Research Report: NRC-HQ-11-6-04-0060

Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants

John Thomas
Francisco Luiz de Lemos
Nancy Leveson

November, 2012

Table of Contents

Figures

Tables

1. Introduction

One of the challenges of reviewing licensing plans is the rapid pace of change in technology, particularly the introduction of digital technology. New technology introduces potential unknowns into our systems and creates new paths to losses. Although digital instrumentation and control promises multiple benefits like self-checking, on-line diagnostics, improved accuracy, fault tolerance, and automated sensor calibration verification, it also presents unique challenges, from software logic errors and unanticipated system interactions to filtering and digital noise problems and trips that result from configuration changes while at power [NEI, 2011]. Challenges exist, however, in keeping review procedures up to date with respect to new technology

A major concern in approving digital I&C systems is the potential for common cause failure in I&C software. Because identical software is used in the redundant channels of safety-related systems, a bug inadvertently designed or implemented into the software (rather than resulting from degradation over time) could cause the same inaccuracies or misbehaviors in all the channels. The NRC has written that "experience with digital I&C systems to date has shown that reliance upon quality assurance processes alone has not been adequately effective at preventing common cause failures even in high-integrity digital systems" [NRC, 2010].

1.1 The Problem

Many effective methods exist for assurance of safety in traditional electro-mechanical safety systems. Unfortunately, many of the assumptions underlying these traditional NPP assurance methods do not apply to software.

First, software does not fail randomly like hardware: software is pure design without any physical realization of that design—it contains only systematic design defects. Software can be thought of as *design abstracted away from its physical representation*, that is, it is pure design without any physical realization of that design. While this abstraction reduces physical limits in design and thus allows exciting new features and functions to be incorporated in system design, it also greatly increases potential complexity and changes the types of failure modes.

Essentially there are two means for "failure" of digital systems. The hardware on which the software executes can fail in the same way that analog hardware does and the protection against these types of computer hardware failures, such as redundancy, is similar. In addition to the computer hardware failing, however, the software (which embodies the system functional design) can be incorrect or include behaviors that are unsafe in the encompassing system. Because the potential problems are always pure design defects, redundancy (which simply duplicates the design errors) is not effective. Knight and Leveson showed, back in the mid-1980's, that making multiple versions of the software using different teams does not solve the problem either [Knight and Leveson, 1986]. Others replicated the Knight and Leveson experiments to try to demonstrate they were wrong, but simply replicated the results [Knight and Leveson, 1990]. People make mistakes on the hard cases in the input space; they do not make mistakes in a random fashion: Therefore, independently developed software is very likely to contain common cause failure modes.

In fact, almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code (computer instructions) [Leveson, 1995]. In most accidents, the software requirements have had missing cases or incorrect assumptions about the behavior of the system in which the software is operating. Often there is a misunderstanding by the engineers of the requirements for safe behavior, such as an omission of what to do in particular circumstances that are not anticipated or considered. The software may be "correct" in the sense that it successfully implements its requirements, but the requirements may be unsafe in terms of the specified behavior in the surrounding system, the requirements may be incomplete, or the software may exhibit unintended (and unsafe) behavior beyond what is specified in the requirements. Redundancy or even multiple versions of the implementations of the requirements does not help in these cases.

Hardware, of course, can also contain requirements and design defects, but hardware can usually be exhaustively tested and the defects discovered and removed before the system is used. In addition, most

hardware designs are not revolutionary, but use or build on standard designs used for decades. Software, on the other hand, cannot be exhaustively tested or even come close to that goal. For example, a software-implemented collision avoidance system required on all commercial aircraft in the U.S. (called TCAS II) has been calculated to contain 10^{20} states. Continuity, which allows infinite state hardware systems to be tested by using interpolation between the test inputs, does not apply to discrete-state digital systems.

In addition, most software represents a new design—it is used to introduce efficiencies or functions that were not in previous hardware designs. Even reuse of old software does not seem to solve the problem [Joyce, 2002; Leveson, 2012]: almost all the software-related spacecraft losses in the past few decades involved reused software from past spacecraft [Leveson, 2004]. These results may stem partly from complacency created by successful use in previous systems and because undocumented assumptions made during the original development may be inappropriate for the new use.

Even if the functionality being provided by software is the same as that of the hardware being replaced, the software-related system failure modes can be and usually are very different than the hardware-based system it is replacing. For example, when an analog mode annunciator in a nuclear power plant control room fails, the screens will go blank and the operators will detect this right away. When a digital box performing the same function fails, the screens will tend to simply freeze, which may take longer to detect. More generally, software tends to "fail" (i.e., not satisfy its requirements) by doing the wrong thing, not by stopping.

Not only do the old reliability enhancing design techniques not work for software, but software is creating new types of accidents and new accident causes that are unrelated to the reliability of the individual components. Accidents in systems with software components are increasingly caused by unsafe interactions among operational (non-failed) components [Leveson, 2012]. These *component interaction accidents* cannot be controlled using the standard redundancy and overdesign (safety margins) effective against hardware component failures. Industries that have been more aggressive about introducing digital technology are experiencing these new types of accident causes. The nuclear power community, which has been more conservative about the use of digital technology, at least until recently, is approaching the level of system complexity where component interaction accidents will increasingly occur.

The violation of these basic causal assumptions about accidents that occurs when using software means that many of the traditional techniques for safety assurance do not apply to the digital components of systems. The problem then is how can we improve our ability to provide software assurance for safety-critical applications and how can these techniques be combined with traditional design and assurance techniques to provide a more effective means of designing and certifying or licensing mixed analog and digital instrumentation in NPPs.

1.2 A Potential Solution

To include software in our safety assurance techniques, we need to include the new types of accident causes that software introduces in our conception of how accidents occur. This goal can be accomplished by extending the models of causation currently used. Most traditional safety engineering analysis and design methods assume a chain-of-events model where a sequence of failure events, each leading directly to the next one, results in an accident. As an alternative, Leveson has created a new accident causality model, called STAMP (System-Theoretic Accident Model and Processes), which is based on system theory [Leveson, 2012] and includes a broader view of accident causation and indirect or non-linear interactions among events.

In STAMP, safety is reformulated as a control problem rather than simply a reliability (or availability) problem. Component failure (and unreliability of the system components) is still included, but more generally accidents are considered to occur when component failures, external disturbances, or unsafe interactions among system components are not adequately handled, i.e., controlled, resulting in unsafe system behavior. Unsafe system behavior is defined in terms of required behavioral safety constraints not being met. For example, a typical system safety constraint for a nuclear power plant is that the reactor protection system must always insert neutron absorbing material into the core when a reactivity excursion is

feared or cooling is inadequate. Failure to enforce that constraint could, under certain circumstances, lead to an unacceptable release of radioactivity into the environment.

To prevent accidents, the system design must enforce the safety constraints on system behavior. The actual process that may lead to the lack of control (or accident) can be very complex and may involve indirect, non-linear, and feedback relationships among the events and the system components.

Safety constraints specify those relationships among system variables or components that constitute the non-hazardous or safe system states—for example, the power must never be on when the access door to the high-power source is open; two aircraft must never violate minimum separation requirements; pilots in a combat zone must be able to identify targets as hostile or friendly; and the public health system must prevent the exposure of the public to contaminated water and food products. In nuclear power plants, common system-level safety constraints are that control rods must be inserted into the core when core reactivity is out of control or when core cooling is insufficient, the reactor core must be provided with sufficient cooling to evacuate heat and prevent damage to the core, fuel cladding must prevent leakage of radioactivity, etc. These high-level behavioral constraints can be refined into more specific constraints on the behavior of each of the system components, which together will ensure the system-level safety constraints. Accidents result from individual component behavior that violates its safety constraints and from interactions among system components that violate the system-level safety constraints—in other words, from a lack of appropriate constraints on component and system behavior.

Besides safety constraints, one other important concept is needed in formulating safety as a control problem. In basic systems and control theory, in order to provide effective control, the controller must have an accurate model of the process it is controlling (Figure 1). For human controllers, this model is commonly called the mental model. For both automated and human controllers, the process model or mental model is used to determine what control actions are necessary to keep the system operating effectively.

The process model includes assumptions about how the controlled process operates and about the current state of the controlled process. Accidents in complex systems, particularly those related to software, often result from inconsistencies between the model of the process used by the controller and the actual process state, which leads to the controller providing unsafe control. Usually, these models of the controlled system become incorrect due to missing or inadequate feedback and communication channels. In the Mars Polar Lander loss, for example, the software thought the spacecraft was on the surface of the planet and issued an instruction to cut off the descent engines. At the time, however, the spacecraft was still 40 meters above the planet surface. As another example, the autopilot software may think the aircraft is climbing when it really is descending and apply the wrong control law or the pilot may think a friendly aircraft is hostile and shoot a missile at it.

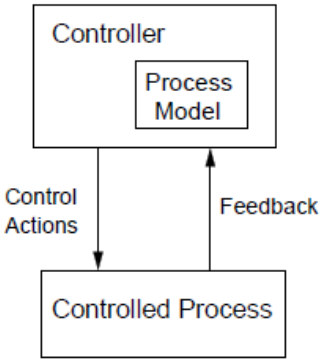

Figure 1: Every Controller Contains a Model of the Process Being Controlled.

A large number of accidents involving software can be explained by inaccurate process models. The same is true for accidents related to human errors. STAMP provides a much more effective way of designing to reduce human error than does treating human error like machine failure.

Designing for safety or analyzing an existing design for safety involves creating and analyzing the controls used to enforce the safety constraints (safe behavior) to ensure that they will be effective in ensuring the safety constraints will be enforced by the system design. Part of the challenge in designing effective safety controls is providing the feedback and inputs necessary to keep the controller's model consistent with the actual state of the process. An important aspect of understanding accidents and losses involves determining how and why the controller was ineffective; often this is because the process model used by the controller was incorrect or inadequate in some way.

Using these concepts, we have created a new hazard analysis technique called STPA (System Theoretic Process Analysis) [Leveson, 2012]. STPA can be used to identify the safety constraints that must be enforced and to ensure that the system design adequately enforces them. It also identifies the required process model (mental model if the controller is a human) that the controller needs in order to provide adequate control and thus the information required in that process or mental model. If that information gets lost or corrupted, accidents can occur.

STPA is basically a rigorous method for examining the control loops in the safety control structure to find potential flaws and the potential for (and causes of) inadequate control. Because the STAMP framework extends current accident models and thus includes component failure accidents, STPA not only identifies the hazard scenarios identified by fault trees, event trees, and other traditional hazard analysis methods, but it also includes those factors not included or poorly handled in these traditional methods such as software requirements errors, component interaction accidents, complex human decision-making errors, inadequate coordination among multiple controllers, and management and regulatory decision making.

1.3 Using STPA

STPA first assists in identifying the safety control requirements. There are four types of inadequate control that can lead to accidents:

1. A required control action is not provided or not followed.
2. An incorrect or unsafe control action *is* provided.
3. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.
4. A control action required for safety is stopped too soon.

We use a table to record the results of this part (called Step 1) of the analysis. Some entries in the table signal incorrect behavior but not a safety problem. When the table is filled for each of the identified system hazards, the hazardous behaviors can be translated into safety constraints (requirements) on system component behavior. This process partially solves the problem of inadequate requirements leading to software-related accidents.

The next step in STPA (Step 2) is to determine how these unsafe control actions could occur, that is the scenarios that can lead to a hazardous system state or accident. Like HAZOP, but unlike fault trees, STPA works on a system model (the functional control structure) and guidance is provided by STPA on what to look for so that omissions of scenarios or causes are less likely to occur.

Flaws in the safety control structure identified by STPA can be used to redesign or reengineer the safety controls. In turn, the model and analysis techniques can be used to evaluate proposed changes. Changes may involve adding or strengthening communication and feedback channels in order to ensure accurate process models and thus improved decision making. Other changes may involve redistributing responsibilities, coordinating or consolidating oversight, or simply clarifying the assumptions and rules under which the system operates.

The important question, of course, is whether this works. Few formal comparisons have been made yet between STPA and traditional techniques such as fault tree analysis, but what has been done shows STPA to be very promising. Two real-world examples of using STPA on complex systems, for example, are the use on the new U.S. Missile Defense System and the use by the Japanese Space Agency (JAXA) on the Japanese HTV (unmanned spacecraft to transport cargo to the International Space Station).

For the ballistic missile defense system (BDMS), STPA was used right before the system was to be deployed and field tested. So many potential paths to inadvertent launch were identified that had not been

found by previous extensive analyses on the system and on the individual system components using traditional techniques, such as fault tree analysis, that deployment and testing had to be delayed for six months to eliminate the previously unidentified scenarios. While the scenarios identified by STPA included those caused by potential component failures, as expected, new scenarios were also identified that involved unsafe interactions among the components without any component failure—each operated according to its specified requirements, but the interactions could lead to hazardous system states. These new scenarios included problems such as missing cases in the software logic of the launch control system and obscure timing relationships in the communication of signals between the system components.

In a paper written by the engineers performing the analysis [Pereira *et.al*., 2006], two other advantages were noted:

1. The effort was bounded and predictable and assisted the engineers in scoping the efforts. Once all the defined control actions are examined, the assessment is complete.
2. As the control structure was developed and the potential inadequate control actions were identified, they were able to prioritize required changes according to which control actions have the greatest role in keeping the system from transitioning to a hazardous state.

The paper concluded:

> "The STPA safety assessment methodology … provided an orderly, organized fashion in which to conduct the analysis. The effort successfully assessed safety risks arising from the integration of the elements. The assessment provided the information necessary to characterize the residual safety risk of hazard associated with the system. The analysis and supporting data provided management a sound basis on which to make risk acceptance decisions. Lastly, the assessment results were also used to plan mitigations for open safety risks. As changes are made to the system, the differences are assessed by updating the control structure diagrams and assessment analysis templates" [Pereira *et.al*., 2006].

A more careful evaluation of STPA was made by JAXA for the HTV unmanned spacecraft [Ishimatsu, 2010]. Because human life on the International Space Station is involved, rigorous NASA hazard analysis standards using fault trees and other analysis methods had been employed and reviewed by NASA experts. Later, STPA was experimentally applied to the same system in an evaluation of the new technique for potential use at JAXA. All the hazard causal factors identified in the fault tree analysis were identified by STPA. But, as with the BMDS comparison, additional causal factors were identified by STPA alone. Those additional causal factors again involved those related to more subtle types of errors beyond simple component failures and those related to software defects and human errors. Other comparisons have been done with similar results.

1.4 Research Goals

Our research goal for this contract was to demonstrate the applicability, feasibility, and relative efficacy of using STPA in the licensing of digital nuclear power plants. STPA has the potential to augment the existing review and certification or licensing regime with the aim of not only providing means to assess hazards associated with the introduction of digital technology in nuclear power plants, but also tools to evaluate the extent to which these hazards are adequately mitigated by the encompassing system architecture and to generate recommendations for safety-driven improvements when they are needed. We expect that STPA could be an effective method at the "guidance" level. ..

2. A Brief STPA Tutorial

STPA has a defined set of discrete procedures to establish the system information for the analysis, identifying unsafe control actions, and identifying the causes of unsafe control. The results can be used to generate safety requirements and design safer systems or, when a system already exists, to evaluate it with respect to safety. To begin, the analysts first need to identify the accidents with which they are concerned and the hazards related to those accidents and then construct a model of the safety control structure.

2.1 Identifying accidents

Before performing STPA, there must be an agreement about the system-level losses, or *accidents*, that are to be considered. The losses often involve loss of human life or human injury, but any loss can be included that is unacceptable and must be prevented. For example, economic losses such as damaged equipment or a mission loss can be specified. In a nuclear plant, the losses (accidents) that can be considered usually involve exposure to harmful radiation by those inside or outside the plant, loss of electrical generating power, unacceptable loss of equipment or machinery, etc.

Accidents must describe the ultimate outcome that needs to be prevented and not an intermediate event. For example, a loss of coolant is not a system-level accident because it does not describe the ultimate outcome that must be prevented. It is, however, a *cause* of a system-level accident.

2.2 Identifying system hazards

Once the system accidents have been defined, the system hazards can be identified. A hazard is defined as:

> **Hazard:** A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).

Each hazard is associated with one or more accidents. For example, consider the accident *humans are exposed to toxic chemicals from a chemical plant*. This accident depends on several external factors outside the boundaries of the system (plant) being considered—that is, outside the control of the designer or operator such as wind direction, speed, and other meteorological conditions. The associated system hazards must define only the factors that are under the control of the system designer or operator. For example, *toxic chemicals released into the atmosphere* is a system hazard for a chemical plant. Other examples are shown in Table 1. Note that hazards are NOT equivalent to component failures. For example, *release of radioactive materials* is a system hazard while *pipe break* is a specific component-level cause of that hazard. Later in the STPA analysis the potential causes of each hazard will be found.

Because accidents may depend on external factors, the existence of a hazard may or may not lead to an accident. In a worst-case environment, however, for example a tsunami that breaches a protective wall, a hazard will lead to an accident. This is an important distinction between traditional methods that focus on nominal or expected conditions and STPA which includes both nominal and worst-case conditions.

Once the system-level accidents have been refined into system-level hazards, the rest of the analysis considers each hazard in detail and identifies the related causal factors and scenarios. Because accidents and hazards describe interactions between the system and its environment, very little knowledge is required about the system itself to identify them.

Table 1: Examples of accidents and hazards

Accident	**Hazard**
Satellite becomes lost or unrecoverable	Satellite maneuvers out of orbit
Humans are exposed to harmful levels of radiation	Nuclear power plant releases harmful levels of radiation
Humans are sickened by food pathogens	Food products containing pathogens are sold

Hazards can be restated as the safety constraints that must be enforced to prevent the hazard. Examples for Table 1 are the satellite must never maneuver out of its orbit, the nuclear power plant must never release a harmful level of radiation, and food products containing pathogens must never be marketed.

2.3 Modeling the Safety Control Structure

The safety control structure is a functional control model of how the system maintains safety, that is, how it enforces the safety constraints. If the system is still being designed, then the first models will be very high-level and will be refined as design decisions are made, ideally using the results of the STPA hazard analysis.

A safety control structure is organized hierarchically, whereby controllers at higher levels operate to fulfill their responsibilities by providing control actions that affect lower level controllers or processes. Feedback is provided by lower level components and is used by higher-level controllers to decide what control actions to provide next. Figure 2 shows a generic control structure that includes both system development and operation.

