Risk Management Using Systemic Theoretic Process Analysis (STPA)

V2.0

By Gregory M. Pope, CSQE

SQE Group Leader

Lawrence Livermore National Laboratory

Presented at 2020 STAMP Workshop

MIT, Cambridge, MA

July 28, 2020

LLNL-CONF-812813

LLNL-CONF-812813

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Table of Contents

LLNL-CONF-812813

Table of Figures

LLNL-CONF-812813

1.0 Introduction and Definition:

The purpose of this white paper is to present a case study to evaluate the suitability of Systemic Theoretic Process Analysis (STPA) to identify managerial risks. Risk identification and mitigation are important tasks of management. The need to actively manage risks can be summarized in Gilb's risk principle[1], "If you don't actively attack the risks, they will attack you". Risks can be technical in nature such as those found in requirements, specifications, designs, software, and components or managerial in nature such as those found in staffing, training, compensation, and culture.

STPA has already demonstrated its usefulness for hazard analysis of technology-based systems, especially those which are controlled by software rather than simple mechanical or electrical controllers[2]. STPA for management considers organizations as systems that may also benefit from STPA analysis. The case study presented is the restart of a manufacturing process after a 30-year hiatus using raw material that has been in storage. The item to be produced is called a widget for the purposes of this case study. The widget is produced with government funding and many levels of oversight. However, the technique used in this case study could apply to many other project types. This case study identified 84 risks using STPA and created an Excel spreadsheet risk tracking tool to add classification and mitigations to each identified risk. This case study indicates that STPA for management can identify risks and document them in an easy to review format.

LLNL-CONF-812813

2.0 Typical Risk Management Process:

A typical risk management process has multiple steps:

1. Identify the risk, what are the undesired outcomes?
2. Assess the risk, how severe is the consequence of the risk?
3. Develop responses to the identified risks to control them.
4. Develop a risk (contingency) plan and preventive measures to continuously monitor the risks and update the plan as appropriate.

2.1 Identifying Risks:

There are several techniques to help identify technical risks such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Root Cause Analysis (RCA), What If Analysis, Cause and Effect or Fishbone Diagrams, Swot (Strength, weakness, opportunity, threat), Brainstorming, Checklists, Interviews, etc. However, the study of several tragic accidents for instance the chemical release at Bhopal[3], and costly security breaches, for instance the security hack at Equifax[4], often reveal causes that are management related such as government oversight failures, budget cutting, reduced staff, valuing performance over safety, inadequate testing, inadequate training, personality conflicts, creating a stressful work environment, etc. STPA for management considers the organizations involved in the project as systems and identifies risks that may be overlooked by risk analysis of the technical requirements and designs.

2.2 Assessing Risks:

Risk is commonly defined as the consequence of an undesired event multiplied by the likelihood of it happening[5]. Theoretically, some risks are high in consequence, but very unlikely to occur. Other risks are more likely to occur and may have a lesser consequence. Determining the actual likelihood of a risk happening may be difficult or impossible[6] as well as misleading. For instance, Boeing calculated that the probability of a lithium ion battery failure on a 787 would be one in 10 million flight hours. However, two batteries malfunctioned in just two weeks in 2013[7]. Many tragic accidents have happened due to errors that were calculated or estimated to be very unlikely to ever occur, yet they did. This is especially true with software-controlled systems, where despite high reliability hardware, the firmware or software and its interaction with other components can still cause an undesired outcome. A system or software component that is reliable does not automatically inherit the property of safety. Highly reliable software (for instance a software component that can execute for long periods of time) may not be safe. The recent 737 Max accidents is an example of reliable MCAS software that did exactly what it was designed to do, point the nose of the aircraft down under certain conditions. However, this reliable software was clearly not safe, as it could not tell the difference between faulty AOA sensor readings and correct

LLNL-CONF-812813

AOA readings. In this case the software did not fail, but it did cause tragic accidents. Reliable software can also be misused or ignored by an operator. For instance, automobile software that automates driving. It may be reliable but lull the driver into complacency and cause the driver to ignore an emergency where the driver needs to take control of the vehicle to prevent an accident. These component interaction accidents are generally due to system or sub-system requirements being incomplete or incorrect.

To address the first part of the risk equation in this case study (magnitude of an undesired outcome) the following categories are used:

- Magnitude of Impact
    - Public Safety
    - Worker Safety
    - Financial Loss
    - Delay
    - Trivial

The magnitude of impact is straight forward. The highest impact is jeopardizing public safety. A lesser but still serious consequence is jeopardizing worker safety. Lesser consequences are financial losses or project delays. Any consequence less than a delay would be considered trivial.

