GRADED APPROACH FOR ASSESSING DIGITAL SYSTEM FAILURE SUSCEPTIBILITIES

R. Torok
Electric Power Research Institute
3420 Hillview Ave., Palo Alto, CA 94304
rtorok@epri.com

D. Blanchard
Applied Reliability Engineering, Inc.
3428 Balboa St. San Francisco, CA 94121
dblanchard@ar-eng.com

ABSTRACT

Owner/operators of nuclear plants must be able to identify and assess susceptibilities to digital system failures and unintended behaviors that could lead to plant system malfunctions, including common-cause failures (CCFs) of multiple controlled components that may impact overall plant safety. Nuclear plant designers and regulators often assess and manage potential failure modes by assuming the failure occurs and showing by analysis that the results are acceptable. In 2016 EPRI published a guideline on Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems (EPRI 3002005326), which takes a more holistic approach that considers digital system failure modes from the perspective of their impact on plant risk and includes a graded approach based on safety significance. This paper describes that graded approach.

The methodology in EPRI 3002005326 systematically identifies potential I&C vulnerabilities that could lead to significant malfunctions of controlled components and systems, including common-cause failures (CCF), and discusses in detail methods to protect against them. It considers both preventive measures that reduce the likelihood of failures, and plant systems and features that mitigate the effects of component failures and misbehaviors. Coping analysis is then performed as appropriate to provide additional assurance of protection. The safety significance based graded approach is an important feature in that it can help users focus attention on overall plant safety, including potentially risk-significant scenarios that might not be considered in traditional safety analyses. The purpose is to help the user ensure that modifications to the I&C that could potentially be safety significant are treated appropriately and at the same time not waste valuable resources on excessive protection against changes that have little or no impact on safety. The graded approach allows the design engineer to tailor the rigor of the preventive, limiting, and mitigative measures commensurately with the effects the I&C modification has on overall plant safety.

The graded approach focuses on safety significance **impact**, which is effectively a qualitative measure of the potential change in safety (or risk) caused by a proposed I&C modification, as compared to the I&C that is being replaced. Safety significance impact should not be confused with importance to safety or risk significance. It is possible that an upgrade to safety-related and/or risk-significant I&C systems may have **little or no safety significant impact** and vice versa. The approach considers three factors that influence the impact on safety significance of a proposed I&C modification: context, likelihood of failure, and consequences of failure. The most significant of the three factors is **context** - what the I&C is connected to, both directly and indirectly, including its potential effects on plant systems that respond to transients or accidents. The graded approach is particularly helpful in assessing potential CCFs resulting from digital I&C failures, and shows why the most problematic CCFs will be those that can affect multiple plant systems.

Key Words: Instrumentation and Control, Digital, Common-cause failure (CCF), Risk insights

1 INTRODUCTION

Owner/operators of nuclear plants must be able to identify and assess susceptibilities to digital system failures and unintended behaviors that could lead to plant system malfunctions, including common-cause failures (CCFs) of multiple controlled components that may impact overall plant safety. Digital instrumentation and control (I&C) systems offer significant advantages over their analog predecessors in terms of fault tolerance, automated diagnostics that increase availability, expanded communications capabilities, and so on. However, they are different from their analog counterparts because of their potential for new and sometimes subtle misbehaviors and failures, such as those that can be caused by software defects, the combining of functions on one controller, or increased connectivity among I&C components that could introduce new interactions.

An approach for assessing the safety significance of potential undesired events caused by digital system failures and misbehaviors can be a valuable tool to help ensure that modifications to the I&C that could have a significant impact on safety are treated appropriately and at the same time not waste valuable resources on excessive protection against changes that have little or no impact on safety. Currently, nuclear plant designers and regulators often assess and manage potential failure modes by assuming the failure occurs and showing by analysis that the results are acceptable, limiting the investigation to events considered in traditional design basis safety analyses. Current methods for assessing plant risk are not applied, leading to both unnecessary analysis expenses and overlooking potentially safety significant failures.