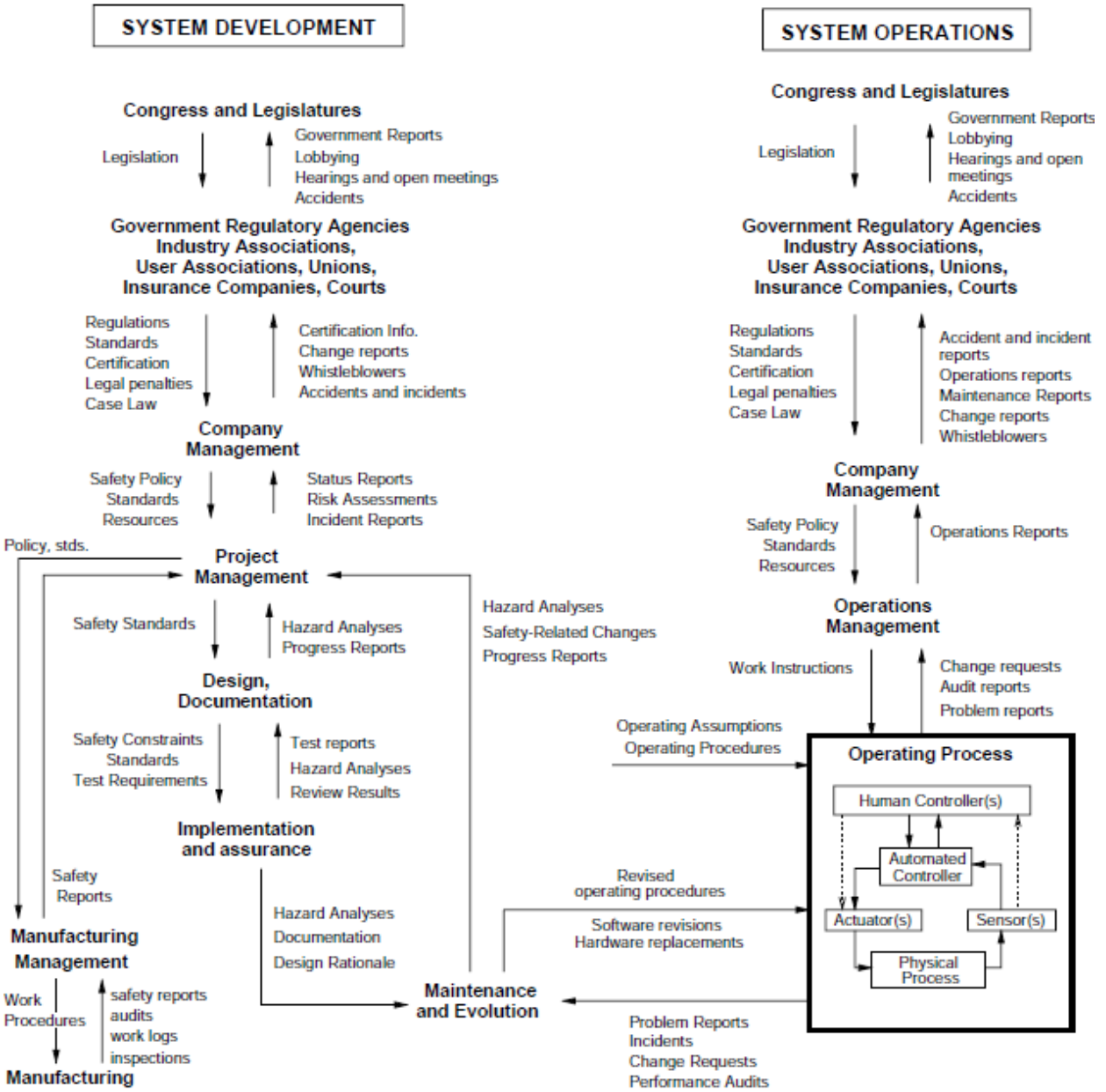

Figure 2: An Example Safety Control Structure

Traditional hazard analysis methods are typically limited to the *Operating Process* in the lower right of Figure 2, and sometimes do not even include the operator, but the rest of the sociotechnical system also plays a critical role in preventing accidents. Because hierarchical control structures include organizational, regulatory, engineering, and human components, STPA can be used to analyze additional accident factors that are not included in traditional analyses.

Figure 2 shows a very high-level control structure, but each component can be refined into a more detailed substructure. For example, Figure 3 shows an example control structure for the *Operating Process* portion of Figure 2. Because STPA is a top-down method, control structures are, in most cases, defined at a very high level of abstraction and then later refined.

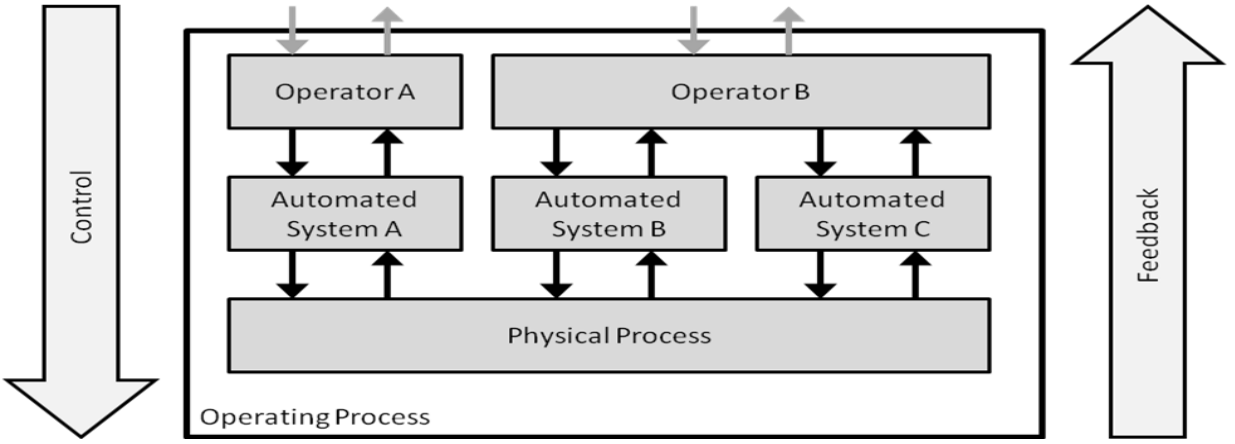

Figure 3: Example Safety Control Structure for the Operating Process in Figure 2

The lowest level of the safety control structure is typically a physical process such as an aircraft, the production line in a food plant, or the nuclear reaction in a power plant. The higher levels contain controllers that directly or indirectly affect the safety of the physical process by enforcing constraints on the behavior of and interactions among the system components at the levels below.

Defining the safety control structure for a specific system involves identifying the controllers/components and their safety-related responsibilities. For example, pilots may be responsible for properly executing all instructions from air traffic control, automated systems may be responsible for maintaining process parameters within certain limits, and plant operators may be responsible for monitoring automated systems and reporting any problems found. The arrows represent control actions (downward arrows), feedback (upward arrows), and other communication paths between the system components necessary to carry out safety-related responsibilities.

Finally, *process models* must also be defined. As stated earlier, each controller—whether human or machine—contains a model of the process they are controlling. The process model is used by controllers to determine the control actions necessary to fulfill their responsibilities. Therefore, the process model must contain the information necessary for the controller to make safe decisions. For example, a pilot's process model would include aircraft parameters such as climb rate, altitude, heading, etc. A chemical plant operator might have a process model that includes the amount of toxic chemicals being produced and various flow

rates in the system. Figure 4 shows a portion of a control structure with responsibilities and process models for a train door control system.

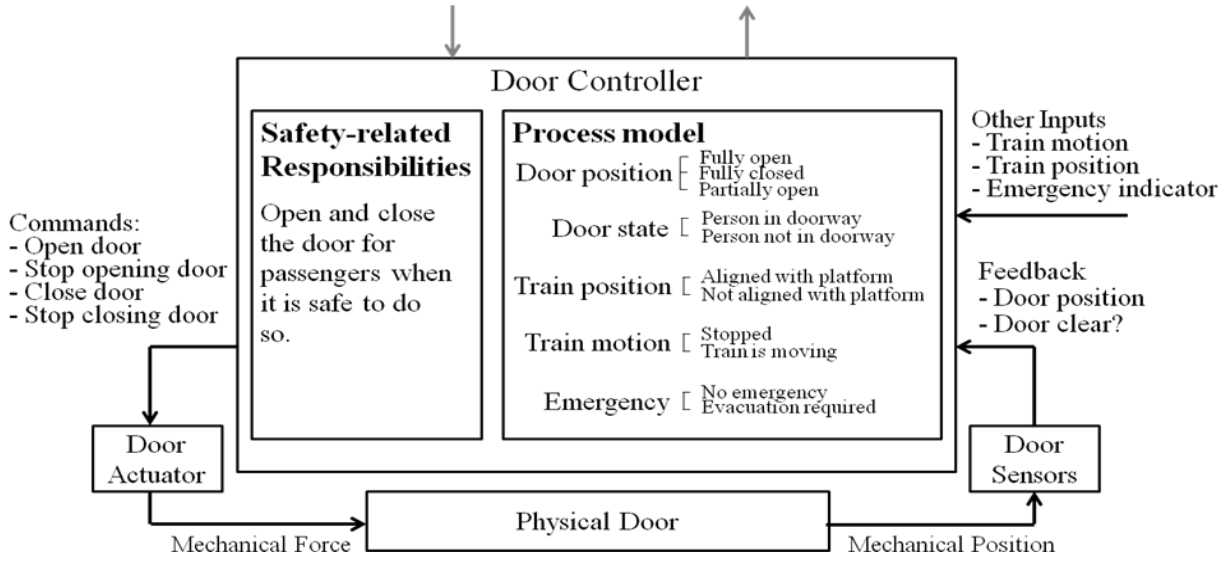

Figure 4: Simple Safety Control Loop for a Train Door Controller

The safety control structure is a powerful way to represent the safety design of complex systems and useful results can be produced even at this early stage of the analysis. Flawed process models, overlapping responsibilities, and conflicting control actions are clearly important contributors to an accident. Although these are all examined in detail later in the STPA analysis, many problems can be detected at this stage through a simple examination of the control structure. For example, if a controller's process model requires information that is not provided in any feedback or communication path, there is likely a flaw in the design. If a component can receive similar control actions from multiple controllers, there is the potential for conflicting control actions. In many cases these types of potential flaws can be detected and corrected at this stage before the rest of the STPA analysis is even performed.

2.4 Identifying Unsafe Control Actions (Step 1)

Each controller in the system can issue control actions, represented by downward arrows in the control structure diagram. This step analyzes each control action to determine how the action can be unsafe, i.e. cause a system-level hazard.

2.4.1 Simple method

Four types of Unsafe Control Actions (UCA) are possible

1) A control action required for safety is not provided
2) An unsafe control action is provided that leads to a hazard
3) A potentially safe control action is provided too late, too early, or out of sequence
4) A safe control action is stopped too soon or applied too long

A simple method of identifying unsafe control actions is to examine each control action in the control structure for each hazard and identify unsafe control actions of these four types. The hazards considered here are the train starts with a door open, a door opens while the train is in motion or is not aligned with a station platform, a door closes while someone in the doorway, and doors cannot be opened for emergency evacuation. Table 2 shows one way the results can be documented.

Table 2: Unsafe Control Actions for Simple Train Door Controller

Control Action	1) Not provided causes hazard	2) Providing causes hazard	3) Wrong timing or order causes hazard	4) Stopped too soon or applied too long causes hazard
Door open command	UCA 1: Doors not commanded open for emergency evacuation	UCA 2: Doors commanded open while train is in motion UCA 3: Doors commanded open while train is not aligned at a platform	UCA 4: Doors commanded open late after emergency situation	N/A

When considering whether a potential UCA is hazardous or not, it is important to avoid assuming that other safety-related barriers are intact or that they are appropriate, sufficient, and error-free. For example: even if there is a physical interlock that should prevent the actuator from opening the doors while moving, it is still considered hazardous to provide the *door open* command while moving. The analysis is looking for unsafe behavior, which is defined as behavior that will cause a hazard given a worst-case environment. A worst-case environment includes the case where the physical interlocks are not operating or effective. There is no requirement that unsafe behavior (control actions) must *always* cause a hazard or that an accident must be guaranteed to occur. If the analysis assumed that other barriers are always operational and adequate, then no behavior (including that of the barriers) would be considered unsafe. Instead, components should behave in such a way that the other barriers are not needed.

The simple method for identifying unsafe control actions is simple, easy to perform, and provides an intuitive way to communicate the results, but it is easy to leave out unsafe control actions. A more systematic method can be helpful in rigorously identifying the unsafe control actions. The results can be documented using the same format as Table 2.

2.4.2 Systematic method

The key to using the systematic method is to recognize that a control action is not hazardous by itself. For example, the control action *open train doors* is sometimes safe but sometimes unsafe. To determine whether the action is unsafe, it is necessary to first identify the context in which the action is provided. *Open train doors <u>while train is moving</u>* would be an unsafe control action, but *open train doors <u>while stopped at a platform</u>* is not only a safe control action, it is one that is required for proper system behavior. Notice that in this example the context also appears as part of the controller's process model in Figure 4. Because the process model captures the information that the controller needs to be aware of to make safe decisions, the context in a UCA can always be decomposed into variables and values that appear in the process model or in information communicated to the controller from its external environment.

In addition to context, there are several other elements that make up a UCA as shown in Figure 5. By decomposing unsafe control actions into several elements, it is possible to first concentrate on identifying each element in the safety control structure and then consider how the different elements can combine to form UCAs.

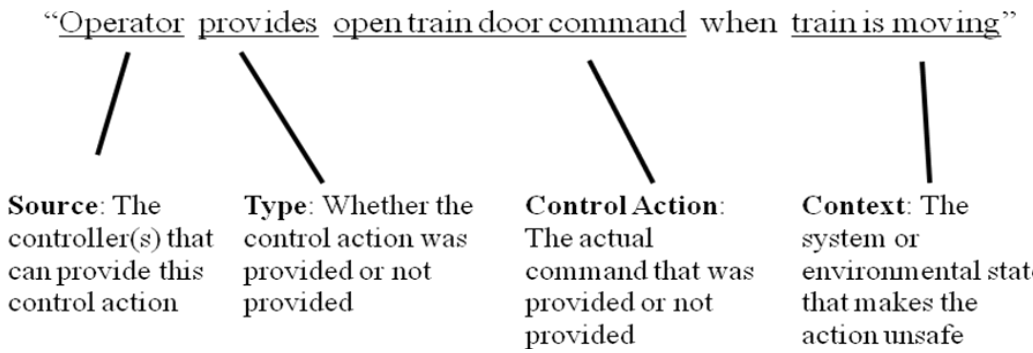

Figure 5: The Structure of an Unsafe Control Action

The first step of the systematic method is to select a control action and construct a *context table* as shown in Table 3. The first column indicates that this table analyzes the control action *Door Open*. The next three columns correspond to the process model variables for the selected control action. Each row is populated with a unique combination of process model values—i.e., a unique context.

Table 3: Example Context Table for Type *Provided*

Control Action (CA)	Train Motion	Emergency	Train Position	Hazardous?		
				if CA provided any time in this context	if CA provided too early in this context	if CA provided too late in this context
Door open command	Train is moving	No emergency	(doesn't matter)	Yes	Yes	Yes
	Train is moving	Emergency exists	(doesn't matter)	Yes	Yes	Yes
	Train is stopped	Emergency exists	(doesn't matter)	No	No	Yes
	Train is stopped	No emergency	Not aligned with platform	Yes	Yes	Yes
	Train is stopped	No emergency	Aligned with platform	No	No	No

Each row is then evaluated to determine whether the control action is hazardous in that context, and the result is recorded in the three columns on the right. The two right-most columns incorporate timing information as well. For example, providing an open door command in the context of an emergency while the train is stopped is not hazardous; in fact, that's exactly what should happen. However, providing the open door command too late in that context is certainly hazardous.

Table 4 shows a similar table for the type *not provided*. Note that too early or too late do not apply because the action is not provided.

Each hazardous row (row with a "yes" in the right column or right three columns) in either table is an unsafe control action that can be recorded in a summary table similar to Table 2. Note that much of this process can be automated given the information in the control structure. The left columns with the control action, type, and context can be generated automatically based on the control actions and process models defined in the control structure. The columns on the right indicating whether the actions are hazardous would still need to be filled in by engineers.

The next step is to translate the unsafe control actions into safety constraints.

Table 4: Example Context Table for Type *Not Provided*

Control Action 9CA)	Train Motion	Emergency	Train Position	Door State	Hazardous if CA not provided in this context?
Door Open command	Train is stopped	No emergency	Aligned with platform	Person not in doorway	No
	Train is stopped	No emergency	Aligned with platform	Person in doorway	Yes
	Train is stopped	No emergency	Not aligned with platform	(doesn't matter)	No
	Train is stopped	Emergency exists	(doesn't matter)	(doesn't matter)	Yes
	Train is moving	(doesn't matter)	(doesn't matter)	(doesn't matter)	No

2.5 Translating unsafe control actions into safety constraints

The unsafe control actions can be translated into safety constraints (requirements) that must be enforced to prevent accidents. This translation is fairly straightforward and usually involves inverting the wording of the unsafe control action. For example:

UCA 2: Doors are commanded open while train is in motion

Safety constraint: Doors must not be opened while train is in motion

The remainder of STPA examines the control structure to identify how the identified safety constraints can be violated, i.e., why unsafe control actions might be issued or why control actions required for safety might not be followed.

2.6 Identifying causal factors (Step 2)

Once the safety constraints are defined, the causal factors are identified that can lead to a violation of the constraint. Figure 6 shows a control loop with general types of causal factors included. These general causal factors can be used as "guidewords" in the analysis, similar to the use of guidewords in HAZOP.

Figure 6 also shows how causal factors can be classified based on the two ways that a safety constraint can be violated:

1. The controller provides an unsafe control action (causal factors above the diagonal line)
2. Appropriate control actions are provided but not followed (causal factors below the diagonal line)

Each case must be considered to identify all the causal factors that lead to a safety constraint violation.

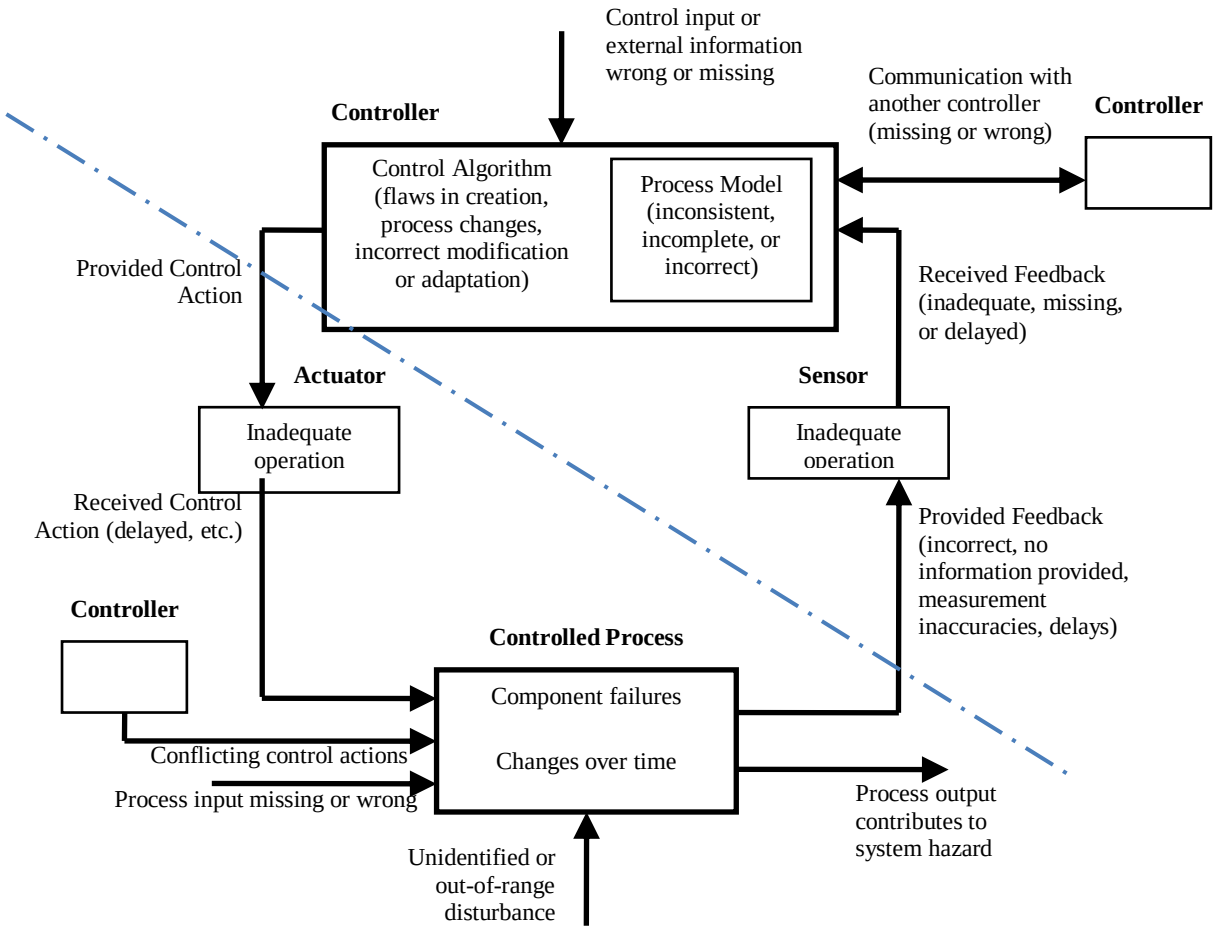

Figure 6: A classification of causal factors leading to hazards

1. The controller provides an unsafe control action

All the causal factors that could lead to the issuance of an unsafe control action must be identified. Consider **UCA 2**: Doors are commanded open while train is in motion.

