MDEP Common Position CP-DICWG-13

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON SPURIOUS ACTUATION

Participation

Regulators involved in the MDEP working group discussions:	All MDEP members
Regulators which support the present common position	All MDEP members
Regulators with no objection:	-
Regulators which disagree	-
Compatible with existing IAEA related documents	Yes

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO 13: COMMON POSITION ON SPURIOUS ACTUATION

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given the increase of use of Digital Instrumentation and Controls (I&C) in new reactor designs, its safety implications, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and IAEA documents. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues[1].

Context:

Spurious actuations produced by I&C systems are a safety concern if such actuations could challenge plant safety. Spurious actuations can 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-analysed state.

Spurious actuation of plant equipment can be caused by factors including, but not limited to, single failures, common cause failures, human (e.g. operator) action, maintenance errors, design errors, or missing requirements. Modern I&C systems can have interconnectivities, dependencies and commonalities that can, if the overall I&C architecture and the individual I&C systems are not adequately developed and operated, facilitate fault propagation, leading to potential spurious actuation of one or more trains of plant equipment. Sources and contributors of spurious actuations of multiple trains of plant equipment may include inadequate independence among redundant portions of I&C systems, inappropriate allocation of I&C functions, inadequate qualification or design of supporting systems (e.g. heating, ventilation and air conditioning (HVAC) system), or non-classified systems that could have been erroneously classified.

Spurious actuations are a type of hazard. Generic Common Position (GCP) DICWG-10 "Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems" provides a set of common positions pertaining to identifying and controlling hazards in an I&C system. This common position was developed to add special considerations when identifying and controlling hazards that include spurious actuations. It is expected that GCP DICWG-10 and the common positions in this document be used together for a complete analysis of hazards and their controls (e.g. prevention of spurious actuations

[1] The goal of MDEP is not to independently develop new regulatory standards. Common Positions are not legally binding and do not constitute additional obligations for the regulators or the licensees but are guidelines, recommendations, or assessments that the MDEP participants agree are good to highlight during their safety reviews of new reactors. Any MDEP member may decide to implement the common positions through its national regulatory process.

in the design of the system/component). Spurious actuations of concern would be those which are plausible and that have not been previously addressed. For example, a potential spurious actuation may not be of concern if the cause was the failure of multiple independent systems. 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, particularly 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. This common position addresses the I&C review role. Other technical disciplines will need to establish their roles in addressing this issue.

Definition of terms:

Architecture: Organisational structure of the I&C systems of the plant (IEC 61513, modified).

Common Cause Failure (CCF): Failure of two or more structures, systems, or components due to a single event or cause (GCP DICWG-01, IAEA Safety Glossary, 2016).

Defect: A problem which, if not corrected, could cause an I&C component or system to either fail or to produce incorrect results (Adapted from ISO/IEC 20926:2003).

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 (IAEA Safety Glossary, 2016).

Failure: Loss of the ability of a structure, system, or component to function within acceptance criteria (IAEA Safety Glossary, 2016 – modified).

Fault: Defect in a hardware, software or system component (IEC 61513-2011). An error may lead to a fault, a fault may lead to a failure, a 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 (Adapted from IAEA Safety Glossary, 2016).

Hazard: Potential source of harm (ISO/IEC Guide 51:2014, Definition 3.5).

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 (IEC 61513-2011).

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 (Adapted from IAEA Safety Glossary, 2016).

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 (IAEA Safety Glossary, 2016).

Plausible: Not eliminated by justified and documented technical means.

Note the term "plausibility" is used in the IAEA Safety Guide SSG-39. In the context of SSG-39, 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 (PIE): An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

Note: The primary cause of a PIE may be credible equipment failures and operator errors (both within and external to the facility) or human induced or natural events (IAEA Safety Glossary, 2016).

Safety Analysis: Evaluation of the potential hazards associated with the operation of a facility or 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, a safety assessment may include the 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 (IAEA Safety Glossary, 2016).

