MARY KAY O'CONNOR
PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

On Model-Based Systems Engineering for Design, Management, and Governance of Protective Systems

Antonio Arreola-Risa, Diana Gallart Hamilton*,
M. Sam Mannan, Paul Nelson, Martin A. Wortman
Texas A&M University
College Station, Texas 77843-4113.
Tecnológico de Monterrey Campus Estado de México, México.
*Presenters' E-mails: dgallart@tamu.edu, dgallart@tec.mx

Abstract

Protective systems failure can be catastrophic, and originates in management failure. These systems rely on a document-based approach, which involves handling disjointed artifacts that are expensive to maintain and may become inconsistent and obsolete. We propose a framework for managing process safety that pioneers the modeling of protective systems according to the tenors of model-based systems engineering (MBSE). The framework embeds management and governance, and harmonizes regulations and inconsistent industry guidelines. Potential users include enterprises and regulators in the chemical process safety industry and the energy sector. The framework starts the development of more sophisticated standards to prevent catastrophic protective systems failures.

Keywords: MBSE, Model-Based Systems Engineering, Protective Systems, Management of Change, Managing Process Safety, SysML.

1 Introduction

Designing and operating protective systems is a major engineering endeavor, due to the intricacy and complexity of its technologically enabled physical components, the management system that supports them, and their wide variety of stakeholders. Furthermore, protective systems need to be constantly evolving, in order to remain effective as disruptive technologies emerge, and policies, regulation, operating conditions or requirements change. This constant evolution brings the additional challenge of management of change throughout their lifecycle.

Every year, incidents happen in safety-critical companies throughout the world. While the majority of them are "near misses", others have significant economic and moral implications, as they result in important business interruption costs, property damages, environmental damages, injuries and fatalities among both internal workers and external civilians who may or may not be aware of the risks imposed on them. Regulators and judges therefore require methods and tools to reduce the asymmetry of information, mitigate moral hazard, and induce preventive and protective measures while facing financial and informational constraints and dealing with a large number of agents. Seeking to deter the risk-creators and compensate the victims, they use *ex post* civil liability and *ex ante* safety regulation in its various forms: compliance-based regulation (prescriptive regulation), performance-based regulation, and process-based regulation (integral supervision).

Many minor incidents have quickly escalated into major events, with poorly mitigated consequences (Marsh-Ltd, 2018). Although several other incidents with significantly less damage have the same root causes, all of the largest property-damage losses that have occurred in the last few decades in the hydrocarbon industry, were due to a simultaneous failure of various prevention and mitigation layers in the protective process-safety management system (Marsh-Ltd, 2014).

The failure of protective systems can be catastrophic; and such failures are associated to management failure (Marsh-Ltd, 2018; Jarvis and Goddard, 2017; Summers and Hearn, 2012). Infrequent inspections, lack of preventive and corrective maintenance, faulty designs, lack of needed redundancies, the use of incompatible equipment, materials or protocols after a deficiently planned change, improper resource allocation, careless operation by personnel not properly trained or with excessive workload, and many other issues that can cause a major incident are originated in management.

Nevertheless, managing protective systems requires more than ensuring compliance with practices and procedures. It is extremely difficult for several reasons, including not having enough historical data to analyze (Selvik and Abrahamsen, 2016) or being uncertain about whether systems indeed function properly in the fortunate absence of initiating causes. Models such as the safety pyramid, based on the work of H. W. Heinrich (Heinrich, 1941) and its extensions (Rebbitt, 2014), suggest that focusing on the underlying causes of near misses, where more data exists, can be useful to prevent serious incidents, as their underlying causes are essentially the same. While identifying and addressing the initiating causes of incidents is undeniably beneficial to advance process safety, if protective systems work as intended, the critical consequences of initiating causes can be prevented or mitigated. The usefulness of information provided by the study of near misses is limited, as it may not always be related to aspects affecting protective systems.

Furthermore, the implications of a shared governance, the dynamic nature of technology and people in the system, as well as the multiple interactions among their elements, increase complexity. Safety is an emergent property (Leveson, 2013); this implies that elements that may be safe on their own, do not necessarily constitute a safe system once they interact with other components. As safety-critical technologies evolve and complexity increases, we need tools to improve our ability to manage them.

Protective systems are often characterized by a group of protection layers, such as inherently safer design, control, supervisory, preventive, mitigative, barrier, limitation, and response (Center for

Chemical Process Safety, 2007), intended to reduce the frequency or consequence severity of hazardous events (Center for Chemical Process Safety, 2001; Center for Chemical Process Safety, 2007; Crowl and Louvar, 2011). This representation, similar to the Swiss Cheese Model of Accident Causation, proposed by Dante Orlandella and James T. Reason of the University of Manchester, is used in Layer of Protection Analysis (LOPA), whose primary purpose is to determine if there are sufficient layers of protection against a hazardous scenario to meet an organization's risk tolerance criteria. Given that no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the incident tolerable (Center for Chemical Process Safety, 2001; Dowell, 2011). Modeling protective systems based on their physical layers designed to prevent, and ultimately respond to a loss of containment in the presence of an initiating cause seems appropriate, but this approach is limited, as it does not encompass management issues, such as who the owners and operators of each layer are or who is accountable for them. When the same agent manages two or more layers, this makes them subject to common-cause failures, which makes the assumption of independence between layers is hard to achieve in practice.

Advancing the efficacy of protective systems requires more than focusing solely on improving their physical components, as several engineering research works do; the way they are designed, but also managed and governed is key as well. The paradigm of High Reliability Organizations (HROs), by Todd LaPorte, Gene Rochlin, and Karlene Roberts, of the University of California, Berkeley, links management to safety (Roberts, 1990a; Roberts, 1990b; Roberts and Bea, 2001; Roberts and Libuser, 1993); however, that paradigm does not provide a model suitable for analyses and simulation, and does not encompass regulatory issues. While industrial associations, regulatory bodies, and other disciplines have done a remarkable work to offer guidelines and best practices involving management (Center for Chemical Process Safety, 1994; Center for Chemical Process Safety, 1995; Center for Chemical Process Safety, 1996; Center for Chemical Process Safety, 2007; Center for Chemical Process Safety, 2008; Center for Chemical Process Safety, 2011), there are some inconsistencies among their publications, which complicates integration, and their work still relies on the traditionally used document-based approach. This implies handling and maintaining a large number of disjointed artifacts, which is expensive and time consuming; but more importantly, may lead to inconsistency and obsolescence, thus aggravates the problem of deficient management of change.

MBSE is a relatively new approach, which emerged in the aerospace industry, that significantly reduces the limitations of its document-based counterpart, and has other benefits beyond maintenance, including traceability and impact analysis capabilities. It has been successfully applied in other technologies, but not yet in protective systems.

Our work presents a framework that embeds governance in protective systems, and pioneers the modeling of the multiple dimensions of protective systems according to the tenors of MBSE. It harmonizes regulations, theories, and inconsistent industry guidelines; provides a realistic approach to manage multiple aspects of change; and offers traceability and visualization capabilities.

2 MBSE

2.1 What is MBSE?

Systems Engineering (SE) has many definitions, as those given by the International Council on Systems Engineering (INCOSE) (Walden et al., 2015), the U.S. Department of Defense (DoD) (Office of the Deputy Assistant Secretary of Defense, 2016), the National Aeronautics and Space Administration (NASA) (NASA, 2007), the Federal Aviation Administration (FAA) (Federal Aviation Administration, 2016), among other institutions and authors. They often refer to an interdisciplinary approach or process to design, realize, manage, operate and retire successful systems, document and satisfy requirements, meet the user needs, while taking into account their socio-technical aspects. SE is seen as an effective way to manage complexity and change (Walden et al, 2015). SE approaches can be either document-based, or model-based. The document-based approach has many drawbacks, because it involves having many disjoint artifacts, which can easily become inconsistent and obsolete. In the model-based approach, the main artifact is an integrated, coherent, and consistent system model (Delligatti, 2014), which evolves and is refined using model-based methods and tools (Friedenthal et al., 2015).

MBSE is “the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases” (Holt, 2004). The three pillars of MBSE are modeling languages, modeling methods, and modeling tools (Delligatti, 2014). Modeling languages are standardized mediums to communicate model elements and their relationships; modeling methods ensure model consistency; and modeling tools enable the creation of models with elements, relationships, and views, in such way that any change made to a model element on a diagram automatically propagates, instantaneously updating all the other diagrams where that element is displayed.

MBSE practitioners commonly use the Systems Modeling Language (SysML). It originated from an initiative between the Object Management Group (OMG) and INCOSE in 2003, intended to adapt the Unified Modeling Language (UML) for systems engineering applications (Holt and Perry, 2014), allowing to represent the structure, the behavior, and the requirements of a system through nine types of diagrams. Block definition diagrams (BDD) display and categorize elements and their relationships. Internal block diagrams (IBD) show the connections between the internal parts of a block and their interfaces. Parametric diagrams (PAR) express constraints using equations and inequalities. Package diagrams (PKG) display the organization of the model as a package containment hierarchy. Requirements diagrams (REQ) use texts to display requirements, and how other model elements satisfy, verify and refine them. Activity diagrams (ACT) depict the transformation of inputs into outputs and the flow of control through a sequence of actions. Sequence diagrams (SD) specify interactions among blocks via operation calls and asynchronous signals. State machine diagrams (STM) specify the states of a block and possible state transitions in response to event occurrences. Use case diagrams (UC) illustrate the actions that a system performs, as well as the actors that invoke and participate in them (Delligatti, 2014).