This UCA might be caused by flaws in the controller's process model, for example, the controller may believe the train is stopped when in fact it is still moving. The reason for the process model flaw could be due to feedback that was missing or incorrect such as the speed indicator displaying 0 while the train is moving. The incorrect feedback, in turn, may have been caused by a speed sensor failure or a design flaw in which the sensor data was delayed. Many different scenarios can be constructed in this way to capture the causes of both component failure accidents and component interaction accidents.

2. Appropriate control actions are provided but not followed

Causal factors must also be identified that can violate the safety constraint even if a safe control action is provided. For example, consider again the train example and the safety constraint: Doors must not be opened while train is in motion.

The analyst needs to consider how the doors might be opened even if no UCA is provided, in other words, the open door command is not provided by the door controller but the doors open anyway. This behavior

could be caused by an actuator failure, by another controller (perhaps a manual lever near the door), or a problem with the controlled process itself (the doors).

2.7 Using Causal Factors

In a hierarchical, top-down design process, identified causal factors may be used to create safety requirements for more detailed refinements of the design or to create design features to eliminate or mitigate the causal factors leading to hazardous behavior. If the hazardous behavior can be eliminated at any point, further refinement may not be necessary.

When a design already exists and is being reviewed, the reviewers must evaluate whether the identified causal factors are adequately handled in the design. This is the place where design features and barriers added to mitigate hazards, such as interlocks, would be considered. Common-cause failures or errors can be identified by examining the causal factors for each of the control loops involved.

2.8 Iterating Through the Safety Control Structure

The STPA process is generally applied first at a high level using a high-level control structure with abstract control actions and feedback paths. For example, the control structure may represent an aircraft flight crew as a single controller with high-level control actions like *execute maneuver* and *abort maneuver*. A complex software system could be represented by a single controller labeled *engine controller* with basic control actions like *increase power* and *decrease power*. Once the analysis has been done for each controller at an abstract level, more detailed control structures can be constructed to analyze lower-level design details. For example, the flight crew might be decomposed into Captain and First Officer with distinct responsibilities and control actions. In this way, each step in the STPA process can be applied in an iterative, top-down fashion to refine the safety constraints as needed. If the hazardous behavior can be eliminated at any point, further refinement may not be necessary. How much refinement is necessary for mitigation measures will be problem specific.

3 Case Study

The case study for this research involves applying STPA to a generic version of an EPR (Evolutionary Power Reactor), which is a type of PWR (Pressurized Water Reactor). The EPR reactor is fully digital, that is, all control systems, including the Reactor Protection System, are digital. The analysis focuses on a sub-set of the Nuclear Power Plant (NPP) system: the systems involved in closing the Main Steam Isolation Valve (MSIV). The same process could be applied to the rest of the system.

A generic diagram of a PWR is shown in Figure 7. During normal operation, the coolant in the primary cooling system (left of the diagram) transfers heat from the reactor to the Steam Generator (SG). The SG contains water that cools the primary coolant and evaporates into steam. The SG prevents primary coolant, which is radioactive, from mixing with the water, which is not radioactive. The steam produced in the SG travels to a turbine connected to a generator to produce electricity. The steam is cooled in the condenser and pumped back into the SG to begin the cycle again. The loop formed by the SG, turbine, and condenser is known as the secondary cooling system.

The MSIV is a valve located on the main steam line from the SG. During normal operation, the MSIV is kept open to permit cooling of the primary cooling system via the secondary system. In case of an abnormal situation, the MSIV can be closed to isolate the SG from the rest of the secondary system. MSIV closure is necessary if there is a break in the main feedwater pipe to the SG that allows water to leak out, an internal SG Tube Rupture (SGTR) that allows primary coolant to mix with secondary water, or a break in the main steam line exiting the SG.

Because MSIV closure prevents the secondary system from adequately cooling the primary system, a number of backup systems are provided to cool the primary coolant in case of MSIV closure. These backup systems include redundant SGs, turbine bypass valves, main steam relief isolation valves (MSRIV) and main steam relief control valves (MSRCV), safety relief valves (SRV), the Chemical Volume Control System

(CVCS), and the Emergency Core Cooling System (ECCS). These systems are included in the analysis only to the extent that they impact the decision to close the MSIV.

The STPA analysis that follows begins by identifying the accidents, hazards, and control structure for the overall system. The remaining steps focus on those systems related to closure of the MSIV.

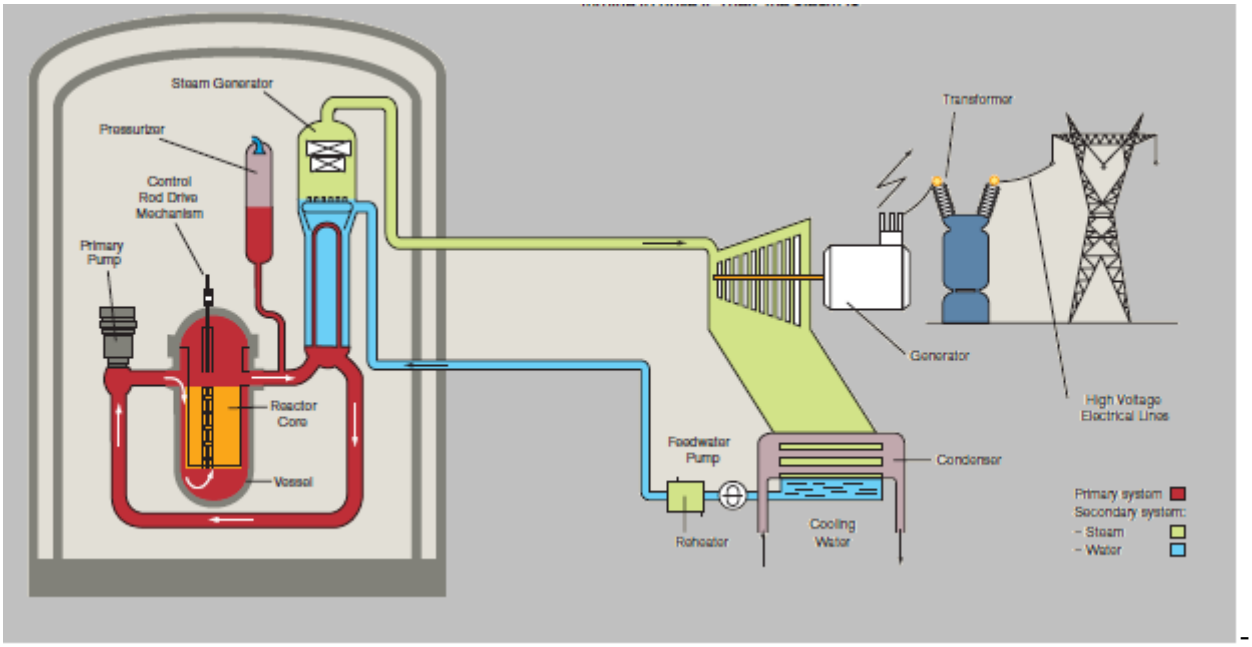

Figure 7: Pressurized Water Reactor (Diagram from AREVA Brochure)

3.1 Accidents

The first step is to identify the system-level losses, or accidents, to be considered. Accidents often involve loss of human life or injury, but any loss can be included that is unacceptable and must be prevented. Table 5 below shows the system-level accidents that are analyzed in this analysis.

Table 5: System-level accidents to be prevented

A-1: People injured or killed
A-2: Environment contaminated
A-3: Equipment damage (economic loss)
A-4: Loss of electrical power generation

People injured or killed (A-1) includes both employees and the general population, and may involve radiation exposure, explosion, or any other mechanism. Environment contaminated (A-2) includes radiation or other harmful release to the air, ground, or groundwater, or any other part of the environment. Equipment damage (A-3) refers to the economic loss associated with any damage to equipment regardless of whether any radiation is released. Loss of electrical power generation (A-4) includes any unplanned plant shutdown.

Priorities may be assigned as not all accidents are equally important. In addition, the accidents are not mutually exclusive, and in fact it is possible to experience all four losses at once. Finally, economic damage such as equipment loss or the loss of electrical power generation (A-4) may not be of immediate importance in a licensing review or a traditional safety analysis but it is certainly a concern for the utility. STPA can be used for any type of loss that is important to those doing the analysis. Incorporating other types of losses,

such as mission or economic losses, can not only allow better decision making with respect to achieving multiple requirements but can also assist in identifying and making tradeoffs between conflicting goals.

3.2 System Hazards

Once the system accidents have been defined, the hazards can be identified. Table 6 summarizes the hazards included in this analysis and the accidents to which they are related.

Table 6: System-Level hazards

Hazard	Related Accident
H-1: Release of radioactive materials	A-1, A-2
H-2: Reactor temperature too high	A-1, A-2, A-3, A-4
H-3: Equipment operated beyond limits	A-3, A-4
H-4: Reactor shut down	A-4

Release of radioactive materials (H-1) refers to any release outside the primary system, regardless of quantity, including releases into the secondary cooling system, groundwater, and air inside or outside the containment structure(s). These releases should be controlled to prevent exposure to people or the environment (A-1 and A-2). *Reactor temperature too high* (H-2) is a dangerous condition that can cause every system-level accident (for example, if the fuel rods melt), or it may lead to A-1 and A-2 without any radiation release (for example, through hydrogen production or other dangerous conditions).[1] Although H-2 may exist without an accident (for example, if there is a hydrogen explosion but containment holds), H-2 is a dangerous condition that should be controlled in the design. *Equipment operated beyond limits* (H-3) includes operation beyond safe limits that causes reactor damage or operation beyond design limits that causes damage to other equipment. *Reactor shut down* (H-4) includes any unplanned shutdown that may result in a loss of electrical power generation.

3.3 Safety Control Structure

The high-level safety control structure developed for this project is shown in Figure 8. The components inside the dashed (red) box control the closing of the MSIV. They are analyzed in further detail for the remainder of the case study. Figure 9 shows a more detailed control structure for the systems highlighted in the dashed box.

The dotted (green) arrow represents the communication between the MSIV controllers and other controllers. For example, the Protection System (PS) contacts the Safety Control System (SCS) in order to initiate the Engineering Safety Features (ESF) controls following ESF actuation. The Reactor Controls (RC) controller also communicates with Non-Safety System Controller (NSSC) in order to provide command signals for actuators used in RC functions other than control rods, such as the BMC (Boron and Makeup Control) components for Boron control.

There are four controllers that can provide a control action to close the MSIV: the Operator, the NSSC, the PS, and the Diverse Automation System (DAS). These four controllers send control actions to the MSIV Priority Module (PM), which uses a pre-programmed priority setting to determine which control actions to forward to the MSIV actuator. In this sense, the PM can also send control actions.

If the operator detects a need to close the MSIV, he or she may issue a *Close MSIV* command to the PM. The PM determines which controller is in charge according to a priority scheme, and forwards commands directly to the MSIV actuator. In this case, the PM would normally forward the command from the operator to the MSIV actuator.

[1] "Too high" is in relation to NRC standards and operation guidelines.

The operator may also send a *Close MSIV* command to the NSSC, which provides manual control for the MSIV. In this situation, the NSSC would normally forward the command from the operator to the PM, which would then forward the command to the MSIV actuator.

The PS is an automated system that can automatically detect some situations in which a *Close MSIV* command is necessary. In these situations the PS can provide the *Close MSIV* command to the PM which can forward the command to the MSIV actuator.

Finally, the DAS is a backup protection system that is used if there is a problem with the PS. The DAS can issue a *Close MSIV* command to the PM, which would normally forward the command to the MSIV actuator.

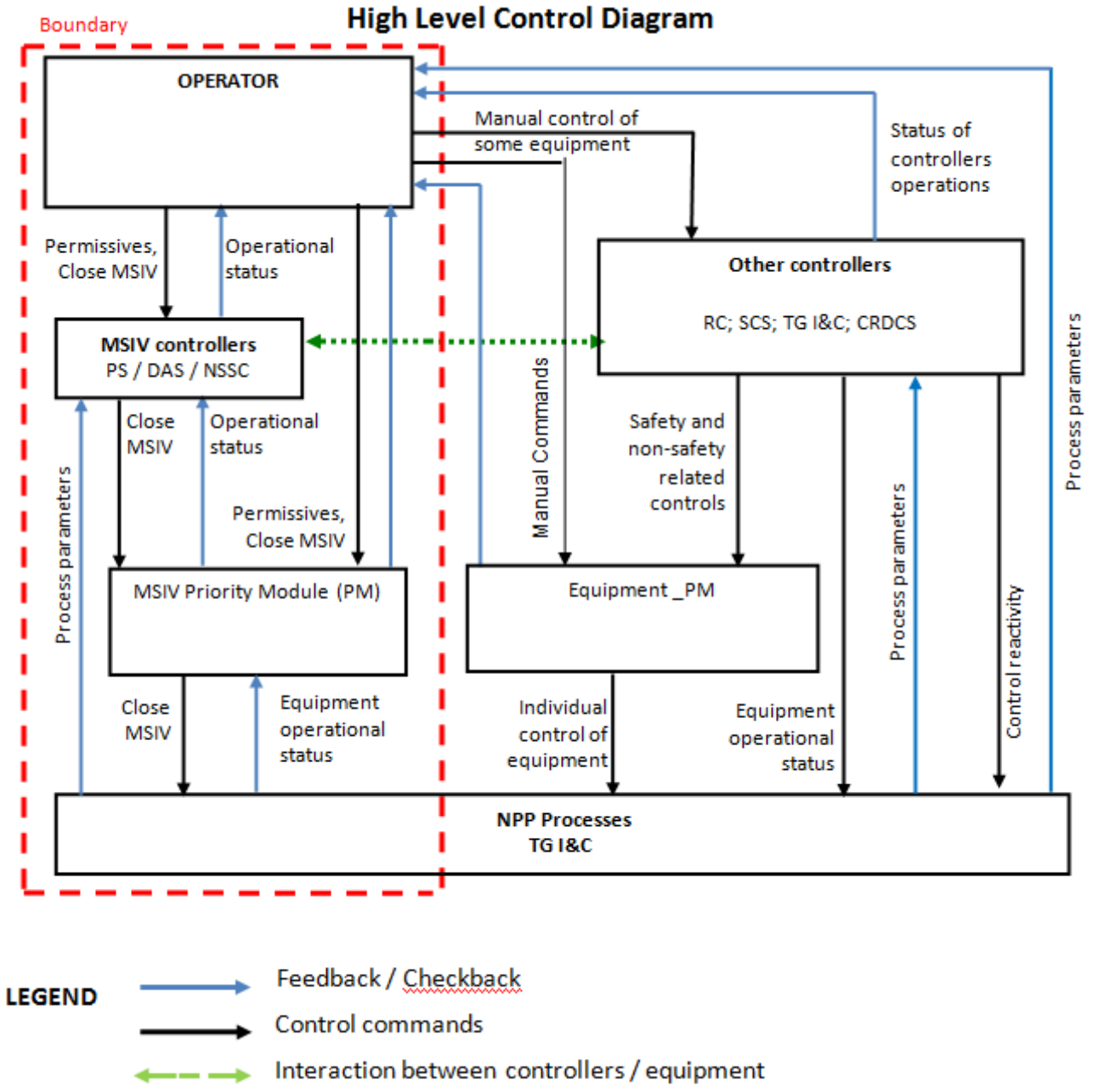

Figure 8: High-Level PWR Safety Control Structure

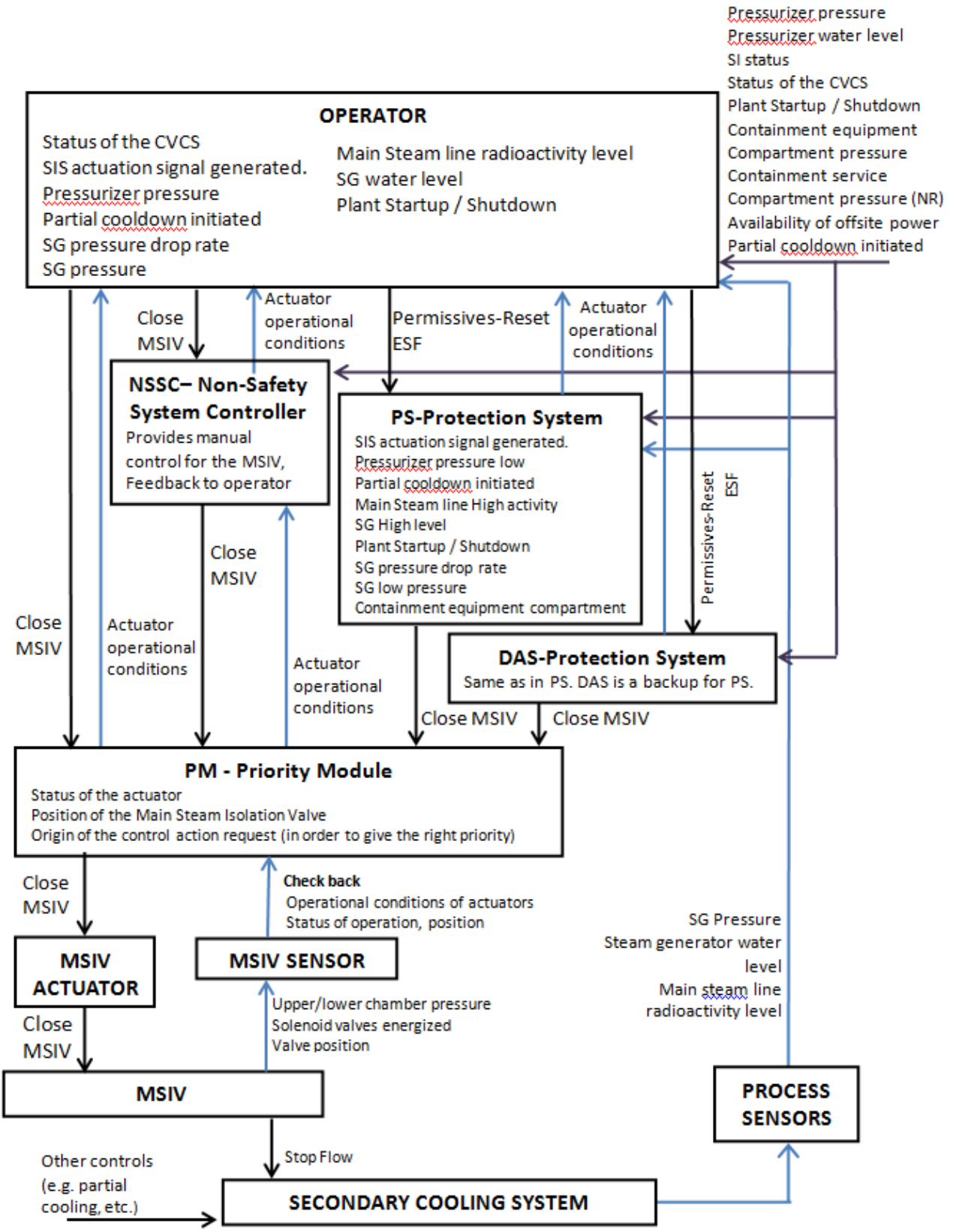

Figure 9: Safety Control Structure for MSIV

A sensor provides feedback about the MSIV status directly to the PM. This sensor does not sense process variables such as pressure, temperature, or steam flux. Instead, it senses torque applied to the valve itself to detect if the valve has closed. The PM receives this feedback and can provide confirmation back to the controller that originally requested the MSIV closure.

