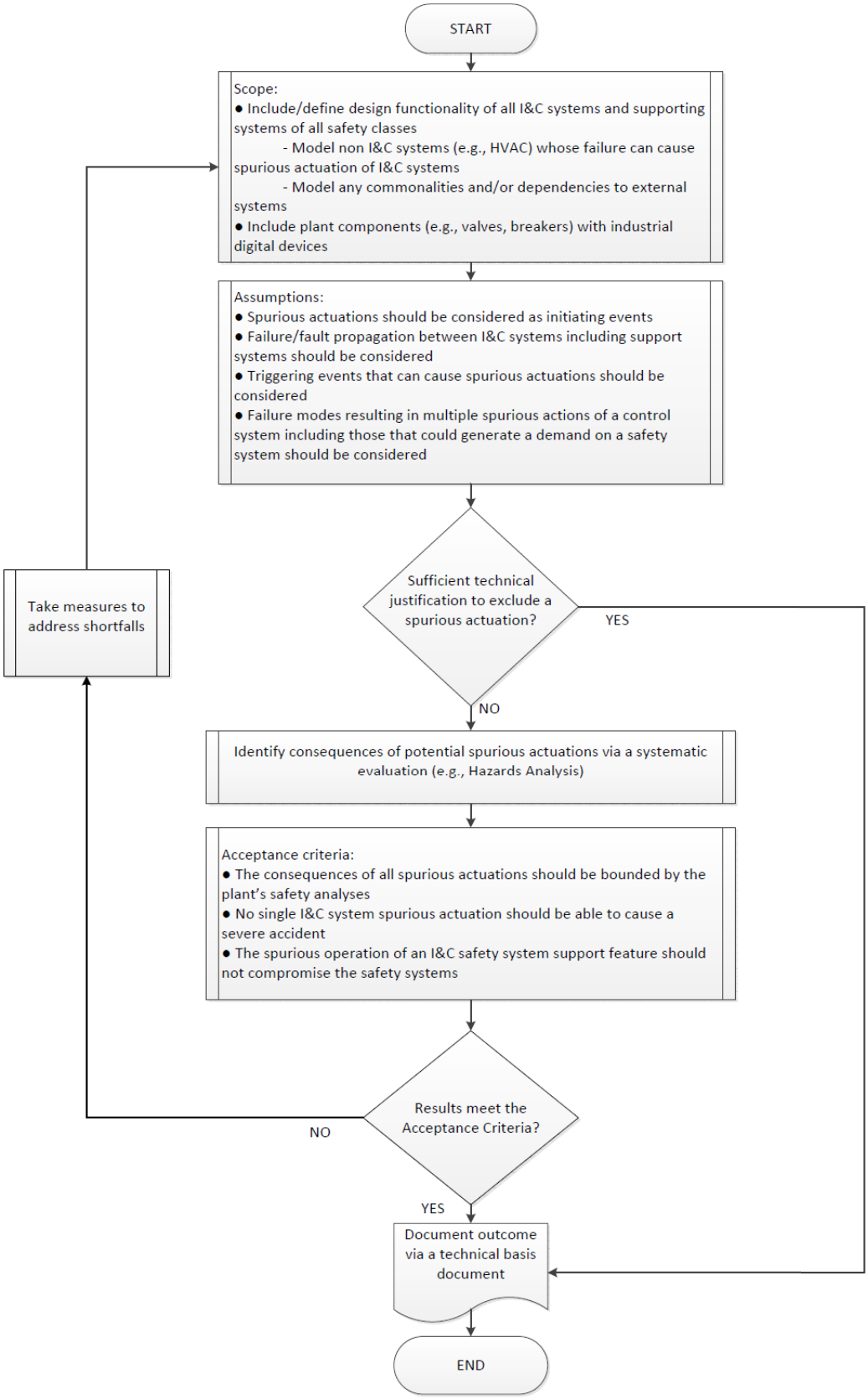

Figure 1. Spurious Actuations in Digital Instrumentation and Control Systems – Evaluation Flowchart.