2.2 Benefits of MBSE

Modeling a system is useful in characterizing existing systems, designing new systems, conducting impact assessments, and training its operators and maintainers (Friedenthal et al., 2015). Modeling helps to address complexity, lack of understanding, and poor communications. When applied effectively, MBSE is a formidable approach to manage complexity and increase the understanding of a system, and brings important benefits such as consistency, coherence, traceability, a common language that improves communication, as well as the automatic generation and maintenance of system documents (Holt and Perry, 2014). The diagrams and texts used in this approach are views of the underlying system model, not the model itself (Delligatti, 2014), thus, they communicate different aspects of the system model, such as its structure, behavior, requirements, at different levels of granularity, and may suit the information needs of different audiences, while remaining consistent and integrated.

2.3 MBSE and safety

SysML has been employed successfully in the aerospace and defense industry (D'Ambrosio and Soremekun, 2017), with safety applications, particularly during the design phase. Jensen and Tumer (Jensen and Tumer, 2013) used SysML to evaluate the safety of a system under critical event scenarios involving one or more component failures in the design stage of a maneuvering system for a satellite. They included in their system model the object view for the software and hardware components, the view of function for their behavior, and a third view called "safety functions", referring to the property of a system to resist moving from a hazardous state to an mishap state, essentially describing protective systems in a broad sense. The use of SysML extensions has been proposed for improving the modeling of mechatronics specificities such as interconnection components and multi-physical interactions in an Electro-Mechanical Actuator for aeronautics industry (Mhenni, Choley, and Nguyen, 2015). The use of MBSE with SysML has also been proposed for handling the increased complexity of the automotive industry (D'Ambrosio et al., 2017).

3 Conceptual Model of Protective Systems

Our conceptual model of protective systems, depicted in Figure 1, shows the broad, interrelated elements that constitute a protective system. Together, they provide a baseline for the structure of our MBSE framework, referred to as the "system model".

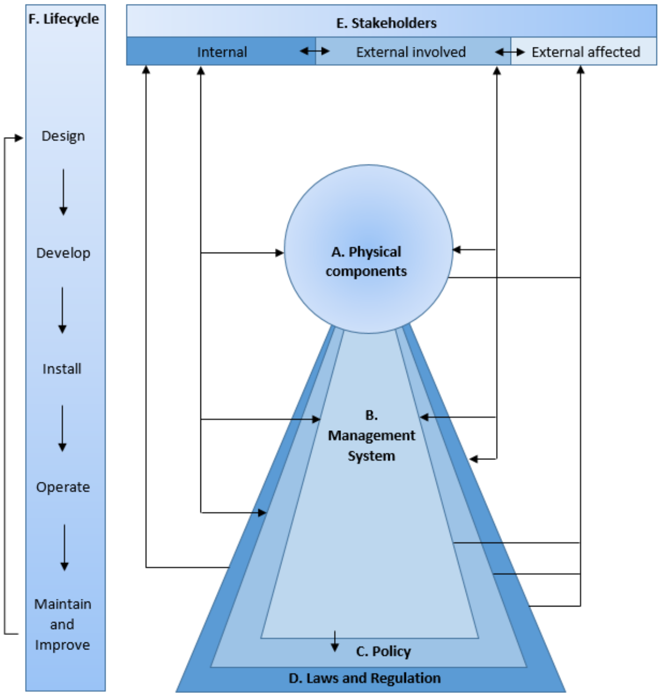


Figure 1. *A conceptual model of protective systems.*

3.1 Model elements

The *physical components* (A) such as sensors, alarms, relief devices, dikes, water curtains, and emergency shutdown systems, for instance, are present in the preventive, mitigative, barriers, and limitation layers of protection. Physical components are supported by a *management system* (B) that includes operating procedures, control systems, monitoring and supervision activities intended to prevent hazardous events and correct anomalies. Management of change, design procedures, documentation, hazard assessment, processes for reviewing and preserving equipment integrity, human factors, training, audits, incident investigation, and emergency response, among others, are activities of major importance that belong to the management system. Industry standards and guidelines such as those from the CCPS of the AIChE (Center for Chemical Process Safety, 2007), serve as a basis for their identification. This element encompasses the structure, processes and resources contained in the inherently safer design, control, and supervisory layers, but also the management part behind the responsive layer. The management system provides the structure, processes and resources to establish the *operating policy* (C), which must comply with the applicable *laws and regulation* (D). The *stakeholders* (E) can be classified into three categories: internal, external involved, and external affected. The internal ones belong to the company and actively participate in the design, operation and management of the protective system. While the external agents do not belong to the company, some are involved in such activities (e.g. manufacturers, first responders, regulatory authorities), whereas others are not, but can be affected by protective systems failure (e.g. near neighbors).

The *lifecycle* (F) acknowledges that there are various stages that depend on and build upon each other over time. For that reason, the system model artifacts need to show in what stages certain activities occur. The outputs of each stage may become the inputs for the subsequent, which implies that they will inherit characteristics, consequences of decisions or issues to address. When referring to the lifecycle, many SE approaches have a “cradle-to-grave approach”, defining it as the entire spectrum of activity, from the identification of needs to the system retirement and material disposal (Blanchard, 2008), including the stages of observation, failing/concern/opportunity awareness, development, transition, operation, maintenance, enhancement, overhaul, decommission, and disposal. Conversely, the CCPS organizes the protective management system lifecycle in seven phases: (1) planning, (2) risk assessment, (3) design, (4) engineering, (5) installation, commissioning, and validation, (6) operational and mechanical integrity, and (7) continuous improvement (Center for Chemical Process Safety, 2007). While the activities of abandonment of outdated practices and decommission and disposal of obsolete or worn out materials are still implicit in the last two stages, this concept of lifecycle phases is consistent with the evolving nature of protective systems, and follows a “cradle-to-cradle” approach, which is the one we chose for our model.

3.2 Interactions among elements

Besides presenting a structural decomposition of the main types of elements of a protective system, it is important to understand some interactions and dependencies depicted by the arrows in the conceptual model. No individual has full visibility of the whole complex system, and yet, changes in one element could affect others as well. The needs of the stakeholders are refined into requirements for the physical components and the management system. Internal stakeholders can determine policy, and some external stakeholders may affect laws and regulation. Both types of stakeholders may be affected by protective system failure. Internal stakeholders, as well as the external involved, possess more information about the protective system compared to the remaining external stakeholders, as the former work together to design and operate it. Nevertheless, the external stakeholders who are involved, such as the regulatory authorities and the citizen participation groups who represent the near neighbors, can take into account the interests of the external affected stakeholders. These interactions can prevent or mitigate asymmetry of information issues.

The management system (B) supports the physical components (A) and establishes the operating policy (C), which must comply with the applicable laws and regulation (D). The arrow that connects (B) and (C) illustrates that unidirectional dependency. Given that policy does not automatically change when the regulation does, the model does not include an arrow connecting (D) and (C). Instead, laws and regulation can affect the internal stakeholders who are able to change policy directly, and the stakeholders who create or modify laws and regulations can affect the management system that establishes policy. Also, the graphical representation of (B), (C) and (D) as various layers, with (D) as the outer layer reinforces the idea of compliance. Presenting (B) as the base for (A) conveys the idea that the management system supports the physical components. The arrows that connect each lifecycle stage represent how stages depend on and build upon each other. The feedback from the “maintain and improve” stage to the “design” stage is consistent with the cradle-to-cradle philosophy. Given the very low level of granularity in our broad conceptual model, the specific interactions between (F) and (E) are not shown; however, other artifacts in the detailed system model developed after it should indicate what stakeholders participate in each lifecycle stage.

For the sake of simplicity, the conceptual model does not show the possible interactions among elements of the same type, but these clearly exist and must be included in the system model. Physical components interact among themselves: sensors provide inputs for logic solvers and final elements; closing a valve on the discharge of a pump may result in pump damage; opening a pressure control vent valve may affect the amount of released gases that incinerators or flares will need to burn. In the management system, new operating procedures, as well as lessons to learn revealed in incident investigations and audits, have to be communicated in the form of training to personnel and contractors; hazard analysis or evaluation require process safety information, and changes in any element need to be assessed and approved by management of change.

3.3 The dynamic nature of protective systems

Protective systems have a dynamic nature. They must respond to the new demands from the safety-critical technologies they are intended to protect, which evolve over time. Their physical components wear out and become obsolete as technology advances, personnel turnover demands training and documentation, laws and regulations are amended, the needs and requirements of the different types of stakeholders change, affecting the management system and the operating policy. Change is constant and inevitable. Failing to manage it effectively can compromise the efficacy of protective systems.

4 Results and discussion

4.1 A computerized model in SysML

Based on our conceptual model of protective systems that encompasses the physical components, the management system that supports them and determines the operating policy, which must be consistent with laws and regulations, and has different stakeholders participating throughout its lifecycle, we created a computerized model, referred to as “the system model”. We used the modeling language SysML, and the software NoMagicMagic Draw 18.3 with its SysML Plugin, and the Paramagic Plugin for simulation purposes. This model details each broad category of elements in order to show their structure and behavior, as well as the relations and interactions among them. It consists of more than 500 blocks, 74 activities, 49 packages, 31 requirements, 77 use cases, and 7 views and viewpoints, sketched in over 65 diagrams. The full diagrams are available from the authors upon request. For its design, we used information extracted and adapted from the CCPS guidelines and Occupational Safety and Health Administration’s Process Safety Management of Highly Hazardous Chemicals (OSHA PSM) (U.S. Department of Labor. Occupational Safety and Health Administration, 2000).