Safety Assessment: Analysis to predict the performance of an overall system and its impact, where the performance measure is the radiological impact or some other global measure of the impact on safety (IAEA Safety Glossary, 2016).

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 (IAEA Safety Glossary, 2016).

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* (IAEA Safety Glossary, 2016).

Severe Accident: Accident more severe than a design basis accident and involving significant core degradation (IAEA Safety Glossary, 2016).

Spurious Actuation: Unintended operation by an I&C component or system.

Note: spurious actuation does not include failures on demand.

Support System or Support Feature: A system or feature designed to support the operation of one or more I&C systems or components (REGDOC-3.6: Glossary of Canadian Nuclear Safety Commission (CNSC) Terminology 2016, Modified).

Note: Systems or features that provide cooling, lubrication, and energy supply (e.g. electrical distribution systems) for systems are examples of support systems or features. An example of a support system failure that could result in the spurious actuation of an I&C system is the failure of the lubrication system for an

HVAC fan that results in loss of HVAC to the I&C system. This loss of cooling for the I&C system may result in a spurious actuation.

Scope:

This common position applies to the evaluation of spurious actuations of I&C components, systems or their supporting systems (e.g. HVAC, electrical systems), which could:

- Place a nuclear plant in an un-analysed state with respect to its safety analysis,
- Challenge the ability of safety systems to provide their intended design functions, or
- Unnecessarily challenge the safety of the plant.

This common position provides evaluation guidance for assessing the sources of spurious actuations, the consequence of identified spurious actuations, and measures to prevent and respond to spurious actuations to maintain plant safety.

This common position assumes there is sufficient independence and diversity between different safety classes of I&C systems.[2] This common position provides high level acceptance criteria for performing an adequate evaluation of spurious actuation of an I&C system.

Generic Common Position:

EVALUATION APPROACH

1) A systematic evaluation (see GCP DICWG-10) should be completed to identify the consequences of plausible spurious actuation(s) which could:

- Place a nuclear plant in an un-analysed state with respect to its safety analysis,
- Challenge the ability of safety systems to provide their intended design functions, or
- Unnecessarily challenge the safety of the plant.

2) All I&C components and systems of all safety classes should be included in the evaluation.

3) It is recognised that there may be different approaches when performing the evaluation for the identification of the consequences of plausible spurious actuation(s) (e.g. system based, function based, component based or combination thereof). This common position does not prescribe a particular approach. However, the approach taken for performing this evaluation should be justified for suitability for the particular application.

4) A documented technical basis should be provided for excluding a plausible spurious actuation from the evaluation. For example, appropriate architectural and design features (e.g. independence) may be used to remove, or reduce to an acceptable level, the likelihood of:

[2] Complete independence and diversity may not be present to address dependencies or commonalities that result from functional or plant process configurations.

(1) Multiple spurious actuations, or

(2) Spurious actuations in combination with independent PIEs.

Such measures may only be used as a justification for exclusion, if sufficient demonstration has been provided.

5) An evaluation for spurious actuation(s) should be performed during the design stage of the I&C component, system or architecture.

i) All I&C systems should be defined to facilitate the evaluation.

Note: There may be interconnections between I&C systems of different safety classes.

ii) The specific attributes of an I&C system design should be used to define the scope and the extent of the evaluation for spurious actuation.

iii) Plant components such as pumps, valves and breakers that contain industrial digital devices should be considered in the analysis.

Note: GCP DICWG-07 and international standards such as IEC 62671 provide guidance on the analysis of industrial digital devices of limited functionality.

iv) I&C support systems or features whose failure could cause spurious actuation of I&C systems (e.g. electrical, HVAC, etc.) should be considered in the evaluation.

v) Fault /Failure propagation between I&C systems, including support systems, even when there is no direct physical connection between systems should be considered in the evaluation as a potential contributor to spurious actuation.

vi) Triggering events that can cause a spurious actuation should be considered in the evaluation. These events can be for example environmental effects, human (e.g. operator) action, plant transients, maintenance errors, software errors, etc.