Fig. 1 above shows a generic framework for evaluating spurious actuations in digital I&C systems, components, or supporting systems that are important to safety. As shown in Fig. 1, the framework provides a methodology for:

1. Defining the scope of the evaluation including supporting assumptions;
2. Providing options for excluding a spurious actuation from the evaluation;
3. Assessing the potential consequences from the assessed spurious actuations; and,
4. Defining a high-level acceptance criteria for performing an adequate evaluation of spurious actuation of an I&C system.

Sections 1.2.1 through 1.2.5 below discuss some of the key takeaways from this generic framework. The methodology discussed herein assumes that there is sufficient independence and diversity between different safety classes of I&C systems. However, it is acknowledged that complete independence and diversity may not be present to address dependencies or commonalities that result from functional or plant process configurations.

This paper does not prescribe a particular evaluation approach as there may be different approaches when performing the evaluation for the identification of the consequences of postulated spurious actuation(s) (e.g. system based, function based, component based, or combination thereof). However, the approach taken for performing the evaluation of spurious actuations should be justified for suitability for the particular application.

1.2.1 Scope

Despite the fact that the methodology discussed herein is focused on spurious actuations in digital I&C systems, components, or supporting systems that are important to safety, the scope of the assessment should include the functionality of all I&C systems and supporting systems of all safety classes. Such a comprehensive assessment is necessary as there may be interconnections between I&C systems of different safety classes; thus errors in one redundant channel or division or lower class systems could cause the failure of another redundant channel or division or higher class systems.

Ways in which control system faults, including multiple spurious faults, could generate a demand on a safety system should also be considered as they could lead to adverse safety conditions [6]. Plant components such as pumps, valves, breakers that contain industrial digital devices should be considered in the analysis (Note: References [7] and [8] provide information related to industrial digital devices).

1.2.2 Assumptions

As part of the evaluation, the user should define the assumptions concerning the occurrence of non-time concurrent multiple spurious actuations or spurious actuations in combination with independent postulated initiating events. It is infeasible to determine the worst combination of all positions in time of all such spurious actuations as it would require performing an infinite number of studies. Therefore the occurrence of such spurious actuations should be avoided, or their likelihood reduced to an acceptable level, by justified and documented technical means.

For this reason, the use of appropriate architectures and design attributes (e.g., independence and diversity) to (1) avoid the occurrence or (2) reduce its likelihood to an acceptable level of multiple spurious actuations or spurious actions in combination with independent postulated initiating events might be used as a justification for exclusion as long as sufficient demonstration is provided [6]. A similar approach could be followed to eliminate a given spurious actuation occurrence from further consideration.

1.2.3 Assessment of Consequences

A systematic evaluation such as a Hazard Analysis should be used to assess the potential consequences of all postulated spurious actuations [9]. The evaluation should employ the use of analysis

techniques that can assess the hazards introduced through interconnected digital systems and devices. The feedback paths enabled when the digital elements are networked could lead to the potential propagation of design flaws or any other unsafe interactions.

1.2.4 Acceptance criteria

The goal of the evaluation should be to ensure that the consequences of all postulated spurious actuations are bounded by the plant's safety analyses. In other words, if the potential effects of the spurious actuations do not invalidate or exceed the assumptions or results of the plant's safety analyses, then the potential consequences of a spurious actuations are bounded. Alternatively, the evaluation could identify the worst case spurious actuation and ensure that its consequences are bounded. A given spurious actuation of an I&C system or component(s) could be considered worst case if its potential consequences envelope those from other potential spurious actuations.

The items below provide additional guidance concerning the acceptance criteria for evaluating spurious actuations in digital I&C systems, components, or supporting systems that are important to safety:

1. For an I&C system-induced initiating event, the acceptance criteria should be derived with a graded approach from the lowest safety class within the I&C architecture. Less consequences of a failure should be allowed for I&C systems with lower safety classification. Nevertheless, the potential for failures in the system of the lower safety class that could cause spurious actuation of safety classified components should be assessed and shown to be acceptable.
2. The spurious operation of a support feature for an I&C safety system should not compromise the independence between redundant portions of safety systems, between safety systems and systems of a lower safety class, or between different levels of the concept of defense in depth applied at the plant.
3. For an I&C component failure, the acceptance criteria should be derived from failure tolerance criteria (e.g. deterministic design criteria) of a system. As far as practicable, the failure of a component should not cause spurious actuation of any safety system. Component level failure modes should be considered in the scope of the failure modes and effects analysis (or FMEA). (Note: Plausible failures to actuate on demand should be taken into account when defining the conservative single failure assumptions for thermal-hydraulic deterministic safety analysis.)