4.1.1 LOPA as one of many views of the system model

According to the MBSE approach, the diagrams and other system artifacts are simply views of the system model. They reveal portions of the model at specific levels of granularity. Our system model presents the current characterization of protective systems, which consists of a group of protection layers used in LOPA, as one view of protective systems. Figure 2 conveys the idea that the protection layers, which are inherently safer design, control, supervisory, preventive, mitigative, barriers, limitation, and response, can be affected by initiating causes, such as instrumentation failure, equipment failure, an external event, human error, or utility failure. While this broad representation may be useful to illustrate the main idea behind LOPA, many other views in our model system provide greater detail regarding the structure, behavior, and relationships between each type of the many elements of a protective system.

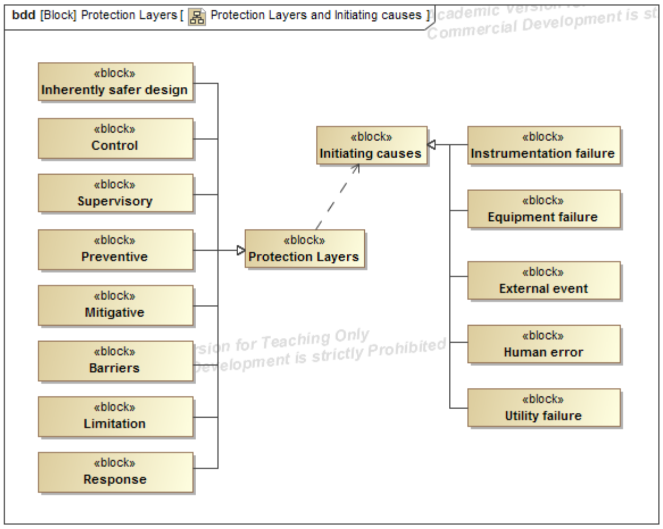

bdd [Block] Protection Layers [Protection Layers and Initiating causes]
«block» Inherently safer design
«block» Control
«block» Supervisory
«block» Preventive
«block» Mitigative
«block» Barriers
«block» Limitation
«block» Response
«block» Protection Layers
«block» Initiating causes
«block» Instrumentation failure
«block» Equipment failure
«block» External event
«block» Human error
«block» Utility failure

Figure 2. *Protection layers and initiating causes.*

Diagram 1 shows a BDD with the taxonomy of the protection layers. It presents the generalization between devices and the type of protection layer into which they can be classified. Generalizations show that the subtype is a type of a supertype. This is useful, as all the properties assigned to a supertype are inherited to the subtypes, whereas those from the subtypes are only specific to them. Diagram 2 has a taxonomy of the initiating causes and displays an accepted definition of each for documentation purposes. Diagram 3 provides further details regarding generalizations, composite associations, reference associations and dependencies of such protection layers. In other words, it conveys structural decomposition, depicts existing connections and possible unidirectional or bidirectional accesses among certain elements, and the notion that whenever one element changes, others stated there may change as well.

Figure 3 corresponds to a portion of Diagram 3, which illustrates that the process alarms have both hardware and software, and that changes to alarms hardware may affect alarms software. It also shows that process alarms, as well as basic process control systems, belong to the Control protection layer. Another portion, depicted in Figure 4, exposes the unidirectional connections among pressure relief devices with knockout drums, condensers and incinerators; pressure relief devices and vents; scrubbers and vents; and scrubbers and flares. It also shows the factors that determine the necessary height of the elevated flares: the stack diameter, the distance from the base of the flare, the desired heat intensity, the vapor rate, and the molecular weight of the vapor, each one with their respective units. The corresponding equations, which appear as constraints, are embedded in the model through the use of PAR. Diagram 4 complements Diagram 3 by revealing the functions that these types of mechanical equipment perform in a relief system, in an ACT. A portion of it is shown in Figure 5.

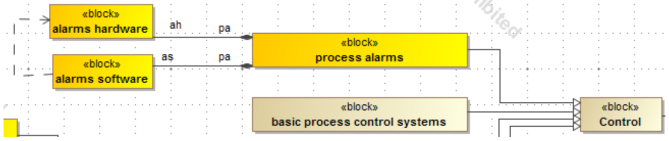


Figure 3. *Portion of BDD in Diagram 3 showing process alarms.*

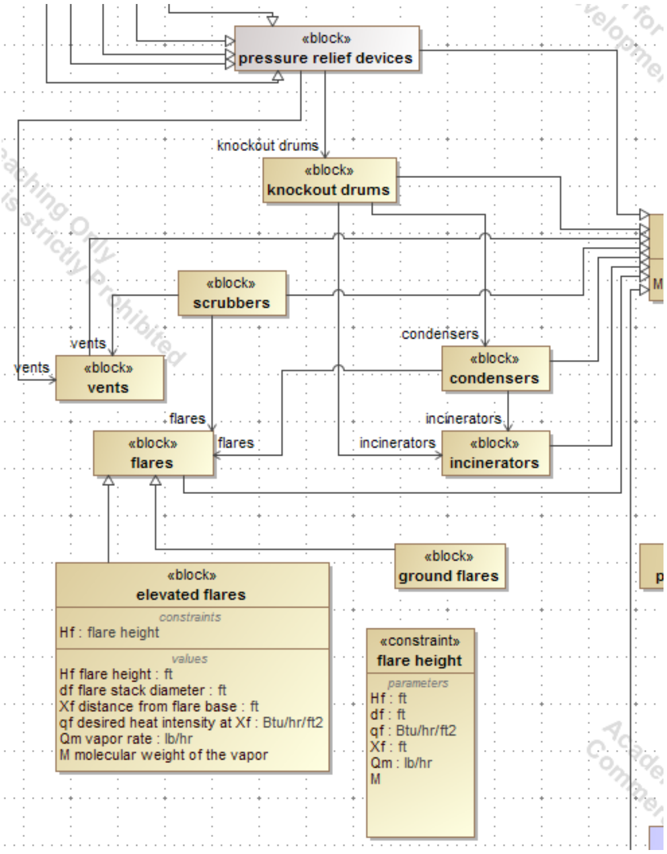


Figure 4. *Portion of BDD in Diagram 3 depicting relations among various types of mechanical equipment.*

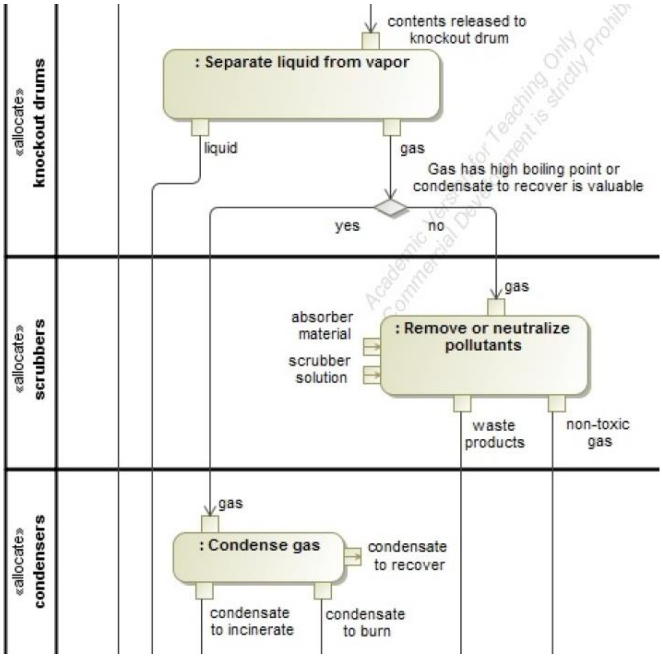


Figure 5. *Portion of ACT in Diagram 4 showing the functions performed by some mechanical equipment.*

4.1.2 Physical components

Many of the elements that constitute the protection layers are physical components. Because of these generalizations, defined in Diagram 5, the structural and behavioral features assigned to the block of physical components are inherited automatically, by transitivity, to all the subtypes. Further properties are assigned only to specific subtypes. Figure 6 illustrates that all physical components have maintenance procedures, installation procedures, and inspection and testing procedures; but only specific physical components have other properties: mechanical equipment has piping and instrument diagrams; various types of pressure relief devices, which are a subset of the mechanical equipment, have a relief system design.

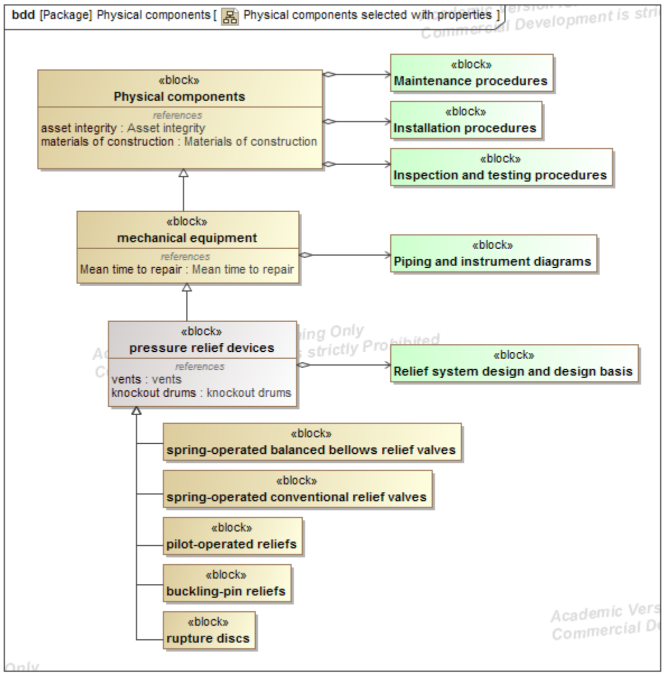

bdd [Package] Physical components [Physical components selected with properties]
«block»
Physical components
references
asset integrity : Asset integrity
materials of construction : Materials of construction
«block»
Maintenance procedures
«block»
Installation procedures
«block»
Inspection and testing procedures
«block»
mechanical equipment
references
Mean time to repair : Mean time to repair
«block»
Piping and instrument diagrams
«block»
pressure relief devices
references
vents : vents
knockout drums : knockout drums
«block»
Relief system design and design basis
«block»
spring-operated balanced bellows relief valves
«block»
spring-operated conventional relief valves
«block»
pilot-operated reliefs
«block»
buckling-pin reliefs
«block»
rupture discs