Other process sensors report process variables to the controllers including various pressures, SG water level, and the operation of other backup systems. This information is used by the controllers to determine, among other things, whether the MSIV should be closed.

The controllers have responsibilities as follows:

Operator :

- Validate/inhibit permissives
- Bring the plant to a controlled shutdown in case of Anticipated Operational Occurrence (AOO) or Postulated Accidents (PA), such as leakage from primary into the secondary loop.
- Activate the safety engineering features (ESF)
- Start main steam line isolation when necessary
- Monitor parameters and look for abnormalities or trends (fault diagnostic)
- Operate the plant during startup
- Operate the plant during programmed shutdown
- Take actions in accordance to written guides upon any transient or emergency

PS - Protection System:

- Bring the plant to a controlled shutdown in case of Anticipated Operational Occurrence (AOO) or Postulated Accidents (PA), such as leakage from primary into the secondary loop.
- Activate the safety engineering features (ESF)
- Start main steam line isolation when necessary

DAS - Diverse Automation System

- Same as PS. DAS is a backup for PS.

NSSC - Non-Safety System Controller

- If an operator command to open/close MSIV is received, then send that command to PM
- If feedback is received from PM, then send that feedback to Operator.

PM - Priority Module

- Give access to control commands according to following priority:
  PS > DAS > SCS > Operator > NSSC
- Forward commands to MSIV actuator
- Forward feedback from MSIV actuator to the active controller
- Ensure that checkback is received when MSIV is closed (indicating that valve torque has reached its maximum)
- Check for any problems with MSIV actuator operability

3.4 Process Model Variables

The process model variables capture the information needed by each controller to decide what control action to provide. Different process model variables may be associated with each control action. The high-level process model variables associated with MSIV closure can be identified by considering the purpose of the MSIV. The MSIV remains open during normal plant operation and is only needed to control a few

specific abnormal conditions. The relevant high-level conditions can be derived from the system hazards and system description as follows: [2]

- Steam generator tube rupture, which can cause an uncontrolled SG level increase and can release contaminated fluid into the secondary system
- Steam system piping leak, which can depressurize the SG and cause an overcooling transient and energy release into containment
- Feedwater system piping leak, which can depressurize the SG and cause an overcooling transient and energy release into containment

While these conditions could be caused by physical failures, the latter two could also be caused by design flaws or unsafe commands elsewhere in the system. For example, a leak in the main steam line could be caused by a physical failure (e.g. rupture in the line) or it could be caused by main steam relief valves that are opened inadvertently or at the wrong time. Both situations could require MSIV closure to prevent depressurization and an overcooling transient while the issue is investigated and resolved.

In addition to helping to mitigate the conditions above, the MSIV also controls the heat exchange that takes place within the SG. Before the SG is closed, other support systems[3] may need to be engaged to provide adequate cooling. Therefore, information about additional cooling provided by other support systems (i.e. inadequate, adequate) may be needed for the decision to close the MSIV and should be included in the process model.

3.5 Unsafe Control Actions

When considering whether a potential control action is hazardous or not, it is important to avoid assuming that other defense barriers are intact or that they are appropriate, sufficient, and error-free. For example, even if there is an emergency feedwater system to provide the necessary cooling in the event of a relief valve inadvertently commanded open, it is still hazardous to inadvertently command the relief valve open. These hazardous actions must be included in the analysis and prevented regardless of other protective systems intended to mitigate unsafe behavior.

Table 7 summarizes the unsafe control actions identified for the command *Close MSIV*.

[2] See also U.S EPR Final Safety Analysis Report Chapter 7 pages 7.3-22 and 7.3-11

[3] *Other support systems* refers to other components designed to cool the primary system. These include the CVCS, SI, CCS, etc. *Adequate* means the system operation is sufficient to provide the cooling normally provided by the SG.

Table 7: Unsafe Control Actions for Close MSIV

Control Action	Unsafe Control Actions			
	Not Providing Causes Hazard	**Providing Causes Hazard**	**Wrong Timing or Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Close MSIV	Close MSIV not provided when there is a rupture in the SG tube, leak in main feedwater, or leak in main steam line [H-2, H-1, H-3]	Close MSIV provided when there is no rupture or leak [H-4] Close MSIV provided when there is a rupture or leak while other support systems are inadequate [H-1, H-2, H-3]	Close MSIV provided too early (while SG pressure is high): SG pressure may rise, trigger relief valve, abrupt steam expansion [H-2, H-3] Close MSIV provided too late after SGTR: contaminated coolant released into secondary loop, loss of primary coolant through secondary system [H-1, H-2, H-3] Close MSIV provided too late after main feedwater or main steam line leak [H-1, H-2, H-3, H-4]	N/A

The unsafe control actions in Table 7 were identified using the following process. First, a controller and control action were selected. The operator and the control action *Close MSIV* were analyzed first, although the results also apply to other controllers in the system. A context table was then constructed for the control action using the corresponding process model variables that were defined previously. Table 8 shows the context table for *Close MSIV provided*.

Table 8: Context table for *Operator provides Close MSIV* control action

	1	2	3	4	5	6	7	8
	Control Action	**Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**	**Control Action Hazardous?**	**Control Action Hazardous if Too Late?**	**Control Action Hazardous if Too Early?**
1	*Close MSIV*	Not Ruptured	No Leak	No Leak	Adequate	H-4	H-4	H-4
2		Ruptured	No Leak	No Leak	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
3		Not Ruptured	Leak	No Leak	Adequate	No	H-2, H-3, H-4	No
4		Not Ruptured	No Leak	Leak	Adequate	No	H-2, H-3, H-4	No
5		Ruptured	Leak	No Leak	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
6		Not Ruptured	Leak	Leak	Adequate	No	H-2, H-3, H-4	No
7		Ruptured	No Leak	Leak	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
8		Ruptured	Leak	Leak	Adequate	No	H-1, H-2, H-3, H-4	H-3, H-4
9		Not Ruptured	No Leak	No Leak	Inadequate	H-2, H-4	H-2, H-4	H-2, H-4
10		Ruptured	No Leak	No Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
11		Not Ruptured	Leak	No Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
12		Not Ruptured	No Leak	Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
13		Ruptured	Leak	No Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
14		Not Ruptured	Leak	Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
15		Ruptured	No Leak	Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
16		Ruptured	Leak	Leak	Inadequate	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4

Column 1 in Table 8 is the control action being analyzed while columns 2 to 5 correspond to the process model variables identified earlier. Column 6 specifies in which contexts it is hazardous to provide the *Close MSIV* control action. For example, row 1 describes a situation in which it is hazardous to close the MSIV: if there is no SG tube rupture, no main feedwater pipe leak, and no main steam line leak, then there is no need to close the MSIV. Closing the MSIV will cause H-4 (reactor shut down). If the operation of other support systems cannot make up for the additional heat exchange required, closing the MSIV will also lead to a loss of necessary cooling (H-2 in row 9 column 6).

If other support systems, including other CVCS, SI, ECCS, etc., are producing the additional cooling required during a rupture/leak, then closing the MSIV is not hazardous (rows 2-8, column 6) and a reactor shutdown is initiated regardless of any MSIV actions. If for some reason the other systems are not capable of producing the additional cooling needed, then closing the MSIV may cause other hazards (rows 10-16, column 6) including excessive temperature increase (H-2), release of radioactive materials (H-1), an immediate reactor shutdown or SCRAM (H-4) if not already triggered, and additional equipment damage (H-3). Depending on the type of rupture, it may actually be better to keep the MSIV open to control the temperature of the reactor (H-2) even though that would permit some radioactive steam to be introduced into the secondary system (H-1).

The last two columns on the right in Table 8 take into account timing information. If there is a rupture/leak and other support systems are adequate, then it is not hazardous to close the MSIV (e.g. row 2-8). The MSIV should be closed. However, if the MSIV is closed *too late* in this context then it is hazardous. If the steam generator tube is ruptured, too much radioactive coolant may have already been released into the secondary system and the environment (H-1). If the steam line has a leak, excessive steam may have been released causing overcooling and overcompensation (H-2). If the steam line or feedwater pipe have a leak, the SG may run dry and cause equipment damage (H-3). Closing the MSIV *too early* may also be hazardous in some situations. For example, if the steam generator tube is ruptured then the SG pressure should be decreased before the MSIV is closed. Otherwise, if the MSIV is closed too early after a SG tube rupture, then the SG pressure and temperature will increase and may cause equipment damage to the SG, SG piping, or other systems (H-3).

The contexts used to define unsafe control actions may not be the same as contexts that are inherently unsafe. The tables in this section are used to analyze controller behavior and control actions in a number of contexts, not to analyze contexts that are unsafe by themselves. For example, row 1 column 6 of Table 8 is marked as hazardous because the control action *Close MSIV* will cause a hazard if provided in that context, even though the context by itself (no ruptures/leaks) does not describe anything hazardous. Conversely, the context in row 2 describes a steam generator tube rupture but column 6 is not marked as hazardous because closing the MSIV is not a hazardous behavior in that context. In fact, closing the MSIV is exactly what should happen in that situation to prevent an accident.

Although providing a control action can be hazardous, *not* providing a control action can be equally hazardous. Table 9 shows the context table for *not* providing the *Close MSIV* control action. As before, a reactor shutdown should be initiated for any rupture regardless of the MSIV control action. However because these tables are used to identify unsafe control actions, only hazards that are affected by an absent *Close MSIV* control action are listed at this stage of the analysis.

If there is no rupture/leak, keeping the MSIV open is not hazardous (rows 1 and 9). However, if there is a rupture/leak, different hazards may be experienced depending on what part of the system is affected. If the SG tube is ruptured and the MSIV is not closed, radioactive material will be released into the secondary system (H-1) and the SG water level may increase uncontrollably. A sustained release of primary coolant will decrease the effectiveness of the primary cooling system (H-2), and the release of radioactive material into the secondary system may cause equipment damage (H-3). If the main steam line has a leak and the MSIV is not closed, excessive steam may be released causing an overcooling transient and overcompensation by other systems to increase reactivity (H-2). Excessive steam release may also lower the SG water level, causing potential equipment damage if the SG runs dry (H-3). If the main feedwater pipe has a leak and the MSIV is not closed, the SG may be depressurized causing an overcooling transient and water level may drop, leading to H-2 and H-3 as above.

Table 9: Context table for *Close MSIV control action is not provided*

	1	2	3	4	5	6
	Control Action	**Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems[4]**	**Not Providing Control Action is Hazardous?**
1	*Close MSIV*	Not Ruptured	No Leak	No Leak	Adequate	No
2		Ruptured	No Leak	No Leak	Adequate	H-1, H-2, H-3, H-4
3		Not Ruptured	Leak	No Leak	Adequate	H-2, H-3
4		Not Ruptured	No Leak	Leak	Adequate	H-2, H-3
5		Ruptured	Leak	No Leak	Adequate	H-1, H-2, H-3, H-4
6		Not Ruptured	Leak	Leak	Adequate	H-2, H-3
7		Ruptured	No Leak	Leak	Adequate	H-1, H-2, H-3, H-4
8		Ruptured	Leak	Leak	Adequate	H-1, H-2, H-3, H-4
9		Not Ruptured	No Leak	No Leak	Adequate	No
10		Ruptured	No Leak	No Leak	Inadequate	H-1, H-2, H-3, H-4
11		Not Ruptured	Leak	No Leak	Inadequate	H-2, H-3
12		Not Ruptured	No Leak	Leak	Inadequate	H-2, H-3
13		Ruptured	Leak	No Leak	Inadequate	H-1, H-2, H-3, H-4
14		Not Ruptured	Leak	Leak	Inadequate	H-2, H-3
15		Ruptured	No Leak	Leak	Inadequate	H-1, H-2, H-3, H-4
16		Ruptured	Leak	Leak	Inadequate	H-1, H-2, H-3, H-4

[4] *Other support systems* refers to other systems designed to cool the primary system. This includes the CVCS, SI, CCS, etc. *Adequate* means the system operation is sufficient to provide the cooling normally provided by the SG.

In the case of SG tube rupture, keeping the MSIV open can cause not only equipment damage but also a more immediate shutdown (H-4) via SCRAM and can increase the amount of time the plant will need to remain shut down for repairs. The overfilling of the SG could allow water to enter the steam lines, damaging the delicate turbine pallets and requiring extensive time for repairs. In addition to actual damage, equipment can be overstressed and require more detailed inspections before the plant can be operational again. The additional contamination will also require more time to decontaminate and will result in the generation of more waste. Because keeping the MSIV open during a SG tube rupture will cause a more severe and prolonged shutdown than would otherwise occur with a contained SG tube rupture, H-4 is included in Table 9 for these cases. H-4 is not listed for other cases because it is assumed that keeping the MSIV open after a leak in the main steamline or main feedwater pipe will not cause a more severe or prolonged shutdown than if the MSIV is closed, although it does contribute to the other hazards listed.

Note that for the purpose of reviewing the tables, the rationale behind each of the "hazardous" vs. "not hazardous" decisions should be documented during the analysis. In fact, the context tables can be used to help verify that the necessary rationales and assumptions are documented during the analysis, as opposed to ad-hoc identification of hazardous control actions that may immediately discount and omit non-hazardous control actions entirely. Of course, the non-hazardous rows could easily be omitted from the context tables if desired; however, documenting the conclusions about what behavior is hazardous can be just as important as documenting behavior that is assumed to be non-hazardous. Such documentation may be especially important for other long-term project goals like future change management activities, design re-use in new environments, and other considerations that arise later in the system lifecycle.

A comparison of Tables 8 and 9 shows that there are conflicts that must be resolved. In both tables, rows 10 to 16 are marked as hazardous. In other words, in these situations it is hazardous to close the MSIV yet hazardous to keep the MSIV open. In some cases, it is possible to revisit the design to eliminate the conflict and provide a safe option. If the conflict cannot be resolved, a decision must be made about what action should be taken in these contexts, that is, which is the *least* hazardous? For this case study, after consultation with nuclear engineers and regulators it was found that rows 10 to 16 may not have been analyzed in previous safety analyses with respect to MSIV control. For the purposes of this research, the consensus was to assume that it may be best to keep the MSIV open in the context of row 10 to maximize the amount of cooling provided even though doing so will contaminate the secondary cooling system and eventually require costly repairs. Rows 11-16, on the other hand, involve leaks in the pipe supplying water to the steam generator and/or the line that carries steam away. If the MSIV is left open in these situations, the amount of water in the steam generator can decrease and eventually lead to less cooling capability or an overcooling transient. Therefore, in these situations (rows 11-16), it was assumed that it may be best to keep the MSIV closed to maximize the amount of cooling provided even though it is only a temporary measure. These solutions were found to differ from current designs of MSIV controllers, which do not act based on the state of other support systems and may automatically close the MSIV during any rupture.

Both of these assumptions should be reviewed and evaluated carefully by domain experts. The purpose of this research case study was not to provide final solutions to these hazardous situations, but to develop and apply hazard analysis methods that can uncover hazardous control and provide the safety-critical questions that need to be considered. Note that although Tables 8 and 9 uses high-level contexts, the analysis can also be performed in more detail if necessary. A more detailed analysis could be necessary if, for example, it is found that the best solution depends on the type of steam generator tube rupture, the amount of pressure in the SG, etc.

Of course, in any of these situations, there are other control actions that need to take place outside the MSIV control loop—they can be analyzed using the same approach. In addition, every effort should be made to prevent many of these contextual conditions from existing in the first place. Although such additional efforts were outside the scope of this initial case study, they are mentioned here to show how the analysis may branch out into other areas of the system to address the issues identified.

3.6 Safety Constraints

Each of the unsafe control actions from Table 7 can be translated into safety constraints as shown in Table 10.

Table 10: Safety Constraints

Unsafe Control Action	**Safety Constraint**
UCA 1: Close MSIV not provided when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate	**SC 1**: MSIV must be closed when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate
UCA 2: Close MSIV not provided when there is a main feedwater or main steam line leak and other support systems are inadequate	**SC 2**: MSIV must be closed when there is a main feedwater or main steam line leak and other support systems are inadequate
UCA 3: Close MSIV provided when there is a SGTR but support systems are inadequate	**SC 3**: MSIV must not be closed when there is a SGTR and support systems are inadequate
UCA 4: Close MSIV provided too early (while SG pressure is high)	**SC 4**: MSIV must not be closed too early while SG pressure is too high
UCA 5: Close MSIV provided too late after rupture/leak (in the SG tube, main feedwater, or main steam line)	**SC 5**: MSIV must not be closed too late after rupture/leak (in the SG tube, main feedwater, or main steam line)
UCA 6: Close MSIV provided when there is no rupture/leak	**SC 6**: MSIV must not be closed when there is no rupture/leak

3.7 Causal Factors

As described in Section 2.6, there are two ways that a safety constraint can be violated:

(1) The controller provides an unsafe control action

(2) Appropriate control actions are provided but not followed

The causal factors shown in Figure 6 are used for the analysis in this case study. The following sections analyze both cases for the Operator, DAS, and PS.

3.7.1 Operator Causal Factors

Causal Factors Leading to Operator Unsafe Control Actions

This section identifies causal factors that can lead to each unsafe control action summarized in Table 10 for the Operator.

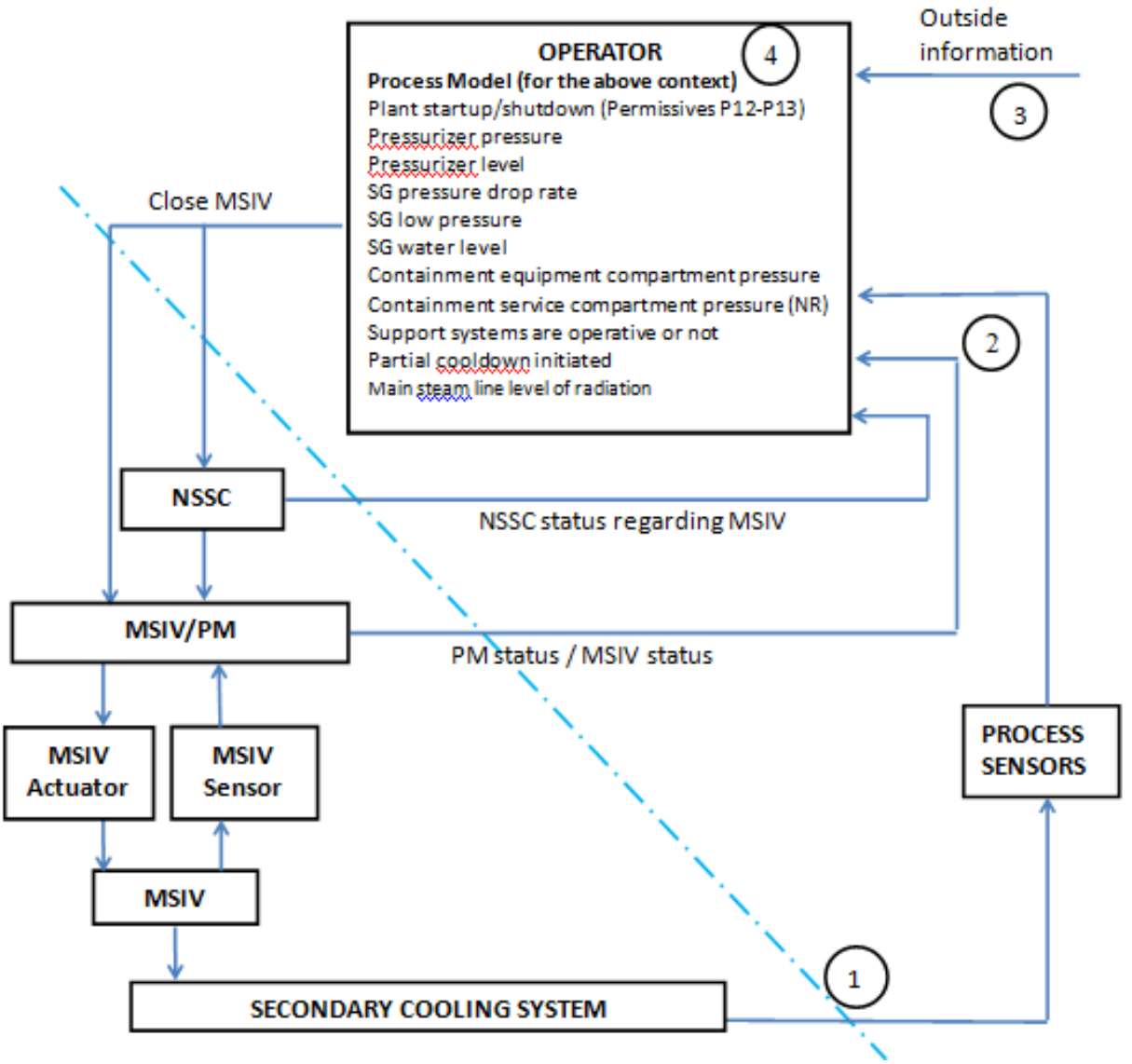

Figure 10: Causal Factors Leading to Operator Unsafe Control Actions

UCA 1: Close MSIV command not provided when there is a leak (rupture in the SG tube, link in main feedwater, or leak in main steam line) and the support systems are adequate.