The methodology in EPRI 3002005326 [1] systematically identifies potential I&C vulnerabilities that could lead to malfunctions of controlled components and systems, including common-cause failures (CCF), and discusses in detail recommended methods to protect against them – process, design and mitigative measures that help reduce the likelihood of I&C failures and/or limit their effects. The method also includes a safety significance impact based graded approach that it can help users focus attention on overall plant safety, including potentially risk-significant scenarios that might not be considered in traditional safety analyses.

The safety significance impact assessment is intended for use in concert with the susceptibility assessment and its investigation of preventive and limiting measures, along with associated reliability and coping analyses. The method here does not recommend specific measures that should be used to provide sufficient overall protection. However, it does provide the engineer useful information that will help focus the assessment of preventive, limiting and mitigative measures on the changes to the I&C that may matter, and will support judgments on appropriate defensive measures and acceptance criteria for determining what constitutes sufficient protection against the failures associated with those changes. It is intended to assist the practitioner in applying engineering judgment to answer the question, how much prevention and mitigation is sufficient for the application?

This paper describes the safety significance based graded approach in EPRI 3002005326, explains key concepts and the underlying rationale, and demonstrates the approach with a couple of examples. Applying this method, a significant fraction of I&C modifications may be shown to have little or no safety significant impact. At the same time, this approach calls attention to the characteristics of I&C modifications that can lead to changes in plant response that may be safety significant and therefore may warrant special consideration in regard to preventive, limiting and mitigative measures within and external to the I&C. The approach described here is based solely on technical considerations and does not address regulatory policies or practices that may affect its use.

2 KEY CONCEPTS

2.1 Safety Significance Impact

Not all digital systems and components have the same importance with respect to safe and reliable plant operation. A digital I&C system may affect plant events in either or both of two ways:

1. Influence the characteristics of transient and accident initiators (including those that are not part of the licensing basis), e.g., increase or decrease the frequency (likelihood) or effects (consequences) of a given initiator, or impact the initial conditions assumed in analyzing events
2. Affect the response of mitigating systems, e.g., disable, delay, change performance, etc.

The graded approach described here focuses on safety significance **impact**, which is effectively a qualitative measure of the potential change in safety (or risk) caused by a proposed I&C modification. In assessing the safety significance of an I&C modification, the safety significance or safety designation of the plant system or component is not of primary importance, as the existing system has already been found to be acceptable from a safety perspective. The real concern is the potential safety significance impact - how the planned modification might change the safety significance of the system. It is possible that an upgrade to safety-related and/or risk-significant I&C systems will have **little or no safety significance impact** and vice versa. For the purposes of this discussion, an upgrade with little or no safety significance impact is one in which safety is improved over the I&C being replaced or any increase in likelihood or consequences of failures in the new I&C are minimal.

2.2 Factors that Affect Safety Significance Impact

The graded approach looks at three factors that can affect the impact that a digital modification can have on safety:

- Context: What the I&C is connected to, both directly and indirectly, including the potential effects on plant systems that respond to transients or accidents. Context is probably the most important factor, as will be seen later.
- Likelihood of failure: A qualitative or quantitative estimate of the effect of the proposed I&C change on the probability (potential) of malfunctions of the controlled SSCs.
- Consequences of failure: Changes to the effects (consequences) of I&C failures at the plant level due to the proposed change, or if likelihood of failure will increase, it may be necessary to reconsider the acceptability of the existing consequences.

2.3 Protecting Against I&C Failures

In assessing protection against potential I&C failures, the EPRI 3002005326 approach investigates and credits three types of defensive measures: preventive, limiting, and mitigative:

- Preventive Measure (*P measure*) - A design feature of an I&C system, or process used in developing an I&C system, that addresses a potential source of failure within the I&C system for the purpose of reducing the likelihood of a malfunction of controlled SSCs caused by that potential I&C failure source.
- Limiting Measure (*L measure*) - A design feature of an I&C system or component that restricts the effects of an I&C failure on one or more SSCs. A limiting measure can reduce the number of SSCs that are affected by an I&C failure, or it can force predictable states in the SSCs that are affected by an I&C failure
- Mitigative Measure - An action or feature of the plant, outside the I&C system that has initiated the failure, that alleviates or limits the undesired effects of the failure and can be credited in the coping analysis.