Figure 6. *Selected physical components with properties assigned at various levels.*

4.1.3 Management system

The management system that supports the physical components is represented in our system model in Diagrams 6 through 20, in order to display the various elements present in OSHA PSM, as well as their respective components, which were modeled as parts. Figure 7 shows them summarized, in the form of one block, with its elements displayed as part properties. In Diagram 21, an IBD details the information and objects that flow across the elements of the management system, which reveals possible interactions among themselves. A portion of it can be found in Figure 8. Management of change (MOC) is one of the main components of the management system. Given the multiple interactions that MOC has with other components, as well as its major importance in process safety, it deserves special attention. Our model includes a section related to MOC systems, based on the CCPS guidelines for the management of change for process safety (Center for Chemical Process Safety, 2008). Diagram 22 displays various packages with the inputs and outputs to and from MOC, such as the package in Figure 9. Diagrams 23 through 32 illustrate diverse aspects of MOC, from the commitment required from management to allocating resources and providing training to those involved in activities derived from or affected by changes, the key principles and essential features of MOC, the activities of MOC decision structure, or the tasks that should be performed during the design and development lifecycle stages in order to create a MOC system, to the roles that internal stakeholders play in MOC, the steps followed during MOC, and details about the request for change review and approval procedure. Figure 10, Figure 11, and Figure 12 present portions of such diagrams.

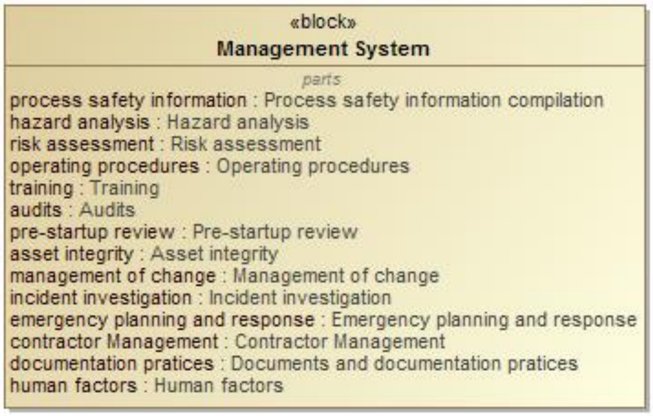

«block»
Management System
parts
process safety information : Process safety information compilation
hazard analysis : Hazard analysis
risk assessment : Risk assessment
operating procedures : Operating procedures
training : Training
audits : Audits
pre-startup review : Pre-startup review
asset integrity : Asset integrity
management of change : Management of change
incident investigation : Incident investigation
emergency planning and response : Emergency planning and response
contractor Management : Contractor Management
documentation pratices : Documents and documentation pratices
human factors : Human factors

Figure 7. *Block of the management system.*

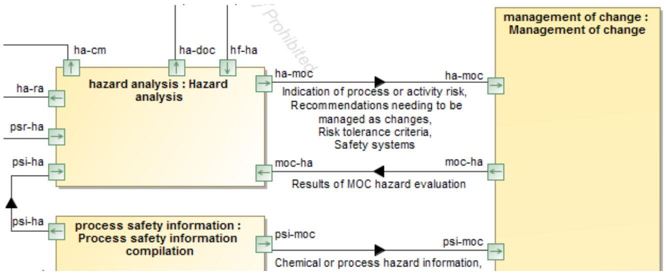

ha-cm
ha-doc
hf-ha
hazard analysis : Hazard analysis
ha-ra
psr-ha
psi-ha
ha-moc
ha-moc
Indication of process or activity risk,
Recommendations needing to be
managed as changes,
Risk tolerance criteria,
Safety systems
moc-ha
moc-ha
Results of MOC hazard evaluation
management of change : Management of change
psi-ha
process safety information : Process safety information compilation
psi-moc
psi-moc
Chemical or process hazard information,

Figure 8. *Portion of the IBD in Diagram 21 depicting information flow within the management system.*

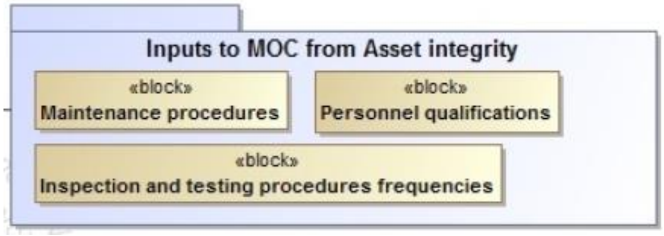

Inputs to MOC from Asset integrity
«block»
Maintenance procedures
«block»
Personnel qualifications
«block»
Inspection and testing procedures frequencies

Figure 9. *Portion of Diagram 22 depicting a package of inputs to MOC from Asset integrity.*

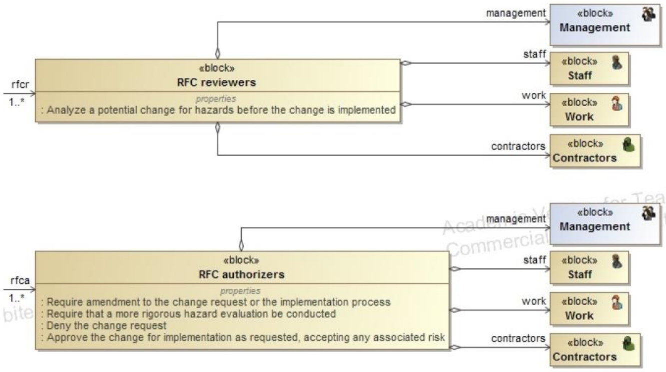

management
«block»
Management
staff
«block»
Staff
work
«block»
Work
contractors
«block»
Contractors
rfcr
1..*
«block»
RFC reviewers
properties
: Analyze a potential change for hazards before the change is implemented
management
«block»
Management
staff
«block»
Staff
work
«block»
Work
contractors
«block»
Contractors
rfca
1..*
«block»
RFC authorizers
properties
: Require amendment to the change request or the implementation process
: Require that a more rigorous hazard evaluation be conducted
: Deny the change request
: Approve the change for implementation as requested, accepting any associated risk

Figure 10. *Portion of the BDD in Diagram 29 depicting the roles in MOC and the stakeholders who play them.*

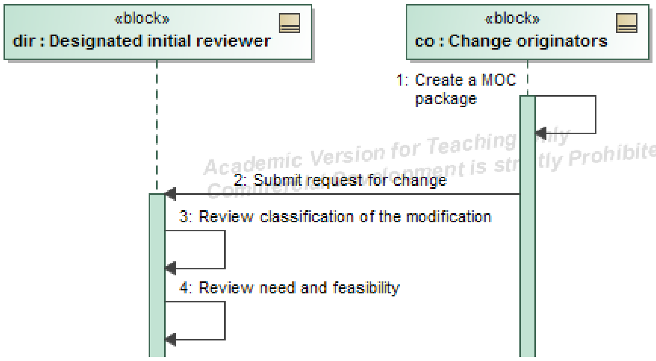

«block»
dir : Designated initial reviewer
«block»
co : Change originators
1: Create a MOC package
2: Submit request for change
3: Review classification of the modification
4: Review need and feasibility

Figure 11. *Portion of the SEQ in Diagram 31 depicting the steps followed during MOC and the interactions among the people playing each role.*

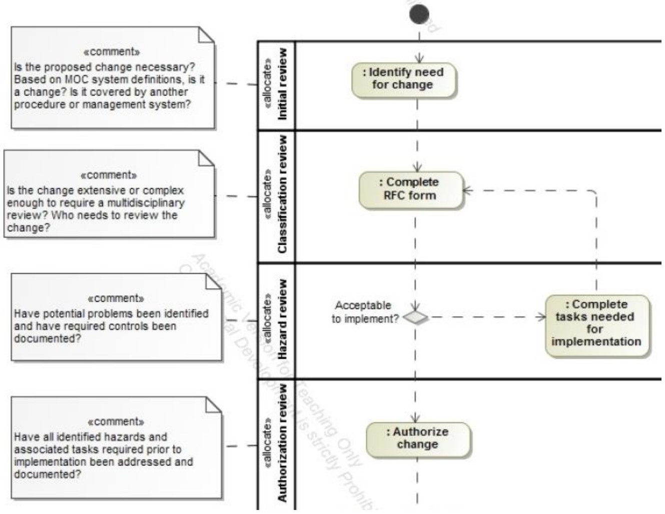
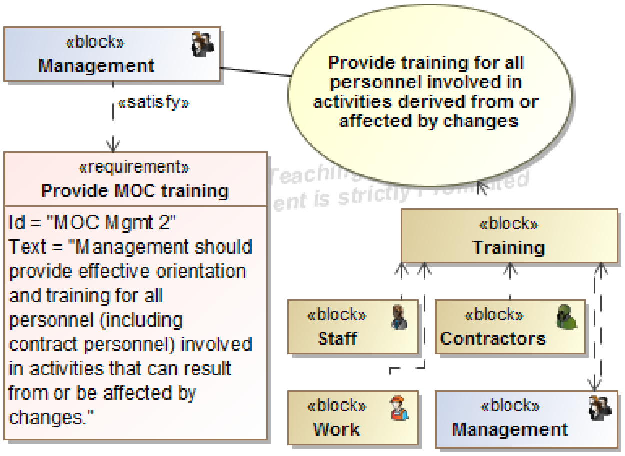