vii) The functionality of I&C and of supporting and connected I&C systems should be included in the evaluation in order to assess any commonalities and/or dependencies. The evaluation results may be used as a tool to determine the acceptability of functional allocation.

viii) Failure modes resulting in multiple spurious actuations of a control system should also be considered. Ways in which control system faults, including multiple spurious faults or failures, could generate a spurious demand on a safety system should be considered.

ix) The results of the evaluation should be used to inform the I&C component, system and architecture design. Design attributes could be added to reduce the likelihood or mitigate the consequences of the spurious actuation such that it can be removed from further analysis (see GCP DICWG-10 for design attributes that could be used).

6) The results of the evaluation should be validated during later stages of the I&C component or system development.

7) The results of the evaluation should be re-evaluated when necessary. A review may be triggered by mandatory periodic review or changes to the I&C components, systems, architecture or supporting systems, etc.

8) Plausible spurious actuations should be considered as initiating events.

EVALUATION ACCEPTANCE CRITERIA

1) A spurious actuation of an I&C system or component(s) could be considered bounding if its consequences envelope the consequences of other plausible spurious actuations which have been analysed and accepted.

2) The consequences of residual[3] plausible spurious actuations should be demonstrated to be within the acceptance criteria specified in each member country's regulatory framework (e.g. safety limits used in the plant's safety analyses).

   i) For a component failure of an I&C system or an I&C support system or feature, acceptance criteria should be derived from failure tolerance criteria (e.g. deterministic design criteria) of a system. As far as practicable[4], the failure of a component should not cause spurious actuation of any safety system.

   ii) Failures which may involve: (1) Multiple spurious actuations; or (2) Spurious actuations in combination with an independent PIE, which are non-time concurrent may not be addressed in the plant's safety analysis. This is because there is no way to know the worst combination of all positions in time of all such actuations (except by doing an infinite number of studies, which is infeasible). Therefore the occurrence of such actuations should be avoided, or their likelihood reduced to an acceptable level, by justified and documented technical means.

   iii) For an I&C system-induced initiating event, acceptance criteria should be derived with a graded approach from the lowest safety class within the I&C architecture. The potential for failures in systems of a lower safety class that could cause spurious actuation of higher safety classified components should be assessed and shown to be acceptable.

3) No single I&C system spurious actuation should be able to cause a severe accident.

4) The spurious actuation of a support system (or feature) for an I&C 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 defence in depth applied at the plant.

5) Measures to cope with spurious actuations or their consequence (such as manual actions) identified as a result of this evaluation should align with guidance provided in GCP DICWG-10 with regard to controlling of identified hazards. The availability of indications for the operator to recognize

[3] Those plausible spurious actuations that have not been demonstrated to be removed from consideration through design attributes.

[4] For some circumstances, it may not be practicable to ensure that a component failure does not result in spurious actuation of a safety function. For example, there may be conflicting commands to a safety component, where the assigned safe state results in spurious actuation of the component. In this case, it would not be practicable to prevent the spurious actuation of this component.

that a spurious actuation has occurred could be important for the identification of coping 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.

References:

MDEP Generic Common Position DICWG No. 1: Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems, 2013

MDEP Generic Common Position DICWG No. 7: Common Position on Selection and Use of Industrial Digital devices of Limited Functionality, 2014

MDEP Generic Common Position DICWG No. 10: Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems, 2016

IAEA SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants, 2016

IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection, 2016 Edition

IEC 61513, Ed.2: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, 2011

ISO/IEC Guide 51: Safety aspects - Guidelines for their inclusion in standards, 2014

ISO/IEC Guide 20926: Software engineering. IFPUG 4.1 Unadjusted functional size measurement method. Counting practices manual, 2003

IEC 62671, Ed.1: Nuclear Power Plants-Instrumentation and control important to safety- Selection and use of industrial digital devices of limited functionality, 2009

CNSC REGDOC-3.6: Glossary of CNSC Terminology, 2016