If the evaluation fails to meet the acceptance criteria, then the user should take hazards control measures to address the shortfall(s) [9]. For example, the user should evaluate the implementation of design attributes such as independence and diversity to avoid the occurrence, or to reduce the likelihood of a spurious actuation to an acceptable level. Subsequently, the user should re-assess the effects of the measures taken to address the shortfall(s) by repeating, as necessary, the evaluation framework shown in Fig. 1.

1.2.5 Additional Considerations

Hazard control measures such as crediting of manual actions identified as a result of this evaluation should be an acceptable option for controlling identified hazards. Such measures should align with guidance provided in reference [9] with regard to controlling of identified hazards. The availability of indications for the operator to recognize that a spurious actuation has occurred could be important for the identification of hazard control measures. For example, a plant parameter can be indicated to the operator such that the operator may be able to determine if a manual action is necessary to cope with the consequences of the spurious actuation.

A preliminary evaluation for spurious actuation should be performed during the early design stages of the I&C component, system or architecture. The results of the preliminary evaluation should be used to inform the I&C component, system and architecture design and should be validated during the later stages

of the design development. The final results of the evaluation should be reviewed and re-evaluated when necessary. Examples of when such a review may be required include changes to the I&C components, systems, architecture or supporting systems, and mandatory periodic reviews [10].

2 CONCLUSIONS

There may be different approaches when performing the evaluation of spurious actuation(s). This paper does not prescribe a particular approach but instead provides a sample framework for evaluating the consequences associated with spurious actuation. Nonetheless, the approach taken for performing the evaluation of spurious actuations should be justified for suitability for the particular application.

The methodology discussed by this paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators. Instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for assessing spurious actuations in digital I&C systems.

3 ACKNOWLEDGMENTS

This paper was derived from the ongoing work being performed by the Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG), which I have the honor and privilege to chair. For additional information concerning the MDEP DICWG visit: https://www.oecd-nea.org/mdep/

(Note: The goal of the MDEP DICWG is not to independently develop new regulatory standards. As such, the technical work develop by the MDEP DICWG is not legally binding and do not constitute additional obligations for the regulators or the licensees. Instead, the technical work resulting from the MDEP DICWG constitutes guidelines, recommendations, or assessments that the MDEP participants agree are good to highlight during their safety reviews of new reactors. The development of technical guidance for assessing spurious actuations in digital I&C systems or components follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents.)

4 REFERENCES

1. "MDEP Generic Common Position DICWG No. 01: Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems," https://www.oecd-nea.org/mdep/common-positions/dicwg-01.pdf (2013).
2. "IEC 61513, Ed.2: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," (2011).
3. "IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection," http://www-pub.iaea.org/MTCD/publications/PDF/Pub1290_web.pdf (2007).
4. "ISO/IEC 20926: Software engineering. IFPUG 4.1 Unadjusted functional size measurement method. Counting practices manual," (2003).
5. "ISO/IEC Guide 51: Safety aspects - Guidelines for their inclusion in standards," (1999).
6. "IAEA SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants," http://www-pub.iaea.org/MTCD/publications/PDF/Pub1694_web.pdf (2015).

7. “IEC 62671: Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality,” (2013).
8. “MDEP Generic Common Position DICWG No. 07: Common Position on Selection and Use of Industrial Digital devices of Limited Functionality,” https://www.oecd-nea.org/mdep/common-positions/DICWG_GCP-DICWG-07.pdf (2014).
9. “MDEP Generic Common Position DICWG No. 10: Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems,” https://www.oecd-nea.org/mdep/common-positions/MDEP_GCP-DICWG-10_HazardIDandControl.pdf (2016).
10. “IAEA SSG-25: Periodic Safety Review for Nuclear Power Plants,” http://www-pub.iaea.org/MTCD/publications/PDF/Pub1588_web.pdf (2013).