«comment»
Is the proposed change necessary? Based on MOC system definitions, is it a change? Is it covered by another procedure or management system?
«comment»
Is the change extensive or complex enough to require a multidisciplinary review? Who needs to review the change?
«comment»
Have potential problems been identified and have required controls been documented?
«comment»
Have all identified hazards and associated tasks required prior to implementation been addressed and documented?
«allocate» Initial review
«allocate» Classification review
«allocate» Hazard review
«allocate» Authorization review
: Identify need for change
: Complete RFC form
Acceptable to implement?
: Complete tasks needed for implementation
: Authorize change

Figure 12. *Portion of the ACT in Diagram 32 depicting the Request for change review and approval procedure.*

4.1.4 Policy, laws and regulation

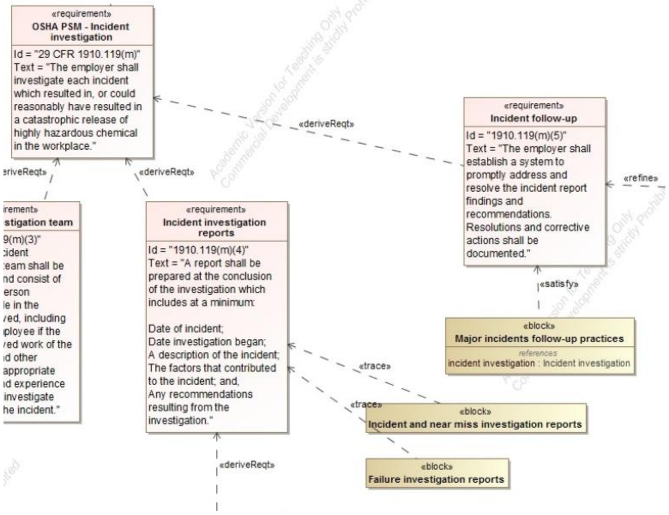
The policy element from our conceptual model is included in the system model in various ways. The operating procedures part of the management system, detailed in Diagram 16, encompasses many aspects of policy, such as the steps required to correct or avoid deviation in the operating limits, the engineering controls and the administrative controls established in safer work practices, failure responses, compensating measures and procedures to apply in the event that a shutdown fails. Another way to represent policy is through the information that flows across the parts of the management system, since it includes procedures (e.g. inspection procedures, maintenance procedures) and criteria (e.g. risk tolerance criteria, criteria for applying procedures). Some blocks from the taxonomy of the protection layers are also elements of policy.

Policy, laws and regulations also appear in our model in the form of requirements. Requirements may be represented as tables, as part of block diagrams, or as REQ. We also used use cases, with their corresponding activity diagrams, to illustrate courses of action, as in Figure 13. Various relationships among requirements and other model elements, such as containment, trace, derive requirement, refine, satisfy, and verify, provide greater detail and further properties regarding how those requirements are fulfilled or can be traced in the system. In Diagrams 35 and 36 we included examples of applicable laws and regulation, such as OSHA PSM, the Toxic Substances Control Act II, the Risk Management Program of the Environmental Protection Agency (EPA RMP), the Emergency Planning and Community Right-to-Know Act, in the form of requirements. A small portion of diagram can be found in Figure 14. Diagram 37 is a REQ that also shows some use cases and blocks to depict the core attributes of the protection layers. A portion of it is shown in Figure 15.



Id = "MOC Mgmt 2"
Text = "Management should provide effective orientation and training for all personnel (including contract personnel) involved in activities that can result from or be affected by changes."

***Figure 13**. Policy depicted with a requirement and a use case.*


«requirement»
OSHA PSM - Incident investigation
«deriveReqt»
eriveReqt»
«deriveReqt»
irement»
stigation team
«requirement»
Incident investigation reports
«requirement»
Incident follow-up
«refine»
«satisfy»
«block»
Major incidents follow-up practices
references
incident investigation : Incident investigation
«trace»
«trace»
«block»
Incident and near miss investigation reports
«block»
Failure investigation reports
«deriveReqt»

Id = "29 CFR 1910.119(m)"
Text = "The employer shall investigate each incident which resulted in, or could reasonably have resulted in a catastrophic release of highly hazardous chemical in the workplace."

9(m)(3)"
cident
team shall be
nd consist of
erson
le in the
ved, including
ployee if the
ved work of the
d other
appropriate
d experience
investigate
he incident."

Id = "1910.119(m)(4)"
Text = "A report shall be prepared at the conclusion of the investigation which includes at a minimum:

Date of incident;
Date investigation began;
A description of the incident;
The factors that contributed to the incident; and,
Any recommendations resulting from the investigation."

Id = "1910.119(m)(5)"
Text = "The employer shall establish a system to promptly address and resolve the incident report findings and recommendations. Resolutions and corrective actions shall be documented."

***Figure 14.** Portion of a REQ exemplifying laws and regulations modeled as requirements.*

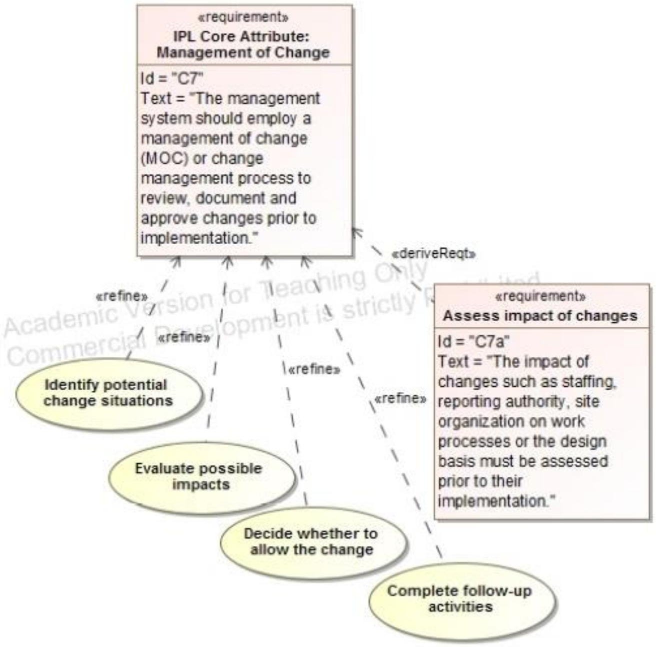

«requirement»
IPL Core Attribute: Management of Change
Id = "C7"
Text = "The management system should employ a management of change (MOC) or change management process to review, document and approve changes prior to implementation."
«deriveReqt»
«requirement»
Assess impact of changes
Id = "C7a"
Text = "The impact of changes such as staffing, reporting authority, site organization on work processes or the design basis must be assessed prior to their implementation."
«refine»
«refine»
«refine»
«refine»
Identify potential change situations
Evaluate possible impacts
Decide whether to allow the change
Complete follow-up activities
Academic Version for Teaching Only
Commercial Development is strictly

Figure 15. *Portion of Diagram 37 illustrating the use of requirements and use cases to include policy, laws and regulation in the system model.*

4.1.5 Lifecycle

The lifecycle is represented in the system model in various views. The first one, presented in Diagram 38 and Figure 16, shows the lifecycle as an aggregate of various stages. An aggregate, in contrast to a composition, is not responsible for its parts (Weilkiens, 2007). The direct reference associations that link the stages convey the idea that they depend and build upon each other. The position of the arrowheads in the system model, as opposed to those from our conceptual model, do not stand for the chronological flow of information. Instead, according to the standards of the modeling language used, they suggest that the later stages can access information from earlier stages.

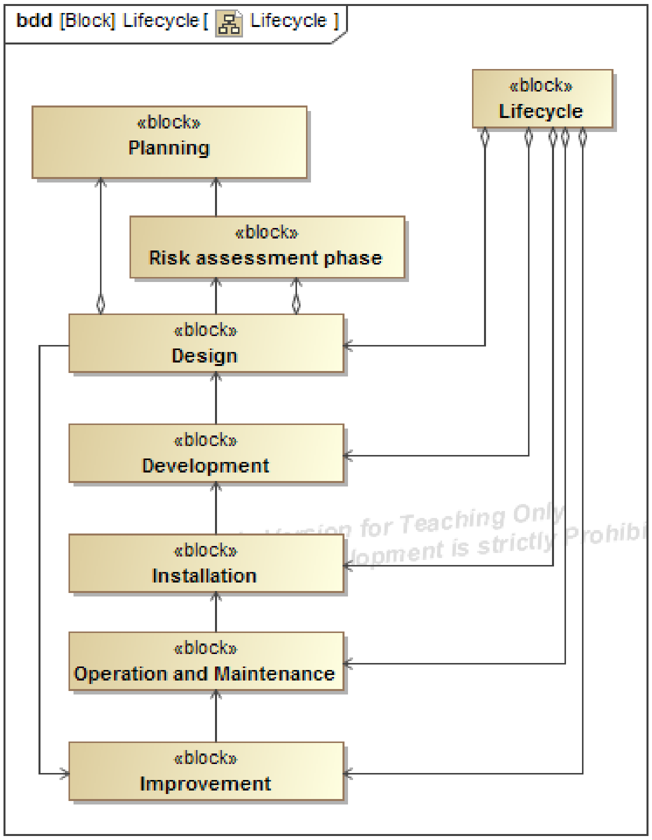


Figure. 16. *Lifecycle stages.*

The lifecycle stages also appear in the model as partitions or swimlanes in Diagram 39, which corresponds to an ACT that allocates major activities to the lifecycle stage where they are expected to occur. The diagram shows the flow of information as object tokens, as well as the control tokens that enable subsequent activities. Each activity has inputs and outputs, which are not just texts; instead, they are referenced to blocks that may appear in other diagrams and reside in a specific repository. They have properties such as parts and references, and may have further capabilities suitable for analysis. Figure 17 shows a portion of Diagram 39.