All three are considered and credited as appropriate in the assessment of safety significance impact.

3 TECHNICAL APPROACH

Figure 1 illustrates the technical approach in a flowchart. The chart contains three columns, corresponding to the three factors that affect the potential safety significance impact of the proposed I&C modification: context, likelihood of failure and consequences of failure. All that is needed to start the assessment is a conceptual design of the proposed modification and identification of the I&C segments and controlled components that may be affected. Context, likelihood of failure, and consequences of failure are then considered to navigate a path through the chart and arrive at one of two possible conclusions: *Little or no safety significant impact*, or *Refine I&C design and/or add mitigation*. It is intended that the flowchart be applied at least twice – once from the safety analysis perspective and once from the PRA perspective. Additional iterations may be needed to address design refinements. The EPRI guidance recommends that a proposed I&C modification should not be implemented until a *Little or no safety significant impact* conclusion can be reached. At various steps and decision points, notes on the flowchart indicate the sections in EPRI 3002005326 where supporting guidance can be found.

Entry to the graded approach occurs in the left most column, which focuses on the context of the changes being made to the I&C in terms of their potential effects on plant systems that respond to transients or accidents. The context of the changes to the I&C with respect to its potential effects on plant response is the most significant of the three factors and can have an impact on the degree to which the other two factors (likelihood and consequences of failure) affect the safety significance of the modification. From top to bottom, the context of the modifications to the I&C ranges from relatively simple and benign (e.g., does not affect SSCs that need to be considered in the safety analysis or PRA or no change in the controlled SSCs or their malfunctions) to increasingly complex and possibly problematic. I&C designs for which failures can affect multiple plant systems (third row of the flowchart) are potentially the most problematic from the safety perspective. Note that the context decision point in the third row looks at three ways in which the context might significantly increase the consequences of a CCF caused by an I&C failure:

1. CCF can cause simultaneous initiating events
2. CCF can cause an initiating event and disable a mitigating system credited for that event
3. CCF can disable multiple mitigating system for any initiating event

For an I&C design that could lead to any of these conditions, compelling assurance of sufficient protection in the forms of P measures, L measures, and acceptable coping analysis results would be recommended.

The center column of Figure 4-1 defines decisions made with respect to the likelihood of the I&C failures and associated controlled SSC malfunctions. Note that there are two types of failure likelihood in the center column depending on the context of the I&C: (1) likelihood as compared to the I&C being replaced; or (2) likelihood of failure of the I&C as compared to the probability of failure of the plant system in which it resides, or put another way, is the I&C a significant contributor to the system failure probability? The first type of likelihood involves a qualitative assessment of the new I&C in terms of its design, design processes and conformance with industry practices as compared to that of the I&C being replaced. The second type of failure likelihood is quantitative and involves a comparison of the relative reliability (or failure probability) of the I&C with respect to that of the trains of equipment that contain the controlled SSCs. This second type of assessment can take advantage of probabilistic information, perhaps available from the PRA.

The third column of Figure 4-1 outlines decisions based on the consequences of I&C failures and their associated SSC malfunctions. The consequences are determined through coping analyses and can take two forms – conservative or best estimate, as described in other sections of EPRI 3002005326. It is expected that applicable coping analyses may already exist as a part of the plant safety analysis or thermal-hydraulic

analyses performed in support of the plant-specific PRA. Note that if a coping analysis is performed to confirm that design basis requirements have been met, it should credit the measures implemented to meet the requirements. Alternatively, a coping analysis can be performed to investigate how the plant will respond if SSC failures occur despite the measures in place to prevent them.