Traditionally risk consequence of error is multiplied by the probability or likelihood of occurrence. However, as previously mentioned the probability of occurrence may be difficult if not impossible to predict. Initially considered for this case study was using history to determine likelihood. The assumption was if the risk had happened multiple times in the past it would be more likely to happen in the future. If the risk happened only once in the past it would be less likely to happen in the future. If the risk was yet to happen it would be the least likely to happen. However, the counter argument with using history is if the consequence had occurred before it might be less likely (as opposed to more likely) to occur again because whatever caused the risk event has been mitigated.

For instance, modern blimps are filled with Helium gas because of several historical accidents occurring using Hydrogen gas to fill lighter than air ships. In this example what has happened in the past is not an indication it is more likely to happen in the future. In fact, it would be less likely to happen in the future. Therefore, using history to predict the future for risks occurring can have serious shortcomings.

Another concern with using likelihood of occurrence is confirmation bias. There have been numerous examples of future predictions that failed to materialize. A few are listed below:

1. 1876 “Telephones will never catch on” William Orton – Western Union

2. 1927 “Who the hell wants to hear actors talk?” H.M. Warner – Warner Brothers

3. 1946 “Television won’t last because people will soon get tired of staring at a plywood box every night.” Darryl Zanuck – 20th Century Fox

4. 1977 “There is no reason for any individual to have a computer in his home.” Ken Olsen - Digital Equipment Corp

5. 2007 #1 above plus: “Especially phones that act like computers” Steve Ballmer - CEO Microsoft

In each case the person making the prediction had an interest in the new technology not being successful because it would compete with or replace their current product. Confirmation bias may well have limited their ability to predict the future. And these were very smart people making the predictions.

This confirmation bias factor can also exist for an employee of a company attempting to put together a risk prediction using likelihood. For example, at Colossaltron Inc. Bob is the risk manager. He is a full-time employee of Colossaltron Inc. and happy with his career there. Bob enjoys his boss and holds stock options in Colossaltron as part of his compensation package. Bob is due for a big promotion soon. However, the culture at Colossaltron is to “not rock the boat”. Can Bob predict the likelihood of an undesired event without confirmation bias?

In this case study the probability or likelihood for the second risk equation term was abandoned for a new term called Institutional Risk (IR). Institutional Risk is based on the concept that the attributes about the Institution(s) could increase or decrease the risk of an undesired consequence happening. The attributes are divided into four categories:

1. Company or Institution
2. System being built,
3. Personal involved,
4. Project Management.

LLNL-CONF-812813

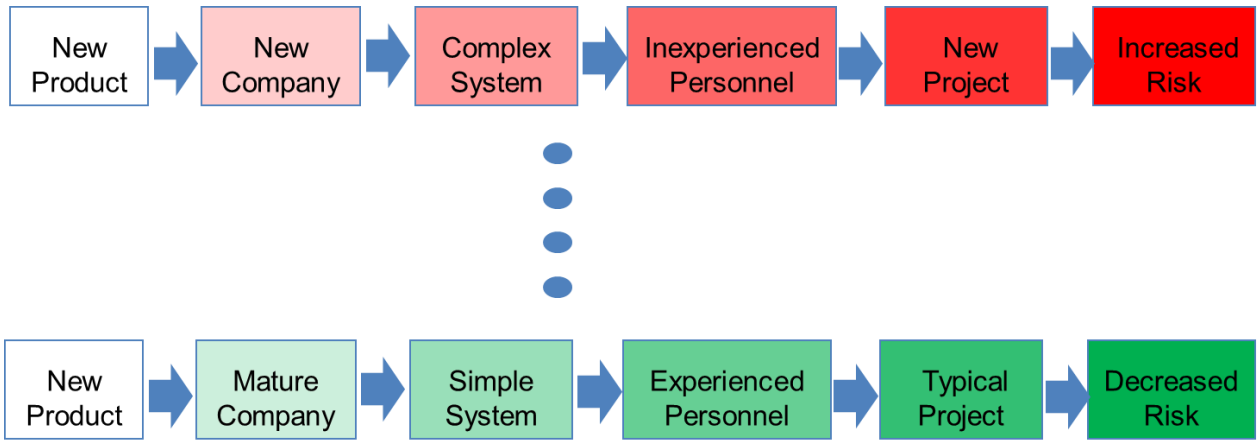

Figure 1 Institutional Risk

In figure 1 two scenarios are presented. The top of figure one (in shades of red) shows a complex system that is going to be built by a new company, using inexperienced staff on a new project. The bottom of figure 1 (In shades of green) shows a simple system that is going to be built by a mature company with experienced personnel on a typical project. The IR would tend to be higher for the case at the top of figure 1. The IR would tend to be lower for the case at the bottom of figure 1. Also, each attribute listed above contains multiple categories of risk contributors. Each risk contributor within each risk attribute is given a risk grade 1-5