(1) Secondary cooling system (CVCS or emergency feedwater system)
   a. Concurrent situation masks another. For example, a feedwater problem could happen concurrent with a SGTR, causing the SG water level to stay practically stable.
   b. Situation that requires MSIV closure is masked. For example, NSSC engages PZR heaters to make up for loss of RCS pressure during SGTR.
   c. Event progresses too slowly to detect

(2) Process Feedback
   a. SG level feedback missing, delayed, or incorrect
   b. SG Pressure, or setpoints, is not correct or delayed
   c. Steam generator water level delayed or incorrect
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not operate properly and gives wrong measures
   g. No indication of partial cool down initiated
   h. Failures in sensors, communication lines, or power
   i. PM reports both MSIV actuators as inoperable when they are
   j. PM reports MSIV already closed, when it is not
   k. NSSC reported as operational (or no feedback provided) when it is not

(3) Outside information
   a. PZR pressure delayed or missing
   b. PZR level incorrectly indicated as normal
   c. No indication of SI initiated
   d. Delayed indication of SI initiated
   e. Inappropriate permissives in effect[5]
   f. Wrong combination of indicators from the 4 divisions

(4) Operator
   a. Operator believes Steam Generator is not ruptured when it is ruptured
   b. Operator believes the main steam line has no leak when it has a leak
   c. Operator believes the main feedwater has no leak when it has a leak
   d. Operator confused about the procedure to be followed
   e. Operator confused because of conflicting indicators[5]
   f. Operator reluctant to shutdown the reactor, unsure if shutdown is necessary or warranted
   g. Operator under pressure not to trip reactor
   h. Operator waits for the PS to handle the situation (e.g. Operator recognizes possible SGTR but believes PS will handle it)
   i. Operator is not aware of the problem due to inadequate feedback (e.g. screen is frozen)
   j. Operator is not aware because NSSC is inoperative or providing inadequate information
   k. Operator closes the wrong valve

[5] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong

l. Operator recognizes the rupture/leak but believes other support systems are inadequate, and keeps MSIV open to maintain sufficient cooling capability.
m. Operator uncertain whether a rupture/leak exists (there is a conflict between being conservative under uncertainty versus immediate manual spurious shutdown which costs money and may be discouraged. May also prefer to wait for the automated system to resolve the problem versus intervening under uncertainty)
n. Operator believes NSSC is operational when it is not (could cause operator to provide command to an inoperative or disabled NSSC instead of directly to PM)

UCA 2: Close MSIV command not provided when there is a main feedwater or main steam line leak and other support systems are inadequate.

(1) Secondary cooling system (CVCS or emergency feedwater system)
   a. Concurrent situation masks another. For example, a feedwater problem could happen concurrent with a SGTR, causing the SG water level to stay practically stable.
   b. Situation that requires MSIV closure is masked.
   c. Event progresses too slowly to detect
(2) Process Feedback
   a. SG level feedback missing, delayed, or incorrect
   b. SG Pressure, or setpoints, is not correct or delayed
   c. Steam generator water level delayed or incorrect
   d. Conflicting data indicating a false situation
   e. Voting system does not operate properly and gives wrong measures
   f. No indication of partial cool down initiated
   g. Failures in sensors, communication lines, or power
   h. PM reports both MSIV actuators as inoperable when they are
   i. PM reports MSIV already closed, when it is not
   j. NSSC reported as operational (or no feedback provided) when it is not
(3) Outside information
   a. PZR pressure delayed or missing
   b. PZR level incorrectly indicated as normal
   c. No indication of SI initiated
   d. Delayed indication of SI initiated
   e. Inappropriate permissives in effect[6]
   f. Wrong combination of indicators from the 4 divisions
(4) Operator
   a. Operator believes the main steam line has no leak when it has a leak
   b. Operator believes the main feedwater has no leak when it has a leak
   c. Operator believes there is an SGTR that does not require MSIV closure when there is actually a main steam line or main feedwater leak that does require MSIV closure
   d. Operator confused about the procedure to be followed

[6] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong

e. Operator confused because of conflicting indicators[5]
f. Operator reluctant to shutdown the reactor, unsure if shutdown is necessary or warranted
g. Operator under pressure not to trip reactor
h. Operator waits for the PS to handle the situation (e.g. Operator recognizes possible leak but believes PS will handle it)
i. Operator is not aware of the problem due to inadequate feedback (e.g. screen is frozen)
j. Operator is not aware because NSSC is inoperative or providing inadequate information
k. Operator closes the wrong valve
l. Operator recognizes the rupture/leak but because other support systems are inadequate, keeps MSIV open in an effort to maintain sufficient cooling capability.
m. Operator uncertain whether a rupture/leak exists (there is a conflict between being conservative under uncertainty versus immediate manual spurious shutdown which costs money and may be discouraged. May also prefer to wait for the automated system to resolve the problem versus intervening under uncertainty)
n. Operator believes NSSC is operational when it is not (could cause operator to provide command to an inoperative or disabled NSSC instead of directly to PM)

UCA 3: Close MSIV provided when there is SGTR but other support systems are inadequate

(1) Secondary cooling system
   a. A concurrent situation could mask another, other support systems could appear adequate but may not be, and automated systems could exacerbate the situation. For example, main steam line high radioactivity may be detected coincident with safety injection, making it difficult to detect whether partial cooldown was initiated by the automation.
   b. Loss of power
(2) Process Feedback
   a. SG level feedback not provided, delayed, or incorrect
   b. SG Pressure or setpoints are not correct, delayed, or missing
   c. Steam generator water level not correct, delayed, or missing
   d. Conflicting data indicating a false situation
   e. Voting system does not operate properly and gives wrong measures
   f. Failures in sensors, communication lines, or power
(3) Outside information
   a. Wrong combination of indicators from the 4 divisions
   b. PZR pressure delayed or missing
   c. False signal SI initiated
(4) Operator
   a. Operator thinks support systems are working when they are not. For example, NSSC may appear to be working but may not be because the screen is frozen. The operator may believe that a partial cool down was initiated by the automation because safety injection was engaged at the same time that main steam line radioactivity was detected
   b. Operator believes there is a main steam line or feedwater leak when there is actually an SGTR
   c. Operator knows support systems are working, but does not realize they are inadequate
   d. Operator confused about the procedure to be followed
   e. Operator confused because of conflicting indicators

f. Operator does not realize other support systems are not operative (e.g. for maintenance or other reasons)

UCA 4: Close MSIV provided too early (while SG pressure is high)

(1) Secondary cooling system
   a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrently with a SGTR, and the SG water level stay practically stable.
   b. Event progress too slowly to detect
   c. Actuation of NSSC could confuse Operator. For example, PZR heaters could make up for loss of RCS pressure

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure, or setpoints, is not correct
   c. Steam generator water level not correctly indicated
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not work properly and gives wrong measures
   g. Sensors failure

(3) Outside Information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates PZR level is normal
   d. No indication of SI initiated
   e. No indication of partial cool down initiated
   f. Permissives wrongly in effect[7]
   g. Wrong combination of indicators from the 4 divisions

(4) Operator
   a. Operator believes it is already safe to initiate action after indications confirm SGTR
   b. Operator believes it is already safe to initiate action after indications confirm Main steam line break
   c. Operator believes it is already safe to initiate action after indications confirm main feedwater break
   d. Operator confused about the procedure to be followed
   e. Operator confused because of conflicting indicators

UCA 5: Close MSIV command provided too late after rupture/leak (in the SG tube, main feedwater, or main steam line)

(1) Secondary cooling system

[7] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong.

a. A concurrent situation could mask another one. For example, a feedwater problem could happen concurrently with a SGTR such that the SG water level stays practically stable.
b. Event progress too slowly to detect
c. Actuation of NSSC could confuse Operator. For example, PZR heaters could make up for loss of RCS pressure

(2) Process Feedback
a. SG level feedback not provided
b. SG Pressure, or setpoints, is not correct
c. Steam generator water level delayed
d. Main steam line activity not correctly indicated or delayed
e. Conflicting data indicating a false situation
f. Voting system does not work properly and gives wrong measures
g. Sensor failure
h. PM reports both MSIV actuators as inoperable when they are
i. PM reports MSIV as already closed, when it is not
j. NSSC reported as operational (or no feedback) when it is not

(3) Outside Information
a. PZR pressure delayed
b. PZR feedback missing
c. False feedback indicates PZR level is normal
d. No indication or delayed indication of SI initiated
e. No indication or delayed indication of partial cool down initiated
f. Permissives wrongly in effect
g. Wrong combination of indicators from the 4 divisions
h. Screen is blank or frozen/NSSC or PS provides no feedback

(4) Operator
a. Operator thinks it is not yet safe to initiate action after SGTR is confirmed
b. Operator thinks it is not yet safe to initiate action after main steam line leak is confirmed
c. Operator thinks it is not yet safe to initiate action after main feedwater leak is confirmed
d. Operator confused about the procedure to be followed
e. Operator confused because of conflicting indicators
f. Operator reluctant whether to shutdown the reactor
g. Operator under pressure not to trip reactor
h. Operator has a conflict between being conservative with uncertainty of whether there is a SGTR, or to do what it is expected, i.e. to wait for the automated system to resolve the problem. In other words, the operator tries to avoid spurious shutdown, which costs money and should be avoided.
i. Operator waits for the PS to handle the situation, does not act in time

UCA 6: Close MSIV provided when there is no rupture/leak

(1) Secondary cooling system
a. Feedwater pumps not working properly
b. Condenser leaking (loosing water)
c. Too much sludge in water (blocking water)
d. Object in water that could cut flux to SG
e. Spurious opening of relief valves

(2) Process Feedback
    a. SG level feedback not provided
    b. SG Pressure low (setpoints not correct)
    c. Steam generator water level delayed or incorrect
    d. False SG isolation signal[8]
    e. Main steam line activity (false positive signal)
    f. Conflicting data indicating a false situation where close valve would be needed
    g. Voting system does not work properly and gives wrong measures
    h. Sensor Failure
(3) Outside Information
    a. PZR pressure indication delayed
    b. PZR feedback missing
    c. False PZR pressure feedback
    d. False feedback shows PZR level as low
    e. False signal of initiation of SI
    f. False Partial cool down initiated signal
    g. Startup/shutdown not recognized[9]
    h. Wrong combination of indicators from the 4 divisions
(4) Operator
    a. Operator thinks Steam Generator Tubes are ruptured when they are not
    b. Operator thinks the main steam line has a leak when it does not
    c. Operator thinks main feedwater has a leak when it does not
    d. Operator confused about the procedure to be followed
    e. Operator confused because of conflicting indicators
    f. Blank screen induces operator to think situation is different
    g. False alarm of radiation
    h. Close wrong valve, other SG

Causal Factors Leading to an Operator Control Action Not Being Followed

In addition to identifying why unsafe control actions might be provided, it is important to analyze how safe control actions may not be followed appropriately. This section identifies how the safety constraints could be violated even if safe control actions are provided. Figure 11 shows areas of the control loop in which additional causal factors can lead to a violation of Safety Constraints 1 to 6.

[8] This could occur, for example, in a situation where the water level at the SG is low concurrent with a SG low pressure, which could be due to an open Relief Valve.

[9] One of the causes for wrong command can be confusion about indicators. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment. Or, SG low level combined with permissive 13 (startup) means there is no need to isolate the SG. It could happen that there would be a problem with the sensors, or the model (inside the controller) could be wrong, or algorithm could be wrong. “Confusion" could mean the model is not clear, or that there is an overlap of values.

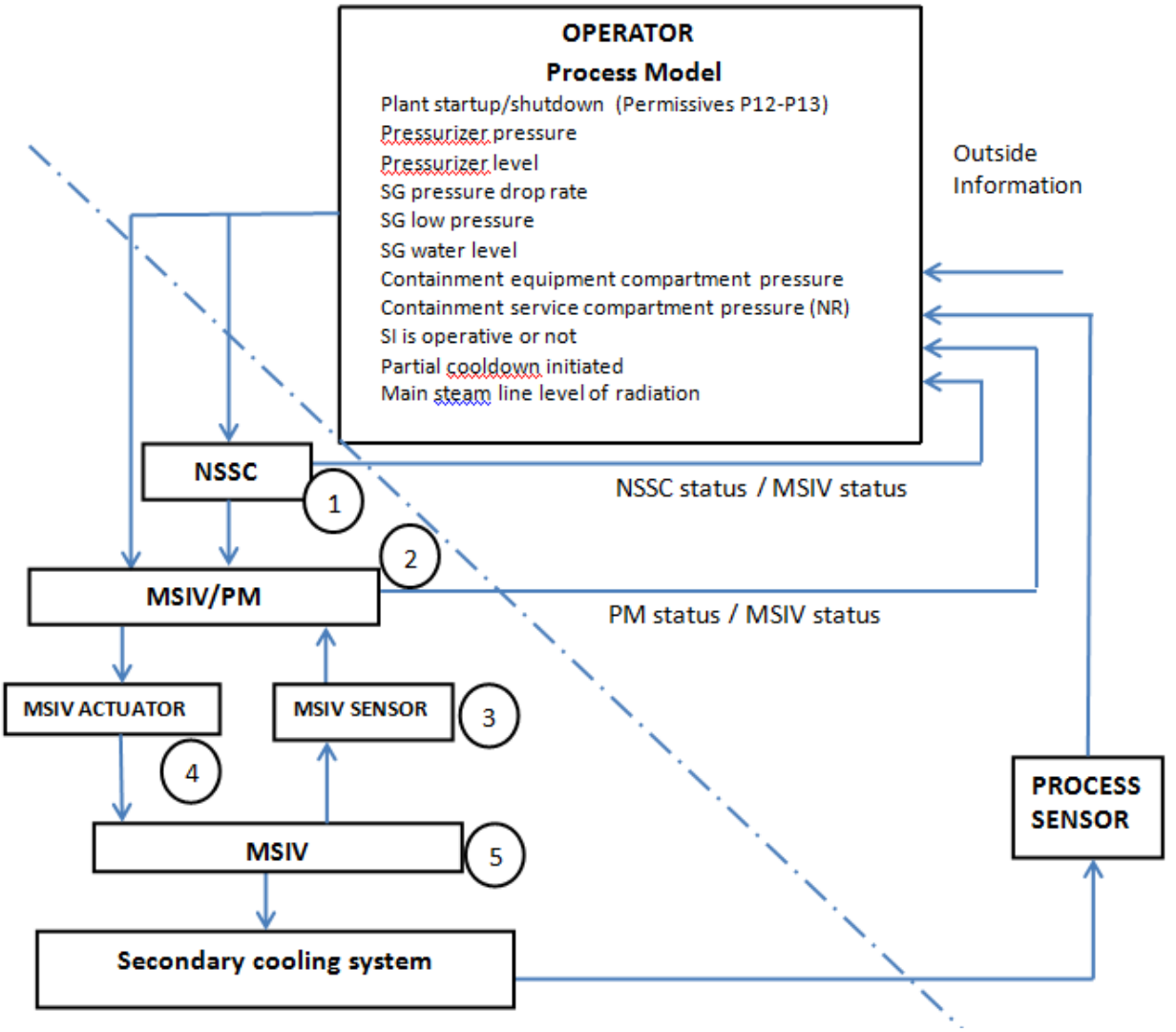

Figure 11: Causal Factors Leading to Operator Control Actions Not Being Followed

SC 1: MSIV must be closed when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate.
SC 2: MSIV must be closed when there is a main feedwater or main steam line leak and other support systems are inadequate.

Basic Scenario: Operator provides *Close MSIV* command, but MSIV does NOT close

(1) NSSC
   a. Physical damage/failure
   b. Does not recognize operator command
   c. Manufacturing defects
   d. Inadequate algorithm
   e. Loss of power or blackout
(2) PM

a. Wrong priority settings causing PM to ignore the close command
b. Does not recognize PS or manual command
c. Physical damage/failure
d. Multiplex malfunctioning
e. An operation (for example checking status of MSIV actuators) takes much longer time than expected/required, and PM ignores new commands
f. Two conflicting commands come at the same or nearly the same time, from different controllers: the first one with lower priority than the second one.
g. PM previously received interlock command from PS or other controller (e.g. to prevent MSIV closure during startup), causing PM to ignore operator commands to close MSIV
h. Conflicting commands are sent (operator/PS, PS/DAS, etc.)
i. Manufacturing defects
j. Loss of power or blackout

(3) MSIV Sensor
a. Reports device operational when it is not (therefore close command cannot be followed)
b. Reports valve position as open when it is not (therefore close command was sent but cannot be followed)
c. Physical damage/failure
d. Manufacturing defects
e. Loss of power or blackout

(4) MSIV Actuator
a. In the case of unavailability of the oil pump (lack of power supply) if the MSIV is already open, then it automatically remains open for a certain period of time.
b. Mechanical failure in the dump valves, preventing the oil from coming to the tank.
c. Debris prevents the valve to be closed, making it to remain partially or completely open
d. The nitrogen pressure, in the upper chamber, is not enough to close the valve, which had not been reported accordingly
e. Upper chamber is under maintenance to restore pressure
f. Dump valves do not open due to mechanical failures
g. Physical damage/failure
h. Manufacturing defects
i. Loss of power or blackout

(5) MSIV
a. The pressure in the lower chamber does not drop
b. The gate of the valve get stuck and does not move
c. Upper has very low pressure that creates a vacuum preventing the piston from moving
d. The upper chamber pressure is not enough to push the piston
e. Debris inside the valve prevent it from closing completely or partially
f. Physical damage/failure
g. Manufacturing defects

Safety Constraints 3-6:

SC 3: MSIV must not be closed when there is a SGTR and support systems are inadequate

SC 4: MSIV must not be closed too early while SG pressure is too high

SC 5: MSIV must not be closed too late after rupture/leak (in the SG tube, main feedwater, or main steam line)

SC 6: MSIV must not be closed when there is no rupture/leak

Basic Scenario: Operator does not provide *Close MSIV* command, but MSIV closes

(1) NSSC
   a. Physical damage/failure
   b. Some error in NSSC algorithm[10]
   c. NSSC has manufacturing defect
   d. Manufacturing defects
   e. Loss of power or blackout
   f. Inadequate algorithm

(2) PM
   a. PM holds execution of command requests due to interlock issued by PS. This causes delaying a new command
   b. Wrong priority settings (e.g. causing valve to close too late or too early)
   c. Does not recognize PS or manual command
   d. Physical damage/failure
   e. Multiplex malfunctioning
   f. Conflicting commands are sent (operator/PS, PS/DAS, etc.)[11]
   g. Manufacturing defects
   h. Loss of power or blackout

(3) MSIV Sensor
   a. Reports device not operational when it is (therefore PM does not forward close command)
   b. Shows valve position as closed when it is open or only partially closed (therefore PM does not forward close command)
   c. Physical damage/failure
   d. Manufacturing defects

(4) MSIV Actuator
   a. The oil pump may have mechanical problems which causes the valve to automatically be kept open, causing delay
   b. The pilots are de-energized (two pilots in series), then the dump valve opens which closes the valve too early
   c. Mechanical failure in the dump valve
   d. Mechanical failure dumps the hydraulic oil from lower chamber and closes valve
   e. Test of closure causes it to be inadvertently closed
   f. Physical damage/failure
   g. Manufacturing defects
   h. Loss of power or blackout

(5) MSIV
   a. Leakage in the upper chamber makes pressure to be not enough to close the valve at the right time, hence delay

[10] As the Operator has to follow a procedure to disable the NSSC automated control to enable manual control, it could happen that the NSSC, through some programming error, starts a control action after it is disabled, at the same time it is disabled, or starts a control action that it never received for some other reason.