Note that some of the decisions from the context column lead to a *little or no safety significant impact* conclusion without the need for a decision about likelihood or consequences. With respect to likelihood, this is not an indication that the reliability of the I&C does not matter or that there is no need for a susceptibility analysis. It is merely an indication that the extent of the implemented P measures is not expected to have a significant impact on safety. The reasons for this are indicated in the questions in the context column. For example, decision point (b) asks if the SSCs controlled by the I&C are relied on in the safety analysis or credited in the PRA. If an SSC is not, the guideline method concludes that it will not be safety significant, regardless of the failure likelihood. Keep in mind, however, that failure likelihood could still warrant additional consideration from a plant operability perspective.

Similarly, decisions regarding context or likelihood do not necessarily lead to the need for a decision on consequences. Again, this should not be interpreted as a suggestion that no coping analysis is needed. It is only an indication that the difference in consequences of I&C failure between the new I&C and the I&C being replaced is minimal. If the consequences of failure of the old I&C were considered to be acceptable, then the acceptability of the same consequences should apply to the replacement I&C as well.

Note that there are seven possible paths through the flowchart that achieve a *little or no safety significant impact* conclusion (labeled NS1-NS7). There also are seven paths to a *refine the design conclusion* (labeled R1-R7). Each of these paths represents a unique combination of characteristics of the I&C related to context, likelihood and consequences. Section 4.1 of EPRI 3002005326 describes the characteristics of each of these paths and provides examples of I&C systems having the characteristics associated with selected paths.