Institutional Risk

a. Highest -5
b. High - 4
c. Moderate -3
d. Low - 2
e. Lowest - 1

This approach assumes risk IR about the Company, System, Staff, and Project will make the consequence of error more or less likely to occur. The Risk Inference spreadsheet is shown in figures 2 thru 5. For the 20 institutional risk categories a selection is made from highest to lowest. The institutional risks are averaged. They may optionally be weighted. The institutional risk average value (figure 5 bottom right) is used as input to the risk inference column on the Risk Tracker Spreadsheet (Sections 5.1 thru 5.9). The Institutional Risk value is multiplied by the Magnitude of Impact of the risk. In this case study two Institutional Risks were calculated because two different institutions were involved (The US government and a National Laboratory).

Risk Inference Factors							
	Increased Infrastructure Risk				Decreased Infrastructure Risk		
Company	5	4	3	2	1	Weight	Score
	○	○	○	○	◉		
Experience of Management	Mostly inexperienced in this field		Moderately experienced in this field		Very highly experienced in this field	1	1
	○	○	○	○	◉		
Corporate Health	Funding very restricted, start up, bankruptcy, merger		Successful track record of profitability		Industry leader, best in breed products, great reputation	1	1
	○	◉	○	○	○		
Competition	Monopoly, only provider		Many competitors, customers have choices		Highly competitive marketplace	1	4
	○	○	○	○	◉		
Cost of Entry	Low cost of entry, relatively easy to enter market		Moderate cost of entry, some capital or intellectual resources required		Capital or intellectually resource intensive	1	1

Figure 2 Institutional Risk, Company

	Increased Infrastructure Risk			Decreased Infrastructure Risk			
System	5	4	3	2	1		
	◉	○	○	○	○		
Complexity	Highly complex system, many decisions required, hostile environment		Moderately complex, some decisions required, known environment		Simple decision making, few decisions required, controlled environment	1	5
	○	○	◉	○	○		
Maturity	Brand new system, one of a kind, early adopter		System fielded for many years with good reputation			1	3
	○	◉	○	○	○		
User Base	Still in Alpha or Beta testing, pre-release or prototype versions		Moderate user base, many users familiar with system use		Very large user base, wide system familiarity	1	4

Figure 3 Institutional Risk, System

LLNL-CONF-812813

	Increased Infrastructure Risk			Decreased Infrastructure Risk			
Personnel	5	4	3	2	1		
	○	○	○	○	◉	1	1
Relevant Experience	Staff has very little or no experience building this type of system		Staff has prior experience building this type of system		Staff has in depth experience building this type of system		
	○	○	◉	○	○	1	3
Staffing	Projects are severely understaffed, continual overtime		Projects occasionally require overtime hours to meet deadlines		Projects staffed appropriately, overtime rare		
	○	○	○	○	◉	1	1
Training and Education	Staff requires little training and education		Staff requires some training and education		System knowledge requires extensive training and education		
	○	○	○	○	◉	1	1
Culture	Non-existent Safety and Security culture		Moderate Safety and Security culture		Very Strong Safety and Security culture		
	○	○	○	○	◉	1	1
Communications	Closed Communication problems are not easily discussed or resolved		Guarded communications some problems are tracked and resolved		Open communications, problems are tracked and resolved		
	○	○	◉	○	○	1	3
Availability of Candidates	Qualified candidates are hard to recruit and hire		Some difficulty finding and hiring qualified candidates		Qualified candidates are readily available		