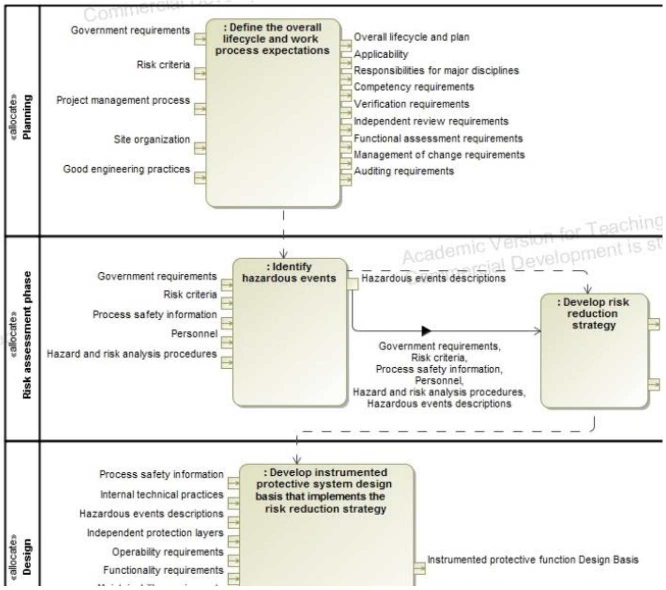

«allocate» Planning
: Define the overall lifecycle and work process expectations
Government requirements
Risk criteria
Project management process
Site organization
Good engineering practices
Overall lifecycle and plan
Applicability
Responsibilities for major disciplines
Competency requirements
Verification requirements
Independent review requirements
Functional assessment requirements
Management of change requirements
Auditing requirements
«allocate» Risk assessment phase
: Identify hazardous events
Government requirements
Risk criteria
Process safety information
Personnel
Hazard and risk analysis procedures
Hazardous events descriptions
Government requirements, Risk criteria, Process safety information, Personnel, Hazard and risk analysis procedures, Hazardous events descriptions
: Develop risk reduction strategy
«allocate» Design
: Develop instrumented protective system design basis that implements the risk reduction strategy
Process safety information
Internal technical practices
Hazardous events descriptions
Independent protection layers
Operability requirements
Functionality requirements
Instrumented protective function Design Basis
Academic Version for Teaching
Commercial Development is st

Figure 17. *Portion of Diagram 39 depicting the allocation of activities within lifecycle stages.*

Diagram 40 contains a very large BDD that reveals further information about the inputs and outputs in Diagram 39, including their structural decomposition and the various lifecycle stages to which they are allocated, as some of them are inputs to more than one activity, or outputs from one activity and inputs to another. Diagram 41 contains the same elements as those in Diagram 40, but rearranged as a tulip, in such way that the blocks that appear at the core are those that are used in two or more lifecycle stages, and the blocks in the periphery are used only during one stage. This suggests that the elements at the core deserve more attention due to their greater importance and complexity in the system. These are: hazardous events descriptions, independent protection layers, instrumented protective function design basis, operability requirements, process safety information, reliability requirements, internal technical practices, functionality requirements, maintainability requirements, independent protection layers analysis report, equipment list, and detailed engineering specification.

4.1.6 Stakeholders

The stakeholders are presented in various diagrams. In Diagram 42 and Figure 18, they are classified, as in our conceptual model, into three categories: internal involved, external involved, and external affected. They appear as icons since the software tool allows it, but they are still blocks with their corresponding functionalities. Diagram 43 has a detailed taxonomy of stakeholders, which includes those mentioned in OSHA PSM (U.S. Department of Labor. Occupational Safety and Health Administration, 2000), Rasmussen's framework (Rasmussen, 1977), and various mismatching CCPS guidelines (Center for Chemical Process Safety, 1994; Center for Chemical Process Safety, 1995; Center for Chemical Process Safety, 1996; Center for Chemical Process Safety, 2004; Center for Chemical Process Safety, 2007; Center for Chemical Process Safety, 2008; Center for Chemical Process Safety, 2011). See Figure 19 for a portion of it. We used generalizations to allow the subtypes to inherit the properties assigned to their supertype. Diagram 44 is a PKG that summarizes the stakeholders that participate in each lifecycle stage, and their respective concerns, according to the guidelines for safe and reliable instrumented protective systems (Center for Chemical Process Safety, 2007). A portion of it is shown in Figure 20.

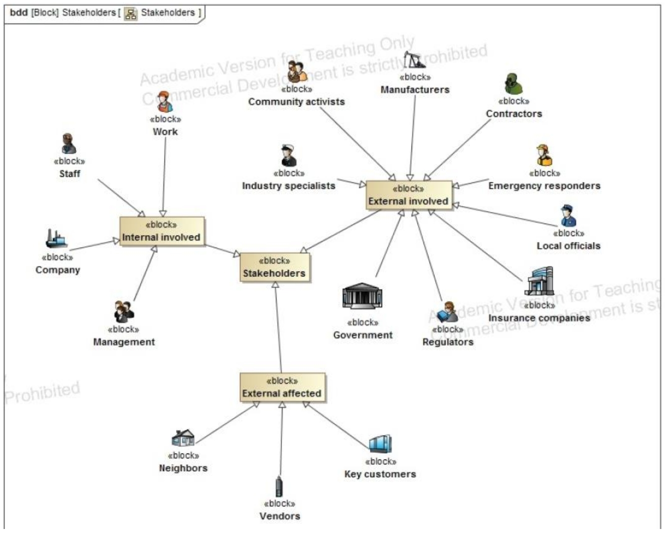


Figure 18. *Protective system stakeholders.*

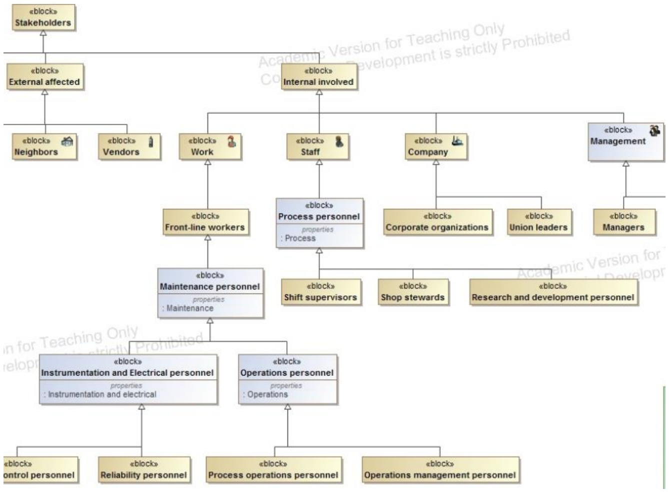
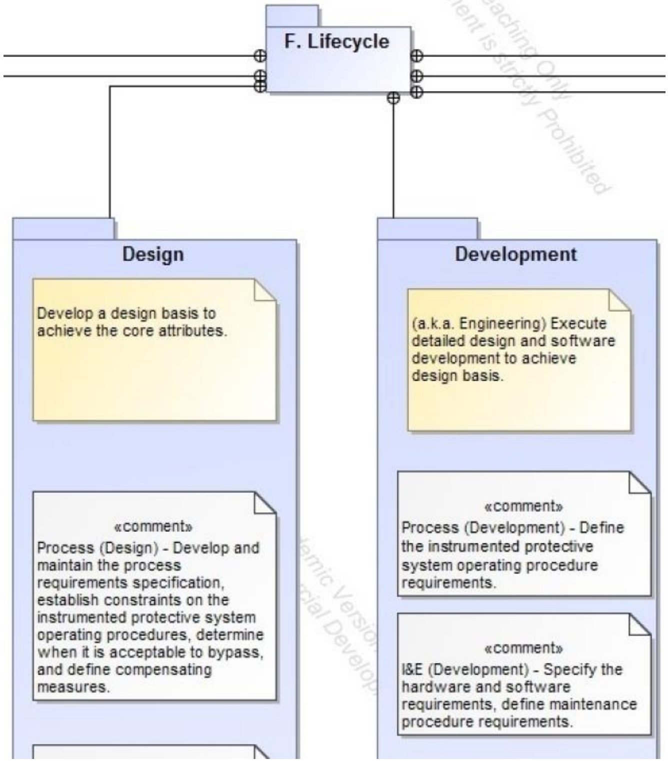

«block» Stakeholders
«block» External affected
«block» Internal involved
«block» Neighbors
«block» Vendors
«block» Work
«block» Staff
«block» Company
«block» Management
«block» Front-line workers
«block» Process personnel
properties
: Process
«block» Corporate organizations
«block» Union leaders
«block» Managers
«block» Maintenance personnel
properties
: Maintenance
«block» Shift supervisors
«block» Shop stewards
«block» Research and development personnel
«block» Instrumentation and Electrical personnel
properties
: Instrumentation and electrical
«block» Operations personnel
properties
: Operations
«block» ontrol personnel
«block» Reliability personnel
«block» Process operations personnel
«block» Operations management personnel

Figure 19. *Portion of Diagram 43 depicting a taxonomy of stakeholders.*



Develop a design basis to achieve the core attributes.

Process (Design) - Develop and maintain the process requirements specification, establish constraints on the instrumented protective system operating procedures, determine when it is acceptable to bypass, and define compensating measures.