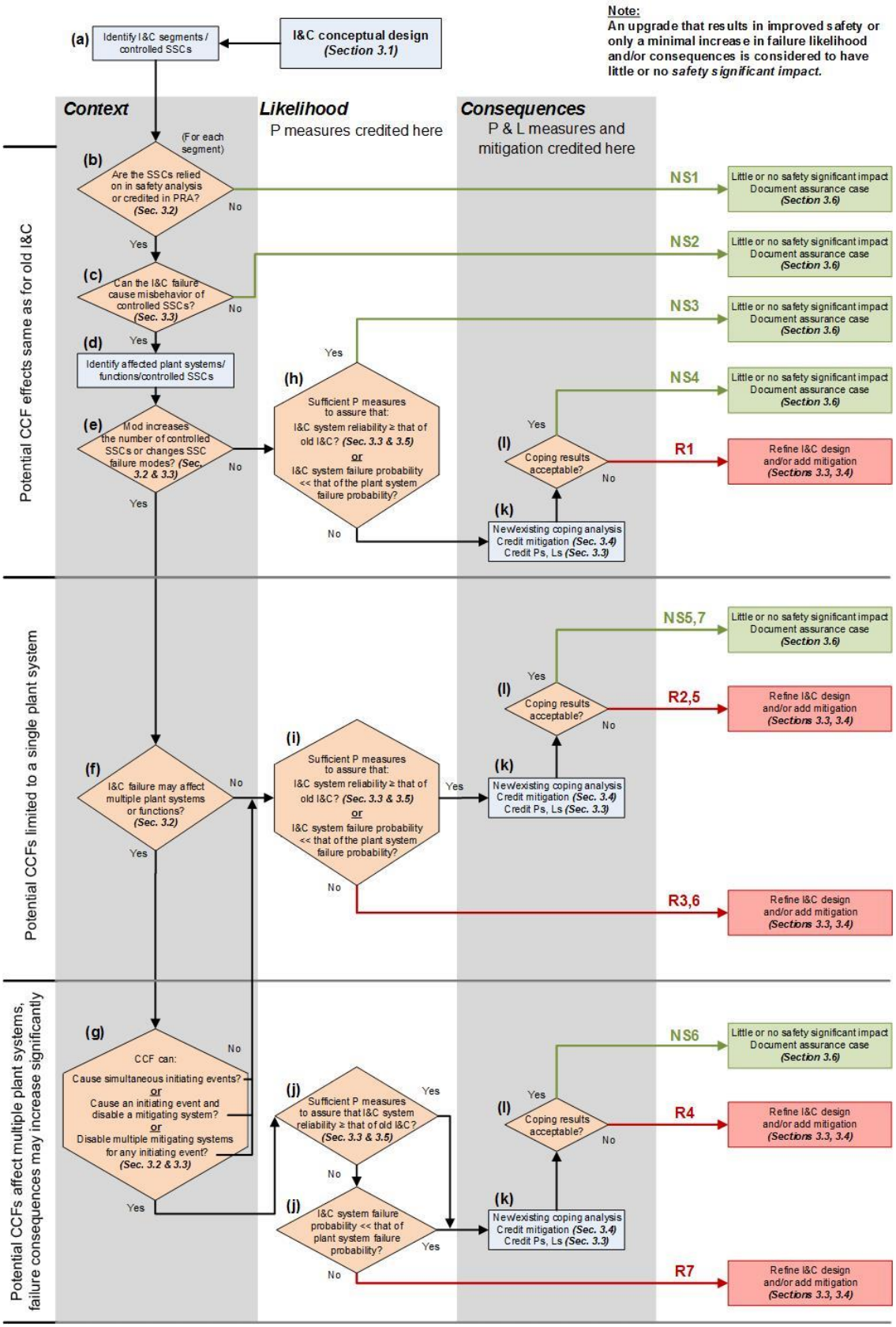

Figure 1. Safety Significance Flowchart.

4 EXAMPLE APPLICATIONS OF THE FLOWCHART

This section presents a summary of the application of the safety significance based graded approach to two of the digital upgrade examples in EPRI 3002005326. The complete descriptions of the examples are contained in Appendices E and F of the EPRI guide.

4.1 Application of Flowchart to CCF of Post-Accident Monitoring (PAM) Recorders

The PAM recorders are both relied upon in the safety analysis and credited in the PRA for the purposes of providing control room operators indication of reactor pressure in support of alignment of the Shutdown Cooling System (SDC). The susceptibility analysis performed per EPRI 3002005326 **without considering safety significance impact** indicates that while the recorders are physically and electrically independent, and commercial grade dedication has provided sufficient information to conclude that failure of the recorders is less likely than what is considered in the safety analysis, the recommended set of preventive design measures have not been fully implemented, so additional assurance may be needed in the form of additional preventive measures or coping analysis.

Figure 2 shows how the example would be viewed from a safety significance impact perspective. For both the safety analysis and the PRA, the reason the PAM recorders are considered to have little or no safety significant impact, because the recorders represent very small contributors to the overall system failure probability. The postulated CCF affects multiple SSCs (the recorders themselves), but not multiple plant systems. CCF of the recorders is considered a small contributor to the probability of failure of the system because, in this case, system failure is dominated by the probability of operator action failure (on the order of 10^{-3} /demand).

Note that a conclusion that the PAM recorder modification has little or no safety significant impact could have been made by considering other paths through the flowchart. For example, if the recorders were functionally equivalent replacements of existing analog recorders and had the same failure modes as the recorders that they were replacing, then it may have been possible to answer the question ‘no’ regarding whether the modification affects additional SSCs or changes their failure modes (malfunctions).

Based on the low safety significance impact finding, the analyst might conclude that the gaps in the preventive measures observed in the susceptibility analysis are acceptable. However, EPRI 3002005326 would still recommend that some form of coping analysis be used to ensure that the failure consequences are understood and considered acceptable from equipment protection and plant operability perspectives.