Figure 4 Institutional Risk Personnel

LLNL-CONF-812813

	Increased Infrastructure Risk			Decreased Infrastructure Risk			
Project	5	4	3	2	1		
Schedule	Schedule created without input from those doing the work, extremely optimistic		Schedule created with some input from those doing the work. Deadlines firm		Schedule is well planned by those doing the work, adjusted if required	1	4
Budget	Budget is inadequate to accomplish project		Budget is close to being sufficient to complete project		Budget is fully sufficient to complete project	1	3
Quality	Functional requirements do not satisfy user needs		Functional requirements satisfy most user needs		Functional Requirements meet or exceed user needs	1	2
Security	Security protections not designed into the system nor considered		Security protections added to the system as an afterthought		Robust security protections designed into the system	1	1
Safety	No system hazard analysis performed, safety requirements not identified or tested		Some system hazard analysis performed, safety requirements identified and tested		Robust system hazard analysis performed, safety requirements identified and thoroughly tested	1	1
Process Maturity	Ad hoc process		Managed Repeatable process		Managed, Repeatable continuously improving process.	1	2
Risk Management	Risks not identified		Risks identified		Risks identified and continuously managed	1	1
							Score
							2.15

Figure 5 Institutional Risk Project with Average

Risk is calculated by multiplying the Magnitude of Impact number, for instance 5 by the Institutional Risk (IR) in this example 2.15, yielding a risk score of 14 as shown in figure 6.In this example all the optional weights are 1, so the highest Risk Score would be 25. The weights can be entered as real numbers to de-emphasize or increase the impact of the risk contributors within each risk attribute. The weighting factors (w) can be tailored to the Institution.

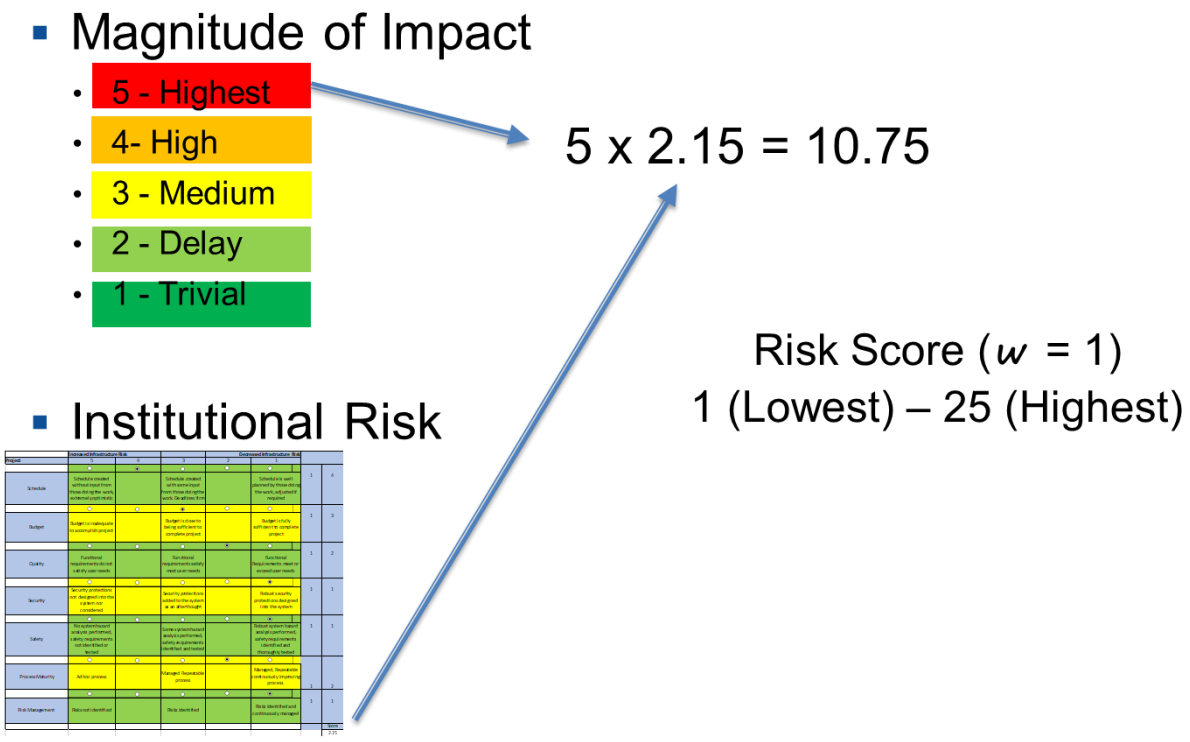

Figure 6 Calculating Risk Score

Institutional Risk can also be applied to multiple Institutions and/or supply chains. Often systems are not built by a single contractor but are built by a combination of suppliers. In this case Institutional Risk may be calculated for each contributing contractor. In this case study three Institutions are involved in restarting the production of widgets. The Government, Private Lab Oversight, and The Lab. Each Institution has a separate Institutional Risk score as shown in figure 8.