(a.k.a. Engineering) Execute detailed design and software development to achieve design basis.

Process (Development) - Define the instrumented protective system operating procedure requirements.

I&E (Development) - Specify the hardware and software requirements, define maintenance procedure requirements.

Figure 20. *Portion of Diagram 44 depicting stakeholders' concerns through different lifecycle stages.*

SysML allows to model views and viewpoints. Views are packages that selectively import various diagrams, packages, model elements, etc., which constitute an aspect that is of interest to a particular set of stakeholders (Delligatti, 2014). Viewpoints specify the stakeholder, the concerns, the purpose, the languages, and the methods. Diagrams 45a and 45b present two ways in which the stakeholders' views and viewpoints can be modeled. Not only do they show in which lifecycle phases they participate, allowing a visual comparison, but they also specify what model information is relevant to them. Figure 21 exemplifies the views and viewpoints of two stakeholders. Diagrams 46 through 52 detail packages that contain all the model elements allocated or associated to lifecycle phases.

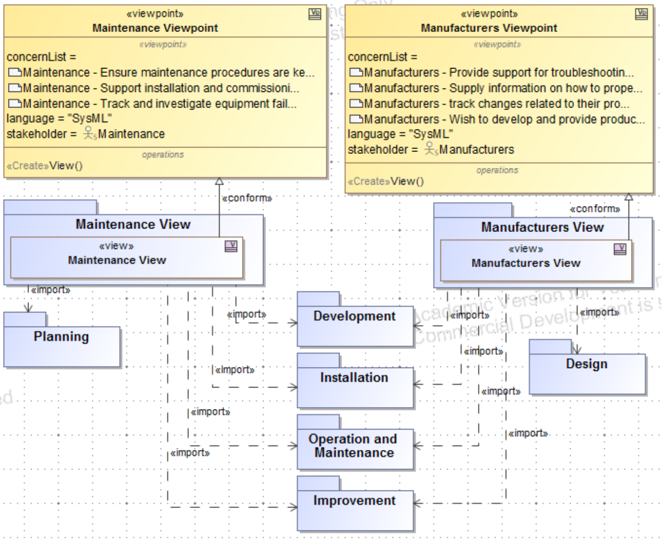
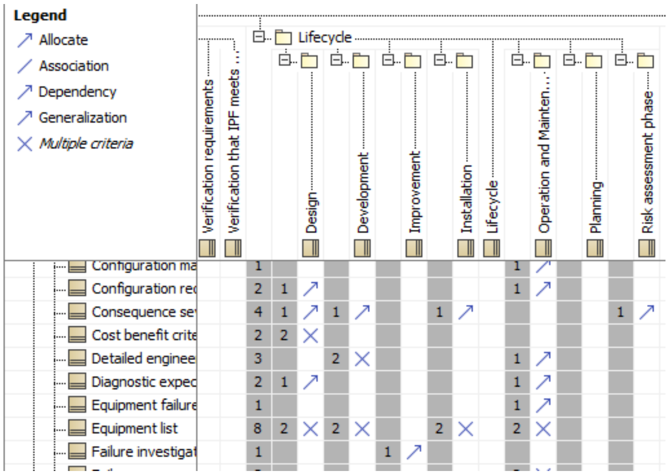

«viewpoint»
Maintenance Viewpoint
«viewpoint»
concernList =
Maintenance - Ensure maintenance procedures are ke...
Maintenance - Support installation and commissioni...
Maintenance - Track and investigate equipment fail...
language = "SysML"
stakeholder = Maintenance
operations
«Create»View()
«viewpoint»
Manufacturers Viewpoint
«viewpoint»
concernList =
Manufacturers - Provide support for troubleshootin...
Manufacturers - Supply information on how to prope...
Manufacturers - track changes related to their pro...
Manufacturers - Wish to develop and provide produc...
language = "SysML"
stakeholder = Manufacturers
operations
«Create»View()
«conform»
Maintenance View
«view»
Maintenance View
«conform»
Manufacturers View
«view»
Manufacturers View
«import»
Planning
Development
Installation
Operation and Maintenance
Improvement
Design

Figure 21. *Views and viewpoints of two stakeholders importing packages.*

4.2 Tools for impact analysis and management of change

Software tools that work with SysML can provide users, including designers, managers, and regulators, with tools for impact analysis and management of change. In the event we wanted to make a change in one of our model elements, it would be important to determine whether that change would impact other parts of the system. The software tool we have chosen can quickly identify in which diagrams the object appears, open them and show the element location, or navigate through the diagrams. Besides knowing the usage of a specific element in other diagrams, before making any changes to it, we need to identify what other model elements interact with it, and the kind of relationships that they have, in order to assess possible impacts. With the software modeling tool we used, it is possible to display in the current diagram the related elements from other diagrams, or display a list with the elements of the model that use it or depend on it. It is also possible to generate a dependency report in Microsoft Word, which will list all the model elements that have any kind of declared relation with the element, the type of relation, or if it is a connector that conveys information from one node to another. Although the dependency report can specify relations such as containment, dependency, allocation, association, direct association, aggregation, direct aggregation, composition, direct composition, generalization, and applied stereotypes including imports of packages, it does not show the direction of the arrows in the relations, that is, it does not specify whether the related element is a client or a supplier, and it does not display inherited relationships, that is, those assigned to a supertype. Nevertheless, these two limitations can be overcome by opening the specification of block properties for the desired blocks.

Some alternatives provided by the tool are to generate either a dependency matrix in Microsoft Excel, or an allocation matrix in NoMagic MagicDraw. A portion of an allocation matrix is shown in Figure 22. These matrices display all the elements in the model in the first row and column vectors, and the existing relations among them in the appropriate entries. Models with many unrelated elements generate sparse matrices. Since both types of matrices have the same limitations from dependency reports, we recommend to use the specification of block properties in conjunction with the matrices. If the model only declares dependencies between elements A and B, and between elements B and C, the user of dependency reports, dependency matrices or allocation matrices may be able to infer that element C could be indirectly affected by element A. Having the big picture that these matrices provide can be beneficial for impact analysis and management of change, as long as the model is well constructed and declares the relations between elements.



Legend
- ↗ Allocate
- ╱ Association
- ↗ Dependency
- ↗ Generalization
- ✕ *Multiple criteria*

			Lifecycle															
	Verification requirements	Verification that IPF meets ...			Design		Development		Improvement		Installation	Lifecycle		Operation and Mainten...		Planning		Risk assessment phase
Configuration ma			1										1	↗				
Configuration rec			2	1	↗								1	↗				
Consequence se			4	1	↗	1	↗			1	↗						1	↗
Cost benefit crite			2	2	✕													
Detailed enginee			3			2	✕						1	↗				
Diagnostic expec			2	1	↗								1	↗				
Equipment failure			1										1	↗				
Equipment list			8	2	✕	2	✕			2	✕		2	✕				
Failure investigat			1					1	↗									

***Figure 22**. Portion of an allocation matrix*

4.3 A model and a method for impact analysis in the context of MOC

One of the key principles and essential features of management of change is to evaluate possible impacts (Center for Chemical Process Safety, 2008). Impact analysis requires a model and a method. The model of protective systems we have presented, which can be adapted to the characteristics of the industries where it will be used, offers the stakeholders tools to perform this activity. Its outputs include lists and matrices that show dependencies and other relations among its elements. The software functions allow the user to identify where each element is used.

Our proposed method for impact analysis with our model recommends the following steps: First, use the software tools to identify where a model element is used, in order to ensure that a possible change that seems pertinent according to a diagram is indeed suitable in the remaining diagrams. Second, refer to the outputs of the model and check what are the other elements that have any dependencies or other declared relations with the element whose impact is being analyzed, and what kind of relation exists among them. If there are dependencies with other elements, the user should go further and identify the dependencies that those related elements have with other not already considered elements. Dependencies communicate that a change in the supplier element (at the arrowhead end) may result in a change to the client element (at the tail end). Therefore, the user must pay attention to the direction of the dependency to determine whether the element is a client or a supplier.

4.4 Cross-sections, views and viewpoints for shared governance and multiple stakeholders

Although many of the model elements are organized according to the lifecycle stages in which they occur, in order to be part of a model library that can be shared with the stakeholders involved, or be imported by another model that encompasses further aspects related to that time frame, in order to understand and address better the concerns of each stakeholder, regardless of the amount of lifecycle stages where they participate, it is possible and convenient to have a subset of the model that contains the parts that are relevant for them. The use of packages or package diagrams allows partitioning the model and presenting it as cross-sections, offering views that filter the model according to the point of view of each stakeholder, or specific aspects intended to address.

A cross-sectional modeling style, combined with the capability of the modeling language to show many views and viewpoints, is beneficial in the context of shared governance, as it can help to specify and clarify the roles and responsibilities of each group of multiple stakeholders, understand the needs and concerns of other groups, and identify possible gaps. It is also possible to create a single view of the elements that two or more types of stakeholders have in common, in order to facilitate collaboration. Creating views that import selected packages only can allow external stakeholders to obtain the information they need to know, without giving them access to aspects of the company that should not be disclosed, such as classified information, confidential business information, and trade secrets. This approach can therefore mitigate asymmetry of information without compromising sensitive information.

4.5 Implications of having a computerized model for maintenance

With regard to maintenance, the MBSE approach offers many advantages compared to its document-based counterpart. Instead of having as system artifacts several disjointed manuals, spreadsheets and other text-based files that need to be updated every time the system changes, with the difficulties inherent to keeping track of all the places in which a modified element appears and the time and resources needed to ensure that all the documents are properly updated, at the risk of having inconsistencies among the updated and outdated artifacts, leading to the obsolescence of the latter if any misses occur, the MBSE approach that our model of protective systems follows allows a fast and inexpensive maintenance that prevents inconsistencies caused by leaving one or more artifacts outdated by mistake, as any changes made to an element of the model are automatically propagated to each and every place where that element appears.