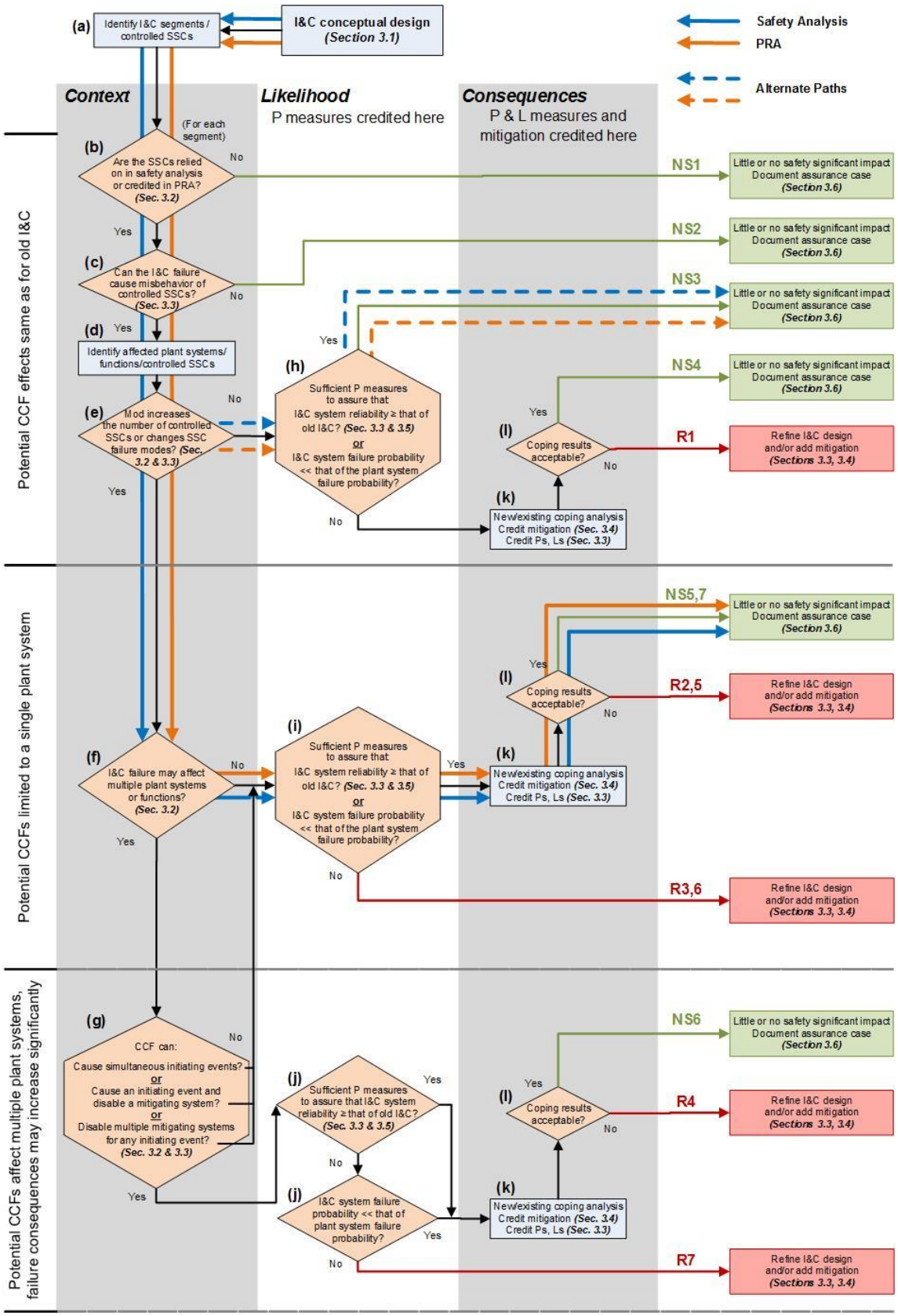

Figure 2. Application of flow chart to a post-accident monitoring recorder example.

4.2 Application of Flowchart to CCF in a Distributed Control System (DCS) Example

Figure 3 shows the paths through the flow chart for a potential CCF of the segmented DCS (feedwater and turbine controls) in the example of Appendix E of EPRI 3002005326.

The initial conceptual design for the DCS in this example segments the controls such that there are no shared controllers, I/O modules, power supplies or network throttling devices between the turbine control and feedwater control systems. However, the two systems share a redundant Ethernet communication network, main control room HSI workstations, an engineering workstation and a date/time clock server. Within each segment are redundant controllers, I/O modules, a redundant pair of regulated power supplies (one provided with a UPS) and a dedicated throttling device for each controller.