[11] Conflicting commands may be sent, for example and operator command sent at the same time as a PS command, causing PM to lock up or execute the wrong command. There may also be problems due to DAS activation after previous PS commands, or other commands sent before PM has finished executing them. Some commands may be ignored because PM ignores all commands until the current command is finished executing, even if it takes a fraction of a second.

b. A mismatch between the necessary pressure, in the oil chamber, to keep the valve open and the actual pressure applied, may cause that the oil pressure is not enough to keep it open causing it to close. Project mistake or assemblage mistake.
c. A mismatch between the minimum pressure in the nitrogen chamber necessary to close the valve may cause that the pressure applied is higher than the necessary and this may cause the valve to be closed. Project mistake or an assemblage mistake.
d. Physical damage/failure
e. Manufacturing defects

3.7.2 DAS Causal Factors

Causal Factors Leading to DAS Unsafe Control Actions

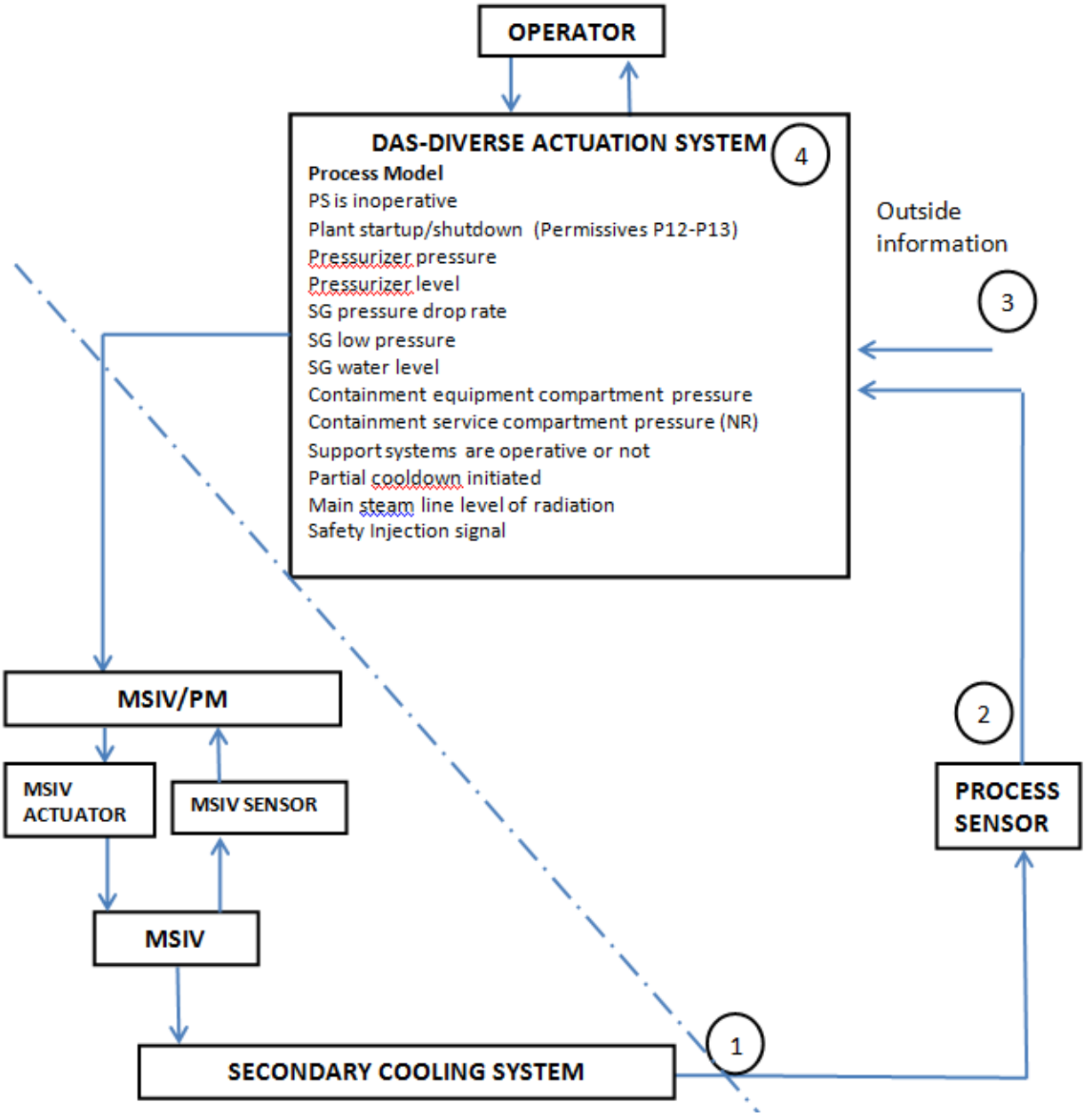

Figure 12: Causal factors Leading to DAS Unsafe Control Actions

UCA 1: Close MSIV not provided when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate

(1) Secondary cooling system (CVCS or emergency feedwater system)
   a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrently with SGTR, and the SG water level may stay practically stable.
   b. Event progresses too slowly to detect
   c. Actuation of CVCS could make up for loss of coolant inventory making DAS delay actuation.

(2) Process Feedback
   a. SG level feedback missing, delayed, or incorrect
   b. SG Pressure, or setpoints, not correct
   c. Steam generator water level delayed
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not work properly and gives wrong measures
   g. No indication of partial cool down initiated
   h. Sensor failure

(3) Outside information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates PZR level is normal
   d. No indication of SI initiated
   e. Delayed indication of SI initiated
   f. Permissives wrongly in effect[12]
   g. Wrong combination of indicators from the 4 divisions

(4) DAS- Diverse Actuation System
   a. DAS does not recognize Steam Generator as ruptured when it is ruptured
   b. DAS does not recognize the main steam line has a leak
   c. DAS does not recognize the main feedwater has a leak
   d. DAS does not recognize that PS is malfunctioning or non-operational and does not take control
   e. DAS has no power supplied
   f. DAS follows incorrect algorithm
   g. DAS has wrong process model
   h. Physical damage/failure
   i. Manufacturing defects
   j. Loss of power or blackout

UCA 2: Close MSIV not provided when there is a main feedwater or main steam line leak and other support systems are inadequate

[12] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong

(1) Secondary cooling system (CVCS or emergency feedwater system)
    a. A concurrent situation could mask another.
    b. Event progresses too slowly to detect
    c. Actuation of CVCS could make up for loss of coolant inventory making DAS delay actuation.
(2) Process Feedback
    a. SG level feedback missing, delayed, or incorrect
    b. SG Pressure, or setpoints, not correct
    c. Steam generator water level delayed
    d. Conflicting data indicating a false situation
    e. Voting system does not work properly and gives wrong measures
    f. No indication of partial cool down initiated
    g. Sensor failure
(3) Outside information
    a. PZR pressure delayed
    b. PZR feedback missing
    c. False feedback indicates PZR level is normal
    d. No indication of SI initiated
    e. Delayed indication of SI initiated
    f. Permissives wrongly in effect[13]
    g. Wrong combination of indicators from the 4 divisions
(4) DAS- Diverse Actuation System
    a. DAS does not recognize the main steam line has a leak
    b. DAS does not recognize the main feedwater has a leak
    c. DAS incorrectly believes problem is SGTR when there is actually a main steam line or main feedwater leak
    d. DAS does not recognize that PS is malfunctioning or non-operational and does not take control
    e. DAS has no power supplied
    f. DAS follows incorrect algorithm
    g. DAS has wrong process model
    h. Physical damage/failure
    i. Manufacturing defects
    j. Loss of power or blackout

UCA 3: Close MSIV provided when there is a SGTR but support systems are inadequate

(1) Secondary cooling system
    a. A concurrent situation could mask another and other support systems could appear adequate but may not be. For example, suppose main steam line high radioactivity is detected

[13] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong.

coincident with safety injection. This may make the controller assume that a partial cooldown was initiated when it may not have. Closing the MSIV would cause the SG pressure to rise in this case.

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure not correct
   c. Steam generator water level not correct
   d. Conflicting data indicating a false situation
   e. Voting system does not work properly and gives wrong measures
   f. Sensor failure

(3) Outside information
   a. Wrong combination of indicators from the 4 divisions
   b. PZR pressure delayed or missing
   c. False signal SI initiated

(4) DAS - Diverse Actuation System
   a. DAS does not recognize that the support systems are not working due to conflicting information
   b. DAS incorrectly believes problem is main steam line leak or feedwater leak when it is actually SGTR
   c. DAS has an inadequate algorithm
   d. DAS close valve while other SG valves are under maintenance or by mistake
   e. Physical damage/failure
   f. Manufacturing defects

UCA 4: Close MSIV provided too early (while SG pressure is high)

(1) Secondary cooling system
   a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrent with a SGTR, and the SG water level stay practically stable.
   b. Event progress too slowly to detect
   c. Actuation of CVCS could make up for loss of coolant inventory making DAS delay actuation.

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure, or setpoint, is not correct
   c. Steam generator water level delayed
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not work properly and gives wrong measures
   g. Sensor failure

(3) Outside Information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates PZR level is normal
   d. No indication of SI initiated
   e. No indication of partial cool down initiated

f. Permissives wrongly in effect[14]
g. Wrong combination of indicators from the 4 divisions

(4) DAS - Diverse Actuation System
a. DAS has conflicting information indicating it is already safe to initiate action after indications confirm rupture/leak
b. Physical damage/failure
c. Manufacturing defects
d. DAS has an inadequate algorithm
e. DAS has wrong process model

UCA 5: Close MSIV command provided too late after rupture/leak (in the SG tube, main feedwater, or main steam line)

(1) Secondary cooling system
a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrently with a SGTR such that the SG water level stays practically stable.
b. Event progress too slowly to detect
c. Actuation of CVCS could make up for loss of coolant inventory making DAS delay actuation.

(2) Process Feedback
a. SG level feedback not provided
b. SG Pressure, or setpoint, is not correct
c. Steam generator water level delayed
d. Main steam line activity not correctly indicated
e. Conflicting data indicating a false situation
f. Voting system does not work properly and gives wrong measures
g. Sensor failure

(3) Outside Information
a. PZR pressure delayed
b. PZR feedback missing
c. False feedback indicates PZR level is normal
d. No indication of SI initiated
e. No indication of partial cool down initiated
f. Permissives wrongly in effect
g. Wrong combination of indicators from the 4 divisions

(4) DAS - Diverse Actuation System
a. DAS does not recognizes the real situation until it is too late after SGTR
b. DAS does not recognizes the real situation until it is too late after the main steam line leak
c. DAS does not recognizes the real situation until it is too late after the main feedwater leak
d. DAS has an inadequate algorithm
e. DAS has wrong process model
f. Physical damage/failure
g. Manufacturing defects
h. Loss of power or blackout

[14] This could occur, for example, in a situation where the water level at the SG is low concurrent with a SG low pressure, which could be due to an open Relief Valve.

UCA 6: Close MSIV provided when there is no rupture/leak

(1) Secondary cooling system
   a. Feedwater pumps not working properly
   b. Condenser leaking (loosing water)
   c. Too much sludge in water (blocking water)
   d. Object in water that could cut flux to SG
   e. Spurious opening of relief valves

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure low (setpoints not correct)
   c. Steam generator water level delayed
   d. False SG isolation signal [15]
   e. Main steam line activity (false positive signal)
   f. Conflicting data indicating a false situation where close valve would be needed
   g. Voting system does not work properly and gives wrong measures
   h. Sensor failure

(3) Outside Information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False PZR pressure
   d. False feedback shows PZR level is low
   e. False signal of initiation of SI
   f. False partial cool down initiated signal
   g. Startup/shutdown not recognized [16]
   h. Wrong combination of indicators from the 4 divisions

(4) DAS - Diverse Actuation System
   a. DAS has wrong information indicating Steam Generator tubes are ruptured when they are not
   b. DAS has wrong information indicating that main steam line or main feedwater has leak when there is no leak
   c. DAS has wrong process model
   d. DAS has an inadequate algorithm
   e. Physical damage/failure
   f. Manufacturing defects
   g. Loss of power or blackout

[15] This could occur, for example, in a situation where the water level at the SG is low concurrent with a SG low pressure, which could be due to an open Relief Valve.

[16] One of the causes for wrong command can be confusion about indicators. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment. Or, SG low level plus permissive 13 (startup) indicates no need to isolate the SG. It could happen that there would be a problem with the sensors, or the model (inside the controller) could be wrong, or algorithm could be wrong. “Confusion" could mean the model is not clear, or that there is an overlap of values.

Causal Factors Leading to DAS Control Actions Not Being Followed

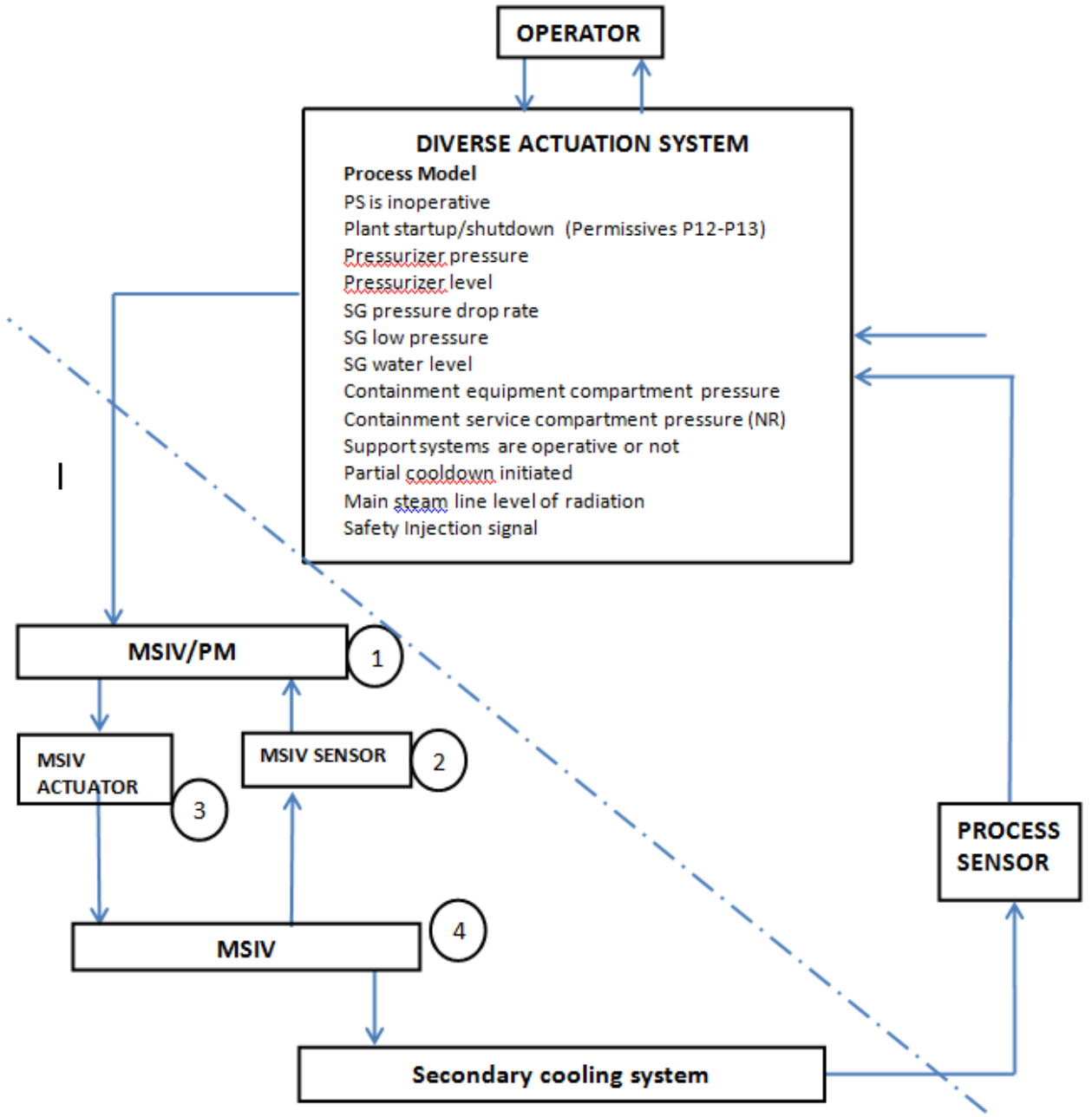

Figure 13: Causal factors leading to DAS control actions not being followed

SC 1: MSIV must be closed when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate.
SC 2: MSIV must be closed when there is a main feedwater or main steam line leak and other support systems are inadequate.