Nevertheless, this advantage also has its drawbacks. It is very dangerous to change an element of the model based solely on one of the diagrams where it appears, because all the other diagrams in which the element to update is present will instantly be modified as well, and perhaps the change may not always be desirable or compatible, or could impact other elements not previously considered. For that reason, besides being cautious about who is given the authority to modify the system model, as well as the timing for the updates, managers should always follow a proper procedure of management of change, which must include the impact analysis discussed earlier. The model should be updated only after the proposed changes have been evaluated and approved. Special attention must be paid at the moment of the update in case the change only took place in some instances of the model element, in order to adjust the model accordingly and avoid the modification of all the instances at once. For example, instead of renaming or modifying the properties of a block that is used in two or more diagrams, which would propagate the changes throughout all the diagrams where it is used, we recommend to replace the block subject to change only in the affected diagram with a new block with a different name and properties.

4.6 Benefits for managers and regulators

Managers can benefit from this model in many ways. It can lower the cost of system documentation maintenance; it provides tools for impact analysis and management of change; it can be used in training, and be used to increase awareness and understanding about the interactions and information flows among physical components, the management system, policies, procedures and requirements from laws, regulation, and recommendations from professional associations; the activities to perform during each lifecycle stage, with their corresponding inputs and outputs; as well as the notion of who the stakeholders are and what are their main roles an concerns.

Besides acknowledging governments and regulators as stakeholders of protective systems, this model also provides them with tools to mitigate moral hazard and asymmetry of information, and perform activities related to loss prevention and the preservation of public safety. Regulators have the authority to enforce the adoption and use of protective systems, but they may also suggest, promote, or demand the use of MBSE to facilitate companies to comply with prescriptive regulation, such as those in OSHA PSM, EPA RMP, or any other applicable. The adoption of MBSE practices may also facilitate audits and inspections, since companies would be able to provide the authorities with the current status of the company regarding the implementation of protective measures, as well as their processes and equipment. Regulators may also benefit from this model as it may help them to keep in hand the specific needs and concerns of the near neighbors and general population they seek to protect, summarized and captured as the views and viewpoints of the external affected stakeholders. Also, having a model that illustrates the structure and behavior of the protective systems that companies use could help them determine what information they should request in order to mitigate moral hazard and answer questions to the public. At the same time, companies can satisfy the requests of regulators by creating packages with the information to disclose to external stakeholders, consistent to their concerns.

5 Conclusions

This work presents a MBSE framework that advances the state of the art in safety-critical protective systems, by integrating the management and governance dimensions. Our model is still consistent with the current characterization of protective systems as a group of protection layers used in LOPA, but it is also suitable for combined design, operation and regulation. It reduces the cost of maintenance of its artifacts and offers tools for impact analysis and management of change. Potential users include any agents invested in the design and management of protective systems, especially enterprises and regulators from the chemical process safety industry and the energy sector. This work significantly reduces the pitfalls of its document-based predecessors, by offering a visual, organic model with traceable, integrated and consistent elements, whose changes automatically propagate throughout every part where the modified element appears, instead of a set of disjointed texts, which are prone to errors, expensive to maintain, or may become inconsistent and obsolete as the system evolves. This framework encompasses the views and viewpoints of multiple owners, whose roles vary throughout the system lifecycle. Therefore, it supports shared governance, and can be used by multiple agents within and beyond the enterprise premises. While it mitigates information asymmetry, since all of its users share the same model, it also renders the possibility to provide its specific audiences with tailored views, at different levels of granularity, filtered according to their roles and concerns. Future publications about the simulation part of this work will encompass its computational and analytical capabilities, which may allow its users to comply with and support the development of both prescriptive and performance-based regulation. The multiple benefits that the use of MBSE standards provides to safety-critical companies and its many stakeholders, at a very low expense, support our conclusion that it should be a regulatory requirement for managing process safety.

6 Acknowledgement

This work was supported by the Mexican National Council of Science and Technology *Consejo Nacional de Ciencia y Tecnología (CONACyT)*, the Mexican Ministry of Public Education *Secretaría de Educación Pública (SEP)*, and *Tecnológico de Monterrey Campus Estado de México*.

7 References

Blanchard, B. S. (2008). System engineering management. Wiley series in systems engineering and management. Hoboken, NJ : John Wiley & Sons, Incorporated.

Center for Chemical Process Safety (1994). Guidelines for implementing process safety management systems. Center for Chemical Process Safety/AIChE.

Center for Chemical Process Safety (1995). Plant guidelines for technical management of chemical process safety. Revised edition. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (1996). Guidelines for integrating process safety management, environment, safety, health, and quality. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2001). Layer of Protection Analysis - Simplified Process Risk Assessment. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2007). Guidelines for safe and reliable instrumented protective systems. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (2008). Guidelines for the management of change for process safety. Hoboken, NJ : Wiley-Interscience.

Center for Chemical Process Safety (2011). Guidelines for auditing process safety management systems. 2nd ed. New York, NY : Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Crowl, D. A. and Louvar, J. F. (2011). Chemical process safety: fundamentals with applications. Upper Saddle River, NJ : Prentice Hall.

D'Ambrosio, J., and Soremekun, G. (2017, October). Systems engineering challenges and MBSE opportunities for automotive system design. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2075-2080). IEEE.

Delligatti, L. (2014). SysML distilled. A brief guide to the systems modeling language. Upper Saddle River, NJ : Addison-Wesley.

Dowell, A. M. (2011). Is it really an independent protection layer? Process Safety Progress, 30(2):126–131.

Federal Aviation Administration. (2016). National Airspace System System Engineering Manual. https://www.scribd.com/document/98230420/NAS-Systems-Engineering-Manual-Vol-1. Accessed: 2016-08-30.

Friedenthal, S., Moore, A., and Steiner, R. (2015). A practical guide to SysML : the systems modeling language. Waltham, MA : Morgan Kaufman.

Heinrich, H. W. (1941). Industrial accident prevention : a scientific approach. 2nd ed. New York, NY : McGraw-Hill.

Holt, J. (2004). UML for systems engineering : watching the wheels. 2nd ed. London : Institution of Electrical Engineers.

Holt, J. and Perry, S. (2014). SysML for systems engineering – A model-based approach. 2nd ed. London : The Institution of Engineering and Technology.

Jarvis, R., and Goddard, A. (2017). An analysis of common causes of major losses in the onshore oil, gas & petrochemical industries. *Loss Prevention Bulletin*, (255).

Jensen, D. C. and Tumer, I. Y. (2013). Modeling and analysis of safety in early design. Procedia Computer Science, 16(2013 Conference on Systems Engineering Research):824 – 833.

Leveson, N. (2013). The Drawbacks in Using The Term 'System of Systems'. Biomedical Instrumentation & Technology. Association for the Advancement of Medical Instrumentation. http://sunnyday.mit.edu/papers/system-of-systems.pdf. Accessed: 2015-09-30.

Marsh-Ltd (2014). The 100 Largest Losses 1974-2013. Large Property Damage Losses in the Hydrocarbon Industry. 23rd edition. https://uk.marsh.com/Portals/18/Documents/100%20Largest%20Losses%2023rd%20Edition%202014.pdf. Accessed: 2015-02-02.

Marsh-Ltd (2018). The 100 Largest Losses 1978-2017. Large Property Damage Losses in the Hydrocarbon Industry. 25th edition. https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/100-largest-losses.pdf. Accessed: 2019-03-15.

Mhenni, F., Choley, J. Y., and Nguyen, N. (2015, September). SysML extensions for safety-critical mechatronic systems design. In *2015 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 242-247). IEEE.

NASA (2007). Systems engineering handbook. Washington, DC : National Aeronautics and Space Administration.

Office of the Deputy Assistant Secretary of Defense. (2016). Systems Engineering. http://www.acq.osd.mil/se/initiatives/init pp-sse.html. Accessed: 2016-08-30.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3):183 – 213.

Rebbitt, D. (2014). Pyramid power. Professional Safety, 59(9):30 – 34.

Roberts, K. H. (1990a). Managing high reliability organizations. California Management Review, 32(4):101 – 113.

Roberts, K. H. (1990b). Some characteristics of one type of high reliability organization. Organization Science, 1(2):160 – 176.

Roberts, K. H. and Bea, R. G. (2001). When systems fail. Organizational Dynamics, 29(3):179.

Roberts, K. H. and Libuser, C. (1993). From Bhopal to banking: Organizational design can mitigate risk. Organizational Dynamics, 21(4):15 – 26.

Selvik, J. T. and Abrahamsen, E. (2016). How to classify failures when collecting data for safety-instrumented systems in the oil and gas industry. Journal of Risk Research, 0(0):1–11.

Summers, A. E. and Hearn, W. H. (2012). Risk criteria, protection layers, and conditional modifiers. Process Safety Progress, 31(2):139–144.

U.S. Department of Labor. Occupational Safety and Health Administration. (2000). Process Safety Management. https://www.osha.gov/Publications/osha3132.html. Accessed: 2016-03-15.

Walden, D. D., Roedler, G. J., Forsberg, K., Hamelin, R. D., and Shortell, T. M. (2015). Systems engineering handbook : a guide for system life cycle processes and activities. 4th ed. Hoboken, NJ : John Wiley & Sons, Incorporated.

Weilkiens, T. (2007). Systems engineering with SysML / UML : modeling, analysis, design. Amsterdam ; Boston, MA : Morgan Kaufmann OMG Press / Elsevier.