The safety analysis largely considers feedwater and turbine controls as sources of plant transients, various malfunctions of a single feedwater regulating valve or turbine control valve being the trigger for a transient. The PRA considers the effects of feedwater and turbine controls on the potential for transient initiators and on mitigating systems (feedwater being credited as a source of makeup to the steam generators and turbine controls, potentially affecting the steam source for the turbine aux feedwater pump).

The susceptibility analysis for the DCS upgrade identifies additional SSCs that can be affected by I&C failures as compared to the original DCS. While the design features described above support an unlikely conclusion for most potential I&C failure sources, this is not the case for a data storm on the shared Ethernet network, which has the potential to result in simultaneous malfunctions across both the feedwater and turbine control segments. Also, within each segment, simultaneous malfunctions of multiple feedwater or turbine valves could be postulated, as opposed to the malfunction of a single valve at a time.

Because the upgraded DCS can impact multiple systems, the paths in Figure 3 drop to the lower portion of the flowchart. Given a potential for multiple simultaneous initiating events (feedwater and turbine control initiated transients) the path exits the bottom of decision point (g) and remains in the lower third of the flow chart, addressing both likelihood and consequence decision points. It is preferable that the likelihood of I&C failures causing such an initiating event be no greater than those that might be caused by comparable analog systems. Defensive measures identified in the reliability analysis (Section 3.5 of EPRI 3002005326) such as self-diagnostics, error checking, prevention of malfunctions propagating to the controllers from other levels of the architecture, preprogramed controller responses on loss of data, need for multiple distinct operator actions to issue commands, etc. result in the conclusion that the DCS will be reliable, and any increase in the potential for plant transients resulting from this system would be minimal.

However, because the susceptibility analysis concluded that failure initiated by a data storm was not sufficiently unlikely, the safety analysis should now consider multiple simultaneous initiating events (e.g., excessive feedwater and steam demand). As the existing safety analysis does not include these initiators simultaneously, either a new safety analysis is needed, or a revision to the design is needed to limit the potential for multiple initiators. The solid blue path in the flowchart reflects the choice made in the example to refine the design to provide defensive measures against simultaneous steam demand and feedwater malfunctions, rather than performing a new safety analysis. The second pass through the flow chart then exits decision point (g) with a *no* answer (dashed blue line) and comes to a *little or no safety significant impact conclusion* based on the applicability of the existing safety analysis.

The PRA already considers the potential for malfunctions within both the feedwater and turbine systems, and thermal-hydraulic analyses performed in support of the PRA have shown that the plant can cope with simultaneous malfunctions in both systems using either the auxiliary feedwater system or, as a backup, feed-and-bleed operation. With these backup capabilities, the PRA path terminates with a little or no safety significant impact conclusion.