Basic Scenario: DAS provides *Close MSIV* command, but MSIV does NOT close

(1) Priority Module
    a. Wrong priority settings causing PM to ignore the close command
    b. Does not recognize DAS command
    c. Physical damage/failure
    d. Multiplex malfunctioning
    e. Some operation (for example checking status of MSIV actuators) takes much longer time than supposed to, and PM ignores new commands
    f. Two conflicting action commands come at the same or nearly the same time, from different controllers: the first one with lower priority than the second one.
    g. PM had received a interlock command from PS, but PS goes down right after, so PM keeps waiting for new commands and does not accept new commands.
    h. Conflicting commands are sent (operator/PS, PS/DAS, etc.)
    i. Manufacturing defects
    j. Loss of power or blackout
(2) MSIV Sensor
    a. Reports device operational when it is not (therefore close command cannot be followed)
    b. Reports valve position as open when it is not (therefore close command was sent but cannot be followed)
(3) MSIV Actuator
    a. In the case of unavailability of the oil pump (lack of power supply) if the MSIV is already open, then it automatically remains open for a certain period of time.
    b. Mechanical failure in the dump valves, preventing the oil from coming to the tank.
    c. Debris prevents the valve to be closed, making it to remain partially or completely open
    d. The nitrogen pressure, in the upper chamber, is not enough to close the valve, which had not been reported accordingly
    e. Upper chamber is under maintenance to restore pressure
    f. Dump valves do not open due to mechanical failures
    g. Physical damage/failure
    h. Manufacturing defects
    i. Loss of power or blackout
(4) MSIV Valve
    a. Leakage in the upper chamber makes pressure to be not enough to close the valve at the right time, hence delay
    b. A mismatch between the necessary pressure, in the oil chamber, to keep the valve open and the actual pressure applied, may cause that the oil pressure is not enough to keep it open causing it to close. Project mistake or assemblage mistake.
    c. A mismatch between the minimum pressure in the nitrogen chamber necessary to close the valve may cause that the pressure applied is higher than the necessary and this may cause the valve to be closed. Project mistake or an assemblage mistake.
    d. Physical damage/failure
    e. Manufacturing defects

Safety Constraints 3-6:
SC 3: MSIV must not be closed when there is a SGTR and support systems are inadequate
SC 4: MSIV must not be closed too early while SG pressure is too high
SC 5: MSIV must not be closed too late after rupture/leak (in the SG tube, main feedwater, or main steam line)
SC 6: MSIV must not be closed when there is no rupture/leak

Basic Scenario: DAS does not provide *Close MSIV* command, but MSIV closes

(1) Priority Module
   a. PM holds execution of command requests due to interlock issued by PS. This causes delaying a new command
   b. PM receives close command from another cotnroller
   c. Wrong priority settings
   d. Does not recognize PS or manual command
   e. Physical damage/failure
   f. Multiplex malfunctioning
   g. Conflicting commands are sent (operator/PS, PS/DAS, etc.)[17]
   h. Physical damage/failure
   i. Manufacturing defects
   j. Loss of power or blackout

(2) MSIV Sensor
   a. Reports device not operational when it is (therefore PM does not forward close command)
   b. Shows valve position as closed when it is open or only partially closed (therefore PM does not forward close command)
   c. Physical damage/failure
   d. Manufacturing defects

(3) MSIV Actuator
   a. The oil pump may have mechanical problems which causes the valve to automatically be kept open, causing delay
   b. The pilots are de-energized (two pilots in series), then the dump valve opens which closes the valve too early
   c. Mechanical failure in the dump valve
   d. Mechanical failure dumps the hydraulic oil from lower chamber and closes valve
   e. Test of closure causes it to be inadvertently closed
   f. Physical damage/failure
   g. Manufacturing defects
   h. Loss of power or blackout

(4) MSIV Valve
   a. Leakage in the upper chamber makes pressure to be not enough to close the valve at the right time, hence delay

[17] Conflicting commands may be sent, for example and operator command sent at the same time as a PS command, causing PM to lock up or execute the wrong command. There may also be problems due to DAS activation after previous PS commands, or other commands sent before PM has finished executing them. Some commands may be ignored because PM ignores all commands until the current command is finished executing, even if it takes a fraction of a second.

b. A mismatch between the necessary pressure, in the oil chamber, to keep the valve open and the actual pressure applied, may cause that the oil pressure is not enough to keep it open causing it to close. Project mistake or assemblage mistake.
c. A mismatch between the minimum pressure in the nitrogen chamber necessary to close the valve may cause that the pressure applied is higher than the necessary and this may cause the valve to be closed. Project mistake or an assemblage mistake.
d. Physical damage/failure
e. Manufacturing defects

3.7.3 PS Causal Factors

Causal Factors Leading to PS Unsafe Control Actions

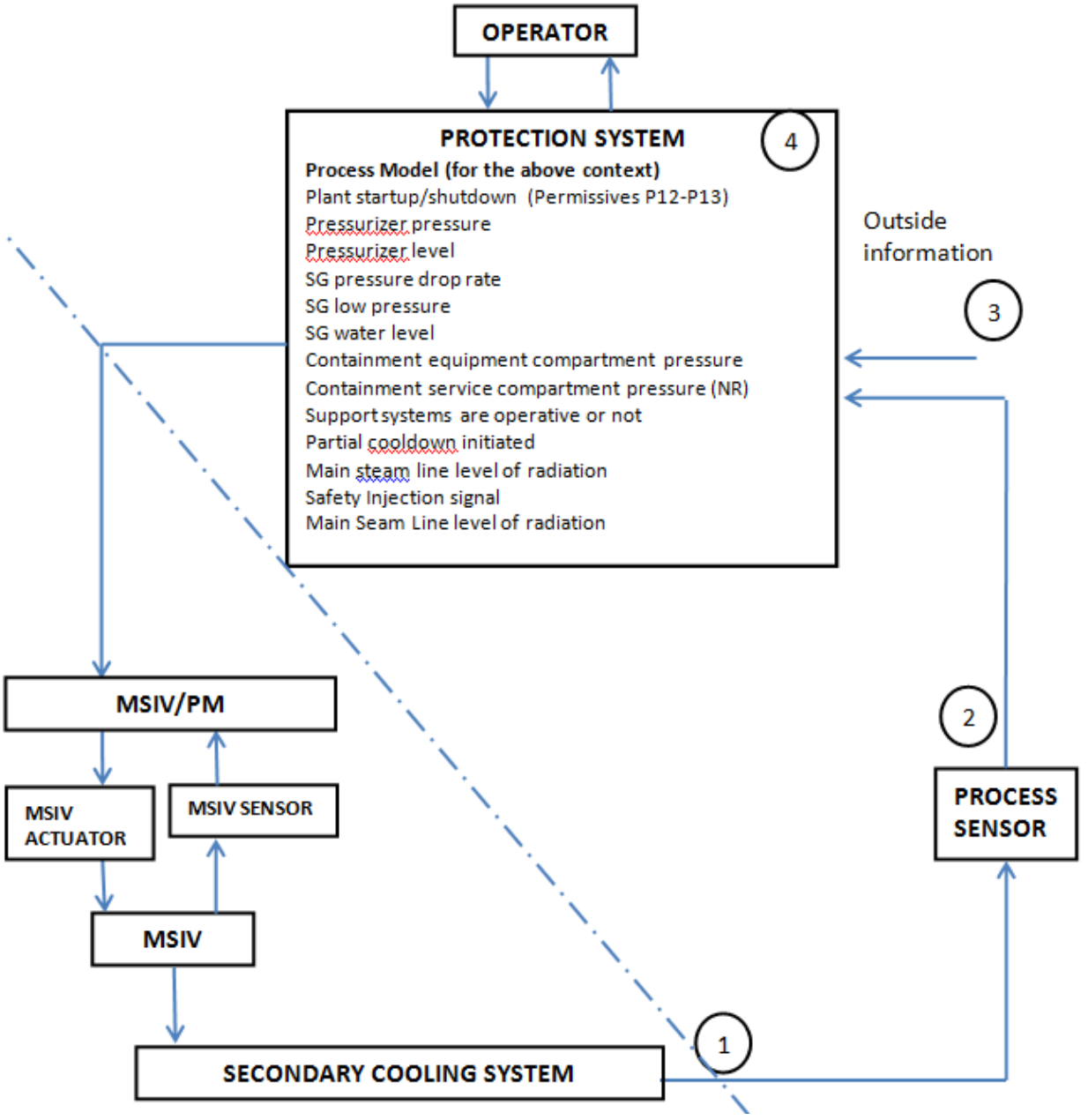

Figure 14: Causal Factors for PS Unsafe Control Actions

UCA 1: Close MSIV not provided when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate

(1) Secondary cooling system (CVCS or emergency feedwater system)
   a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrently with a SGTR, and the SG water level may stay practically stable.
   b. Event progress too slowly to detect
   c. Actuation of CVCS could make up for loss of coolant inventory making PS delay actuation.

(2) Process Feedback
   a. SG level feedback missing, delayed, or incorrect
   b. SG Pressure, or setpoints, is not correct
   c. Steam generator water level delayed
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not work properly and gives wrong measures
   g. No indication of partial cool down initiated
   h. Sensor failure

(3) Outside information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates` PZR level is normal
   d. No indication of SI initiated
   e. Delayed indication of SI initiated
   f. Permissives wrongly in effect[18]
   g. Wrong combination of indicators from the 4 divisions

(4) PS-Protection System
   a. PS does not recognize Steam Generator is ruptured
   b. PS does not recognize main steam line has a leak
   c. PS does not recognize the main feedwater has a leak
   d. PS has no power supply
   e. PS follows inadequate algorithm
   f. PS has a manufacturing defect
   g. Physical damage/failure
   h. Loss of power or blackout
   i. PS has wrong process model

UCA 2: Close MSIV not provided when there is a main feedwater or main steam line leak and other support systems are inadequate

(1) Secondary cooling system (CVCS or emergency feedwater system)
   a. A concurrent situation could mask another
   b. Event progress too slowly to detect

[18] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong.

c. Actuation of CVCS could make up for loss of coolant inventory making PS delay actuation.

(2) Process Feedback
   a. SG level feedback missing, delayed, or incorrect
   b. SG Pressure, or setpoints, is not correct
   c. Steam generator water level delayed
   d. Conflicting data indicating a false situation
   e. Voting system does not work properly and gives wrong measures
   f. No indication of partial cool down initiated
   g. Sensor failure

(3) Outside information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates` PZR level is normal
   d. No indication of SI initiated
   e. Delayed indication of SI initiated
   f. Permissives wrongly in effect[19]
   g. Wrong combination of indicators from the 4 divisions

(4) PS-Protection System
   a. PS does not recognize main steam line has a leak
   b. PS does not recognize the main feedwater has a leak
   c. PS believes there is an SGTR when there is actually a main steam line or feedwater leak
   d. PS has no power supply
   e. PS follows inadequate algorithm
   f. PS has wrong process model
   g. PS has a manufacturing defect
   h. Physical damage/failure
   i. Loss of power or blackout

UCA 3: Close MSIV provided when there is a SGTR but support systems are inadequate

(1) Secondary cooling system
   a. A concurrent situation could mask another and other support systems could appear adequate but may not be. For example, suppose main steam line high radioactivity is detected coincident with safety injection. This may make the controller assume that a partial cooldown was initiated when it may not have. Closing the MSIV would cause the SG pressure to rise in this case.

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure not correct
   c. Steam generator water level not correct
   d. Conflicting data indicating a false situation

[19] One of the causes for wrong command can be confusion about indicators. “Confusion" could mean the model is not clear, there is an overlap of responsibilities, or conflicting process values are indicated. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment and low SG water level. However, SG low level together with permissive 13 (startup) may indicate there is no need to isolate the SG. It could happen that there is a problem with the sensors, the model (inside the controller) could be wrong, or the algorithm could be wrong.

e. Voting system does not work properly and gives wrong measures
f. Sensor failure

(3) Outside information
a. Wrong combination of indicators from the 4 divisions
b. PZR pressure delayed or missing
c. False signal SI initiated

(4) PS-Protection System
a. PS does not recognize that the support systems are not working due to conflicting information
b. PS believes there is a main steam line or feedwater leak when there is actually an SGTR
c. PS has an inadequate algorithm
d. PS has wrong process model
e. PS close valve while other SG valves are under maintenance or by mistake
f. PS has a manufacturing defect
g. Physical damage/failure
h. Manufacturing defects
i. Loss of power or blackout

UCA 4: Close MSIV provided too early (while SG pressure is high)

(1) Secondary cooling system
a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrent with a SGTR, and the SG water level stay practically stable.
b. Event progresses too slowly to detect
c. Actuation of CVCS could make up for loss of coolant inventory delaying PS actuation.

(2) Process Feedback
a. SG level feedback not provided
b. SG Pressure, or setpoints, not correct
c. Steam generator water level delayed
d. Main steam line activity not correctly indicated
e. Conflicting data indicating a false situation
f. Voting system does not work properly and gives wrong measures
g. Sensor failure

(3) Outside Information
a. PZR pressure delayed
b. PZR feedback missing
c. False feedback indicates PZR level is normal
d. No indication of SI initiated
e. No indication of partial cool down initiated
f. Permissives wrongly in effect *
g. Wrong combination of indicators from the 4 divisions

(4) PS-Protection System
a. PS has an inadequate algorithm
b. PS has conflicting information indicating it is already safe to initiate action after indications confirm rupture/leak
c. Physical damage/failure
d. Manufacturing defects
e. Loss of power or blackout

f. PS has wrong process model

UCA 5: Close MSIV provided too late after rupture/leak (in the SG tube, main feedwater, or main steam line)

(1) Secondary cooling system
   a. A concurrent situation could mask another. For example, a feedwater problem could happen concurrently with a SGTR such that the SG water level stays practically stable.
   b. Event progress too slowly to detect
   c. Actuation of CVCS could make up for loss of coolant inventory making PS delay actuation.

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure, or setpoints, is not correct
   c. Steam generator water level delayed
   d. Main steam line activity not correctly indicated
   e. Conflicting data indicating a false situation
   f. Voting system does not work properly and gives wrong measures
   g. Sensor failure

(3) Outside Information
   a. PZR pressure delayed
   b. PZR feedback missing
   c. False feedback indicates PZR level is normal
   d. No indication of SI initiated
   e. No indication of partial cool down initiated
   f. Permissives wrongly in effect
   g. Wrong combination of indicators from the 4 divisions

(4) PS-Protection System
   a. PS does not recognize the real situation until it is too late after SGTR
   b. PS does not recognize the real situation until it is too late after the main steam line or feedwater leak
   c. PS has an inadequate algorithm
   d. PS has wrong process model
   e. PS has a manufacture defect
   f. Physical damage/failure
   g. Loss of power or blackout

UCA 6: Close MSIV provided when there is no rupture/leak

(1) Secondary cooling system
   a. Feedwater pumps not working properly
   b. Condenser leaking (loosing water)
   c. Too much sludge in water (blocking water)
   d. Object in water that could cut flux to SG
   e. Spurious opening of relief valves

(2) Process Feedback
   a. SG level feedback not provided
   b. SG Pressure low (setpoints not correct)

c. Steam generator water level delayed
d. False SG isolation signal[20]
e. Main steam line activity (false positive signal)
f. Conflicting data indicating a false situation where close valve would be needed
g. Voting system does not work properly and gives wrong measures
h. Sensor Failure

(3) Outside Information

a. PZR pressure delayed
b. PZR feedback missing
c. False PZR pressure
d. False feedback indicates PZR level is low
e. False signal of initiation of SI
f. False Partial cool down initiated signal
g. Startup/shutdown not recognized [21]
h. Wrong combination of indicators from the 4 divisions

(4) PS-Protection System

a. PS has wrong information indicating Steam Generator tubes are ruptured when they are not
b. PS has wrong information indicating that main steam line or feedwater has a leak they do not
c. PS has wrong process model
d. PS has an inadequate algorithm
e. PS has a manufacture defect
f. Physical damage/failure
g. Loss of power or blackout

[20] This could occur, for example, in a situation where the water level at the SG is low concurrent with a SG low pressure, which could be due to an open Relief Valve.

[21] One of the causes for wrong command can be confusion about indicators. The controllers check several indicators to decide what the specific problem is. For example, the main steam pipe break would also cause high pressure in the main steam line compartment. Or, SG low level together with permissive 13 (startup)indicates no need to isolate the SG. It could happen that there would be a problem with the sensors, or the model (inside the controller) could be wrong, or algorithm could be wrong. “Confusion" could mean the model is not clear, or that there is an overlap of values.

Causal Factors Leading to PS Control Actions Not Being Followed

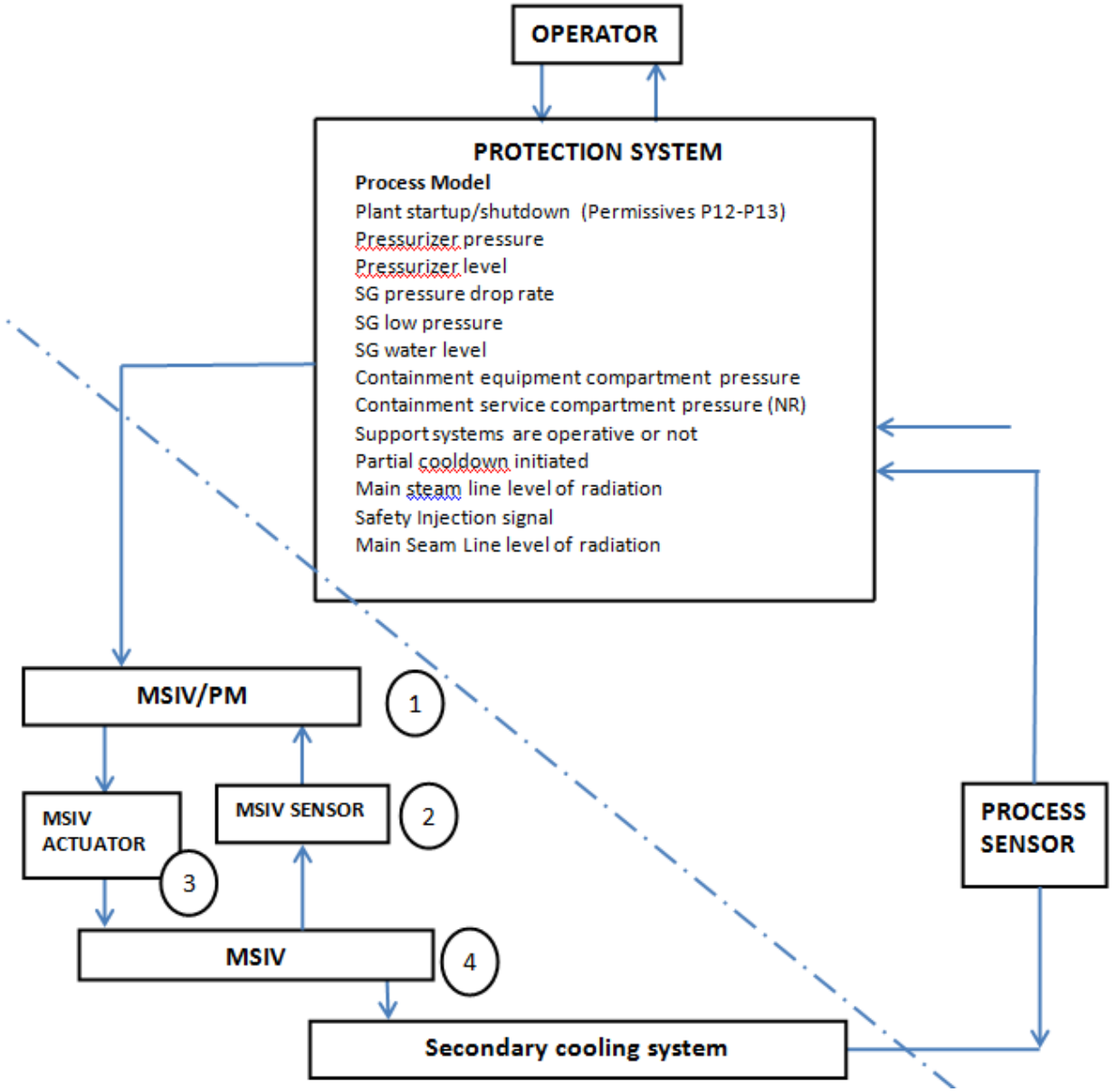

Figure 15: Causal factors leading to PS control actions not being followed

SC 1: MSIV must be closed when there is a leak (rupture in the SG tube, leak in main feedwater, or leak in main steam line) and the support systems are adequate.
SC 2: MSIV must be closed when there is a main feedwater or main steam line leak and other support systems are inadequate.