LLNL-CONF-812813

Government

Private Oversight

Lab

Figure 7 Calculating Multiple Institutional Risks

The example shown in figure 8 is a supply chain example, the primary contractor or supplier is Sacred Cow Inc. Sacred Cow has a relatively low Institutional Risk score; however, they are dependent upon Trusty's Widgets for certain components. Trusty's Widgets has a slightly higher IR than Sacred Cow. Trusty's Widgets however obtains some of its components from Shifty's Widgets. Shifty's Widgets has a much higher IR score because it obtains some of its components from questionable sources such as eBay.

An Institutional Risk sheet would need to be completed for each of the three suppliers. The score to be used for the risk calculation could be calculated most conservatively by using the highest IR in the supply chain. This asserts the IR for the combined Institution is only as good as the highest IR (or the highest risk supplier). In this case Sacred Cow would be subject to the risk of ordering components from eBay. However, when researching the suppliers to obtain information for their Institutional Risk sheets attention should be paid to each supplier's ability to spot defects or poor quality on components that are supplied to them. If the supplier can demonstrate an incoming inspection process that assures defective parts will be rejected, then the IR could be based on an Institutional Risk higher in the supply chain.

LLNL-CONF-812813

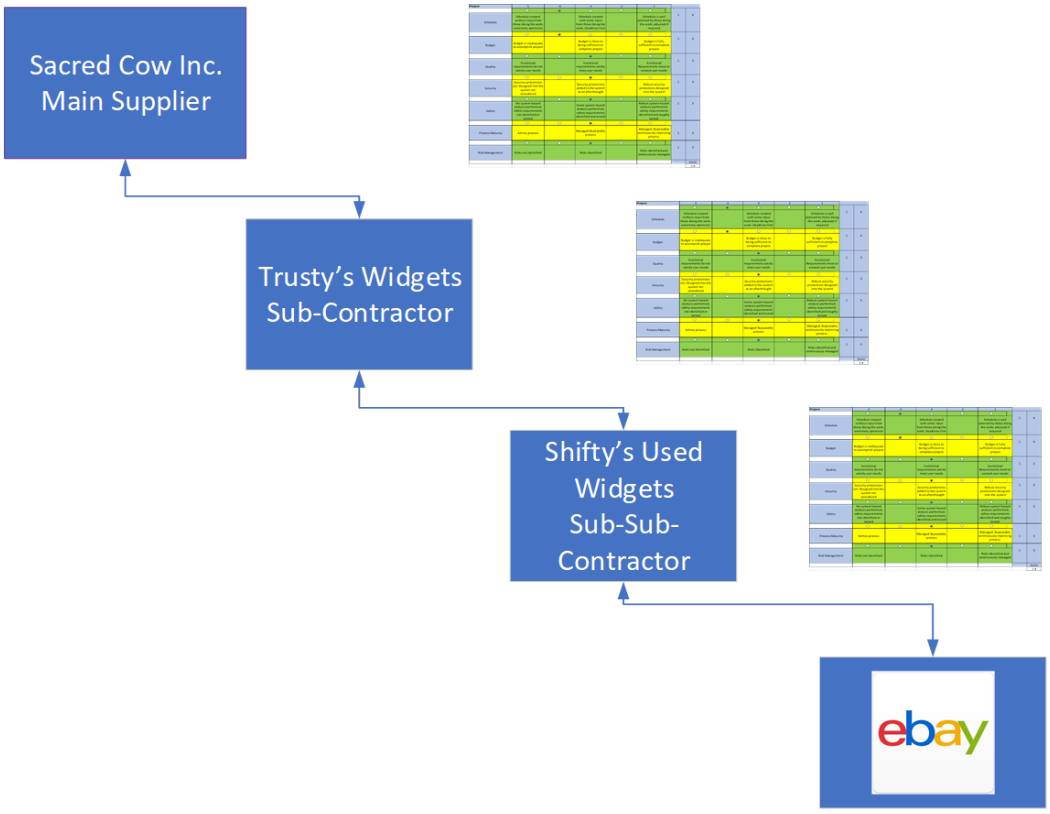

Figure 8 Supply Chain

In summary, using Institutional Risk (IR) was used to replace likelihood of failure. Likelihood of failure can be subject to errors such as mitigation of historical events and confirmation bias. Using Institutional Risk eliminates these error sources and allows the consequence of error to drive risk. Confirmation bias can still play a role in doing an Institutional Risk assessment, so the person(s) doing the Infrastructure Risk assessment should be as impartial as possible.