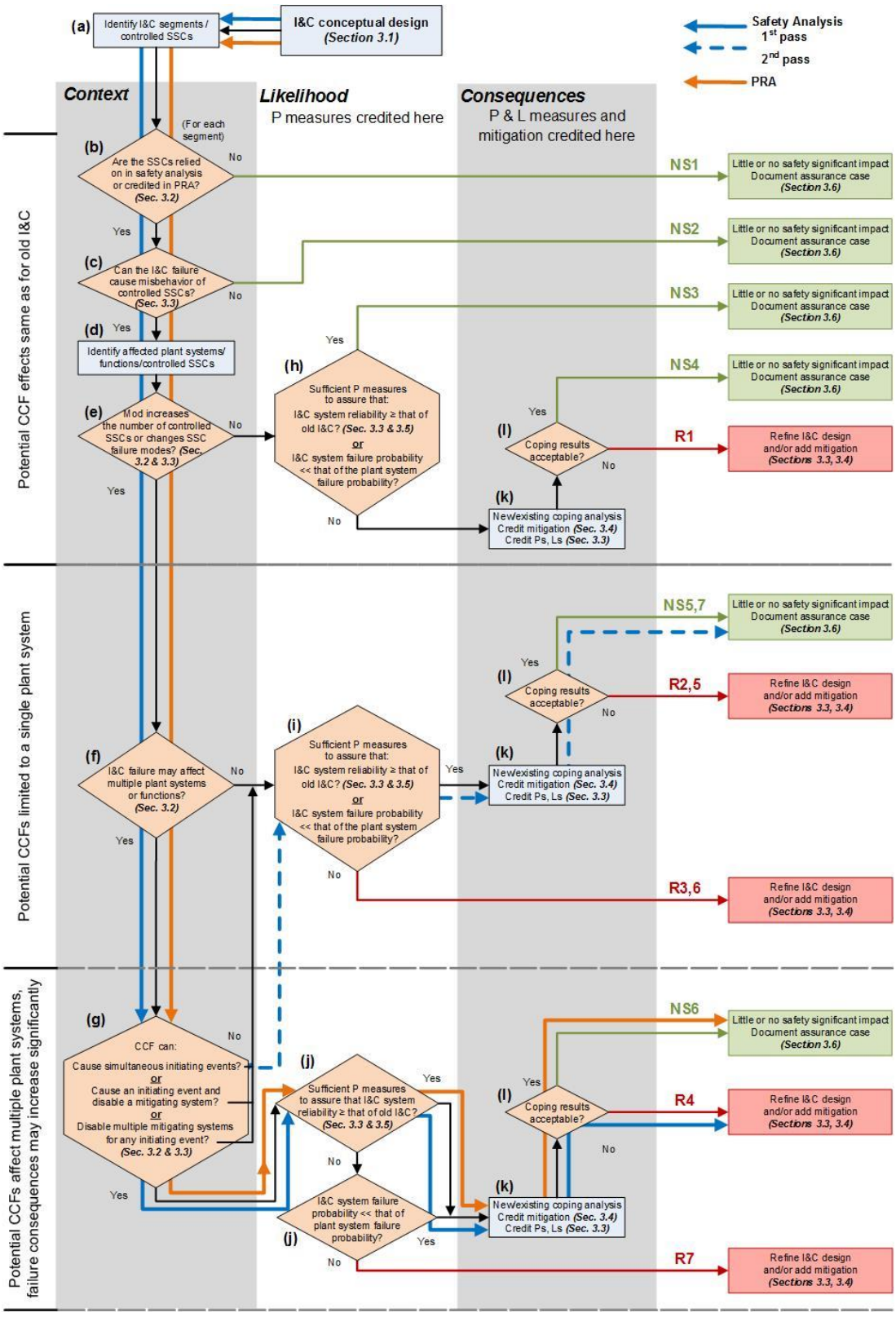

Figure 3. Application of the safety significance flow chart to a distributed control system (DCS) example.

5 SUMMARY AND CONCLUSIONS

In 2016 EPRI published a guideline on Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems [1], which provides specific recommendations on design and process measures that provide protection against the undesired effects of potential failures and misbehaviors of digital equipment, especially failures that can lead to CCF of multiple controlled components or plant systems. The report also includes a graded approach based on safety significance impact that enables the user to tailor the rigor of the protective measures commensurate with the effects that the I&C modification has on safety. The graded approach guides the user through a flowchart with decision points that systematically assess the potential impact on safety of a proposed I&C design modification based on its context in the plant, the likelihood of I&C failures, and the potential consequences of failures. The approach is intended to assist the practitioner in applying engineering judgment to answer the question, how much prevention and mitigation is sufficient for the application?

6 REFERENCES

1. *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems*. EPRI, Palo Alto, CA: 2016. 3002005326.
2. *Protecting Against Digital Common-Cause Failure: Combining Defensive Measures and Diversity Attributes.* EPRI, Palo Alto, CA: 2010. 1019182
3. *Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants*. EPRI, Palo Alto, CA: 2009. 1019183.
4. *Estimating Failure Rates in Highly Reliable Digital Systems*. EPRI, Palo Alto, CA: 2010. 1021077.