Basic Scenario: PS provides *Close MSIV* command, but MSIV does NOT close

(1) Priority Module
   a. Wrong priority settings causing PM to ignore the close command
   b. Does not recognize PS command
   c. Physical damage/failure
   d. Multiplex malfunctioning
   e. An operation (for example checking status of MSIV actuators) takes longer time than expected/required, and PM ignores new commands
   f. Two conflicting action commands come at the same or nearly the same time, from different controllers: the first one with lower priority than the second one.
   g. PM had received a interlock command from PS, which is not removed so PM does not accept new commands.
   h. Conflicting commands are sent (operator/PS, PS/DAS, etc.)
   i. Manufacturing defects
   j. Loss of power or blackout

(2) MSIV Sensor
   a. Reports device operational when it is not (therefore close command cannot be followed)
   b. Reports valve position as open when it is not (therefore close command was sent but cannot be followed)
   c. Physical damage/failure
   d. Manufacturing defects
   e. Loss of power or blackout

(3) MSIV Actuator
   a. In the case of unavailability of the oil pump (lack of power supply) if the MSIV is already open, then it automatically remains open for a certain period of time.
   b. Mechanical failure in the dump valves, preventing the oil from coming to the tank.
   c. Debris prevents the valve to be closed, making it to remain partially or completely open
   d. The nitrogen pressure, in the upper chamber, is not enough to close the valve, which had not been reported accordingly
   e. Upper chamber is under maintenance to restore pressure
   f. Dump valves do not open due to mechanical failures
   g. Physical damage/failure
   h. Manufacturing defects
   i. Loss of power or blackout

(4) MSIV Valve
   a. Leakage in the upper chamber makes pressure to be not enough to close the valve at the right time, hence delay
   b. A mismatch between the necessary pressure, in the oil chamber, to keep the valve open and the actual pressure applied, may cause that the oil pressure is not enough to keep it open causing it to close. Project mistake or assemblage mistake.

c. A mismatch between the minimum pressure in the nitrogen chamber necessary to close the valve may cause that the pressure applied is higher than the necessary and this may cause the valve to be closed. Project mistake or an assemblage mistake.
d. Physical damage/failure
e. Manufacturing defects

Safety Constraints 3-6:
SC 3: MSIV must not be closed when there is a SGTR and support systems are inadequate
SC 4: MSIV must not be closed too early while SG pressure is too high
SC 5: MSIV must not be closed too late after rupture/leak (in the SG tube, main feedwater, or main steam line)
SC 6: MSIV must not be closed when there is no rupture/leak

Basic Scenario: PS does not provide *Close MSIV* command, but MSIV closes

(1) Priority Module
   a. PM holds execution of command requests due to interlock issued by PS. This causes delaying a new command
   b. Wrong priority settings
   c. Does not recognize PS or manual command
   d. Physical damage/failure
   e. Multiplex malfunctioning
   f. Conflicting commands are sent (operator/PS, PS/DAS, etc.)[22]
   g. Manufacturing defects
   h. Loss of power or blackout
(2) MSIV Sensor
   a. Reports device not operational when it is (therefore PM does not forward close command)
   b. Shows valve position as closed when it is open or only partially closed (therefore PM does not forward close command)
   c. Physical damage/failure
   d. Manufacturing defects
   e. Loss of power or blackout
(3) MSIV Actuator
   a. The oil pump may have mechanical problems which causes the valve to automatically be kept open, causing delay
   b. The pilots are de-energized (two pilots in series), then the dump valve opens which closes the valve too early
   c. Mechanical failure in the dump valve
   d. Mechanical failure dumps the hydraulic oil from lower chamber and closes valve
   e. Test of closure causes it to be inadvertently closed
   f. Physical damage/failure
   g. Manufacturing defects

[22] Conflicting commands may be sent, for example and operator command sent at the same time as a PS command, causing PM to lock up or execute the wrong command. There may also be problems due to DAS activation after previous PS commands, or other commands sent before PM has finished executing them. Some commands may be ignored because PM ignores all commands until the current command is finished executing, even if it takes a fraction of a second.

h. Loss of power or blackout

(4) MSIV Valve

a. Leakage in the upper chamber makes pressure to be not enough to close the valve at the right time, hence delay
b. A mismatch between the necessary pressure, in the oil chamber, to keep the valve open and the actual pressure applied, may cause that the oil pressure is not enough to keep it open causing it to close. Project mistake or assemblage mistake.
c. A mismatch between the minimum pressure in the nitrogen chamber necessary to close the valve may cause that the pressure applied is higher than the necessary and this may cause the valve to be closed. Project mistake or an assemblage mistake.
d. Physical damage/failure
e. Manufacturing defects

3.8 Extension to Multiple Steam Generators

Thus far, the analysis has considered a single Steam Generator and a single MSIV. However, the results can be extended to multiple Steam Generators without repeating the entire analysis. One approach is to revise the existing context tables to reflect the control action "Close MSIV #1". Because any feedwater or steamline leak concerning SG #1 will affect the control action "Close MSIV #1" in a similar way as for the single SG system, these columns can remain the same. Similarly, a Steam Generator Tube Rupture in SG #1 is relevant to the closure of MSIV #1, however a Steam Generator Tube Rupture in other Steam Generators does not affect closure of MSIV #1. Therefore, the values in the column Steam Generator Tube Rupture could be replaced with "SG #1 ruptured" and "SG #1 not ruptured", while keeping the rest of the table the same. Similarly, the resulting table can then be converted for the other three MSIV commands by simply replacing #1 with #2, #3, or #4. If each redundant SG can compensate for the heat exchange performed by another SG then the definition of"other support systems" in both tables can be extended to include the other SGs.

.

3.9 Limitations of this Analysis

This report does not contain a detailed low-level analysis down to the individual components such as PLDs inside PM. We did not have the time or resources in this small research grant to analyze down to that level, and it was not our goal. STPA is a top-down analysis, and we have performed the analysis from the highest level (accidents and hazards) down to the module level to identify the control flaws that can cause hazards. The potential flaws and safety constraints we found should be the starting point for a more detailed analysis. For example, we found that the system-level design is such that incorrect priority settings for PM could cause a hazard if MSIV close commands are ignored. The next step would be to make sure that never happens. There are many options, including changing the system architecture (may not be practical at this point) or enforcing constraints on lower levels. The latter might be achieved by making the priority settings fixed within PM and not programmable and making sure PM internal logic and PLD design is such that MSIV commands are never ignored regardless of current priority. Other solutions are also possible. Of course, any potential solutions must be checked to ensure other safety constraints are not violated and new hazards are not introduced.

4 Results of the Analysis

Although this study covered only a limited portion of the secondary cooling system, some important insights can be derived from it by examining the causes of unsafe control actions for the assumed scenarios.

An example insight obtained from the analysis is the difficulty of detecting a Steam Generator Tube Rupture (SGTR) through the normal indicators, which can lead to a delayed response by the automated controllers and the operator. The current solution relies on (i.e., gives credit to) the operator's ability to detect and intervene in certain cases. Relying on the operator, however, may not be effective because of other

factors that will influence the operator decision-making process. These factors are identified in STPA Step 2 as possible causes for the operator not to provide the control action to close the MSIV or to provide it too late. The identified factors can be used to improve the design to make the operator error less likely or to mitigate it.

One reasonable recommendation, for example, is for regulators to ask the designers to simplify the indicators for the case of SGTR by making the level of radiation at the Main Steam Line a major indication to isolate the affected SG. This way, the Protection System (PS) would be able to detect the event earlier. In the current design, an indication of radioactivity is not sufficient for the PS to take action, and, as a result, there are additional scenarios in which neither the operator nor the PS may take action. For example, the operator may feel pressed to avoid spurious shutdowns and, as a consequence, he or she may wait longer for stronger evidence of the real problem. This type of response, in fact, is a common one identified by human factors experts in many real accidents. There could also be a situation where, after many years of work, the operator learns to completely rely on the automated controls to handle some incidents and becomes overconfident in its correct operation. This overreliance could lead to non-action or delayed action even though other analyses have assumed he or she will immediately take action in that case.

Part of the problem is the nuclear industry tendency to "credit the operator" (or credit some other device such as the PS), which means that the hazard analysis assumes that the operator (or other component) will detect and resolve the problem appropriately in a given situation. This thought process relates to the problem of only examining the "nominal" case versus identifying and resolving the worst case (as mentioned several times in this report). STAMP provides a more general alternative model that includes more potential paths (scenarios) to losses and can trace operator or other errors into the design to detect design flaws or weaknesses.

It is important to identify the factors under which a component, like the operator, may not act adequately and use those factors to improve the design of the system. The alternative is to simply blame the operators after an accident or incident for any failure to detect and resolve the problem as it was assumed they would. New NPP designs are placing the operators in a highly automated environment and telling them that the PS can handle almost everything. There are many subtle scenarios in which the PS may give up, or worse, ignore the problem without alerting the operator because it is assumed the operator will detect the problem and resolve it. Assuming that A is not safety-critical because B exists as a backup to A and that B is not safety-critical because it is only a backup system leads to circular reasoning and, potentially, accidents. A worst case analysis is necessary that assumes there may be design flaws or common-cause/common-mode failures in both.

The introduction of digital systems exacerbates the problem. Software allows highly complex systems to be created. While identifying safety-critical versus non-safety-critical components in a nuclear power plant was relatively straightforward for primarily electromechanical designs, the extensive use of software allows much more complex designs than previously possible and the potential for unintended and unexpected interactions among components. The more interactions between system components and the more complex the functional design, the more the opportunities for unintended effects and, consequently, the more opportunities for unsafe control actions that can lead to hazards. In other words, the more complex the system, the more possibilities of unintended effects due to the interactions among components. For example, the operator has to manually change settings by manipulating priority logic in order to allow NSSC to process the manual commands. This requirement can be a problem in case of an emergency.

Exhaustive system testing is not possible with software-intensive systems. Even if the individual components can be exhaustively tested, that will not guarantee system safety. The interactions between PM and other controllers and equipment are such that each component may operate in a reasonable manner given the local environment and information available, but from a global systems perspective the combined behavior of multiple components may be unsafe. For example, as discussed above, the PS may not take action in some situations where operator intervention is required while the operator may wait for the automated PS to take action. The STPA analysis in this case study was limited in scope to the MSIV commands and publically available information, but a more detailed STPA analysis seems warranted due to the central importance of this equipment in the control system.

Using a hazard analysis method based on STAMP allows more extensive analysis that includes events in which nothing failed but the hazards arise due to unsafe interactions among components. The identification of weaknesses in the overall PWR design are possible using STPA because the STPA analysis examines the interactions between the various controllers and system components. These weaknesses are unlikely to be found by hazard analysis methods based on assumptions about accidents being caused by chains of component failure events.

These are only some of the flaws or weaknesses in the design that can be identified from the partial system modeling and STPA hazard analysis performed for this research effort. A more complete modeling and analysis effort would most likely uncover even more.

5. Potential Use of STPA in Licensing

STAMP provides a more comprehensive basis for analyzing safety and licensing nuclear power plants. The following sections review several potential advantages.

5.1 Classification of Components as Safety-Related vs. Non-Safety-Related

While identifying safety-critical versus non-safety-critical components in a nuclear power plant was relatively straightforward for primarily electromechanical designs, the extensive use of software allows much more complex designs than previously possible and the potential for unintended and unexpected interactions among components. STPA does not begin with an assumption that certain equipment or controllers are safety-related and non-safety-related. Instead, an important output of STPA is a set of unsafe control actions for every controller analyzed and how they can directly or indirectly affect a hazard. The unsafe control actions identified in Step 1 describe how each controller can contribute to a hazardous situation. The output of STPA, therefore, could be used to classify components as safety-related or non-safety-related or to verify an existing classification. STPA Step 2 goes further and considers how each component—including sensors, actuators, logic devices, and communication paths—can contribute to hazardous situations. Analysts can identify hazardous behavior related to the interactions between components that otherwise would not be captured by traditional analyses

Although there should be independence[23] between safety-related and non-safety-related controllers as classified in the U.S. EPR system, the STPA analysis on the example system in this case study showed that some systems classified as non-safety-related can still contribute to hazardous situations and are not truly independent from safety-related systems and functions. For example, NSSC, which is defined as a non-safety related controller, can hinder or slow down the successful closure of the MSIV when needed by reporting erroneous feedback to the operator or acting in unsafe or unexpected ways upon receiving a close MSIV command from the operator (or a combination of both). In this way, through its interaction with several safety-related controllers, NSSC can affect their ability to perform their safety-related functions. As another example, the safety-related PM contains the non-safety-related communication device Profibus, which communicates with NSSC. Incorrect behavior of NSSC together with Profibus can potentially affect the safety-related functions of PM by potentially directly interfering with the control actions processed by PM. The interference could also be caused indirectly by interfering with the feedback provided to the operator or by providing inadequate or incorrect feedback to the operator. Without appropriate feedback, the operator cannot be assumed to be able to provide safe control actions, including MSIV and other controls.

5.2 Identifying Potential Operator Errors and Their Causes and Safety Culture Flaws

[23] We use "independence" here as used in NUREG-0800: "data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function. … In practical terms, this means that for communications between safety and non-safety systems, the communications must be such that the safety system does not require any non-safety input to perform its safety function, and that any failure of the non-safety system, communications system, or data transmitted by the non-safety system will not prevent or influence that independent safety determination." [NUREG-0800 Appendix 7.1-D].

STAMP/STPA treats the operator as integral part of the system and thus an integral part of the hazard analysis. Factors such as "pressure to save time and money" can be as dangerous as a mechanical failure of a component and can be captured in this method.

5.3 Broadening the Analysis and Oversight

Other aspects of the overall socio-technical system can also be included in the STPA analysis although they were not included in the case study for this report. The NRC has responsibility for overseeing safety culture and other aspects of nuclear power plant operations. The inclusion of social, organizational, and managerial factors in the hazard analysis (which is possible for STPA) can identify potential risks and leading indicators of increasing risk. that the regulators can use to audit performance by the utilities.

5.4 Assisting in Understanding Applicant Functional Designs

The model of the safety control structure constructed as part of the STPA analysis can help regulatory. authorities to improve their understanding of the functional design of the system and to aid in communication and interchanges with applicants. In performing the case study, we found the existing documentation for the system provided a comprehensive description of the physical design, but we had great difficulty extracting the functional or logical design from this documentation. The control structure diagrams can help in providing this information and identifying missing information or ambiguous design descriptions.

The documentation for STPA can also facilitate discussions between experts from different disciplines, which in practice tend to speak different technical languages and have different perspectives and priorities. We have found that simply using a control structure model of the system can help with communication among diverse groups about the functionality provided by the system design.

5.5 Enhancing the Review of Candidate Designs

STAMP/STPA can be used as a platform to provide the authorities with a broader and more systemic view of the system and can uncover unanticipated or unexpected behavior that emerges from the complex interactions that occur. This approach, as mentioned earlier, has the advantage of being able to capture both human and equipment behavior in the same control-theoretic model. Because the system is modeled in an integrated control structure rather than considering components in isolation, authorities will be better able to visualize weaknesses that otherwise would not be possible.

The Step 1 tables can provide a wide range of scenarios that could lead to unsafe control actions related to the identified hazards. These tables consider the possibilities of occurrences without relying on the availability or accuracy of probabilistic estimates, which makes STAMP/STPA a very powerful tool to assist in certification and licensing. Each unsafe control action can be directly and easily translated into component-level safety constraints, which can be compared with the safety requirements of an existing design to identify gaps, inconsistencies, or incompleteness. The Step 2 analysis guides the identification of possible causes of the unsafe control actions as well as other ways the safety constraints can potentially be violated. These results can also be used as a guide for the authorities to generate a list of requirements or mitigation measures that the licensee has to meet. Finally, .the results can also be used as a basis to generate other requirements not yet identified, as there is a possibility that new issues will be raised after experts study the Step 1 and Step 2 results.

Glossary

Credited: A system that can perform a safety function and is qualified and relied upon to do so.
Interlocks: interlock signals used to enable or disable certain protective actions according to current plant conditions (e.g., to ensure high pressure to low pressure system interlocks)
Non-Credited: A system that can perform a safety function, but is not qualified or relied upon to do so.
Permissives: A permissive is a condition to be satisfied based on the information given by a set of sensors. The conditions associated with a permissive indicate the validity of certain protective functions with respect to the operating status of the plant. A validated permissive can enable or disable protective functions. Likewise, an inhibited permissive can enable or disable protective functions. Additionally, a validated or inhibited permissive can directly launch selected actions and enable or disable complete functions.
Protection System: That part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features.
Safety-Related Function: One of the processes or conditions (e.g., emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, postaccident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a DBE.(design basis event)
Safety-Related System: A system that is relied upon to remain functional during and following design events to maintain: (a) the integrity of the reactor coolant pressure boundary (RCPB), (b) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (c) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR 100 guidelines.

Acronyms

AOO - Anticipated Operational Occurrence (AOO)
CVCS - Chemical Volume Control System
DAS - Diverse Actuation System
ECCS - Emergency Core Cooling System
ESF - Engineered Safety Feature
FMEA - Failure Modes and Effects Analysis
NRC - US Nuclear Regulatory Commission
NPP - Nuclear Power Plant
MSIV - Main Steam Isolation Valve
PA - Postulated Accidents
NSSC - Non-Safety System Controller
PM -Priority Module
PLD - Programmable Logic Device
PS - Protection System
PZR - Pressurizer
BMC – Boron and Makeup Control
RCS - Reactor Controls
RCS - Reactor Coolant System
RT - Reactor Trip
SCS - Safety Control System
SC- Safety Constraints
SG - Steam Generator
SGTR - Steam Generator Tube Rupture
SI - Safety Injection
STAMP - System-Theoretic Accident Model and Processes

STPA - System Theoretic Process Analysis
TG I&C – Turbine and Generator Instrumentation and Control
UCA - Unsafe Control Actions
U.S. EPR- U.S. Evolutionary Power Reactor

References

AREVA NP Inc., "U.S. EPR Protection System"; Technical Report ANP-10309NP - Revision 3 - June 2011

Ishimatsu, T., Leveson, N., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H. ``Modeling and Hazard Analysis using STPA," *Int. Association for the Advancement of Space Safety*, Huntsville, May 2010.

Joyce J., Software Safety for Air Traffic Management Systems, 21rst Digital Avionics Systems Conference, October 2002, IEEE Proceedings

Knight, J. C. and Leveson, N. G. "An experimental evaluation of the assumption of independence in multiversion programming". IEEE Transactions on Software Engineering, vol. 12, no. 1, Jan. 1986, 96-109.

Knight, J. C. and Leveson, N. G. "A reply to the criticisms of the Knight & Leveson experiment.", SIGSOFT Software Engineering Notes, vol. 15, no. 1, Jan. 1990, 24-35.

Leveson N., *Safeware*, Reading, MA: Addison-Wesley, 1995.

Leveson, N.G. ``The Role of Software in Spacecraft Accidents," AIAA (American Institute of Aeronautics and Astronautics) *Journal of Spacecraft and Rockets*, vol 41, no. 4, July 2004.

Leveson N., *Engineering a Safer World*, MIT Press, 2012.

National Academies Press, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety and National Research Council, Digital Instrumentation & Control Systems in Nuclear Power Plants: Safety and Reliability Issues, 1997. URL: http://www.nap.edu/catalog.php?record_id=5432

NEI, "USA's first fully digital station", January 21, 2011.

NRC, "Diversity and Defense in Depth in Digital Instrumentation and Controls", 2010, http://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/diversity-defense.html.

NRC, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems", NUREG/CR-7007 (ORNL/TM-2009/302), 2009

NRC Advisory Committee on Reactor Safeguards, Proceedings of the digital Instrumentation and Control Systems Subcommittee Meeting, March 2008, Rockville Maryland.

NRC, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing", Volumes 1 and 2 (NUREG-1860), December 2007

NRC, "Standard Review Plan (SRP) For The Review of Safety Analysis Reports for Nuclear Plants", NUREG-0800, March 2007

NRC, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", Reg. Guide 1.152 rev. 2, January 2006

Pereira S., Lee G., Howard J., "A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System," *American Institute of Aeronautics and Astronautics (AIAA) Missile Sciences Conference*, Monterey, CA, November 2006.