For environmental risks, and electro/mechanical parts which contain either historical data or reliability data a binary approach was used for this case study. The binary approach is to assume that events with likelihoods of 1 in 100,000 are going to happen, and events over 1 in 100,000 are not going to happen and will not be considered. The threshold of 100,000 is somewhat arbitrary and can be adjusted. The environmental likelihoods also vary by region. For instance, Earthquakes are more likely in California than Florida. Hurricanes are more likely in Florida than California. Earthquakes were considered in this case study based on the location of the widget production facility. Hurricanes were not.

2.3 Developing Risk Responses to Control the Risks:

Part of the risk management process is to develop responses to the risks that are identified. The statuses are:

- Identified
- Active

- Closed
- Unassigned

To be on the list of risks the risk must be identified and the risk response (below) is initially unassigned. When a mitigation (or other risk response) is put in place it is then deemed active. When the risk no longer exists, it is closed. The risk response is selected from the list below:

- Leave It
- Monitor
- Avoid
- Move
- Mitigate
- Unassigned

In this case study the identified risks are active and mostly contain example mitigations. However, there are other possible risk responses, some of which are listed above. The risk can be accepted, and the status set to “leave it”. The risk can be monitored by setting up surveillance or data acquisition and monitoring. The risk can be avoided if the activity that causes the risk can be eliminated. The risk can be moved, for example moved to a sub-contractor. Or as in most cases in this case study the risk is mitigated, actions are put in place to reduce or eliminate the possibility of the risk occurring.

2.4 Develop a Risk (Contingency) Plan and Preventive Measures

A Risk Plan is created to:

- Track the identified risks,
- Periodically assure the risk responses are being applied,
- Update as new risks are identified,
- Modify existing risks or risk responses,
- Remove identified risks that are no longer a concern.

There are several excellent Risk Management techniques that are widely used and are successful. The object of this case study is focus on the first two tasks in the Risk Management process, identification and assessment of risks, that can then become part of a new or existing Risk Management plan. In the example of this case study a Risk Management Plan was done many decades ago for the original production run of widgets. Therefore, the risks identified in this case study would be in addition to any that were previously identified with other techniques.

3.0 Applying STPA to Risk Management, Modeling the Control Structure:

STPA uses a hierarchal control structure shown in figure 9 which is a system model composed of feedback and control loops. A controller provides control actions to control some process and to enforce constraints on the behavior of the controlled process. The control algorithm represents the

controller's decision-making process—it determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs used to make decisions. Process models may include beliefs about the process being controlled or other relevant aspects of the system or the environment. Process models may be updated in part by feedback used to observe the controlled process[8].

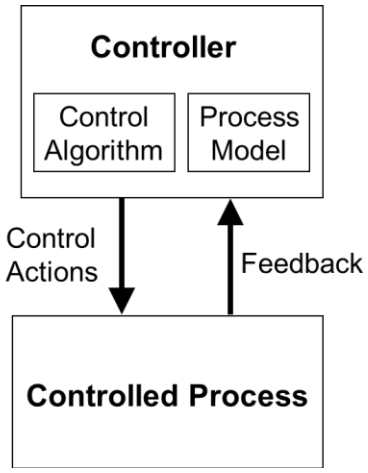

Figure 9 Basic Hierarchal Control Structure

STPA uses the control actions path shown in figure 9 to analyze what could happen if inadequate control actions are taken:

- Control Action Not Given
- Control Action is given but is unsafe
- Control Action is too late, too early, or in the wrong sequence with other control actions
- Control Action is executed for too long or for too short a time.

STPA uses the feedback path shown in figure 9 to analyze what could happen if inadequate feedback is given:

- Feedback not given
- Feedback is incorrect
- Feedback is late
- Feedback is too long or too short

For example, an air traffic controller asks a pilot to change altitudes to avoid terrain directly ahead. Assume the pilot and air traffic controller are appropriately trained and are appropriately experienced in their jobs. They are both familiar with FAA regulations (the control algorithm).

In our example the air traffic controller directs the pilot by broadcasting the flight designation followed by the requested altitude. For instance, "AA 327 climb to FL70". This tells the pilot of Acme Airlines flight 327 to climb to a flight level of 7,000 ft (control action). The pilot or copilot of

Acme Airlines flight 327 would report back what they heard, for instance “AA 327 climb to FL70” (feedback). By the aircraft reporting back verbally what they think they heard reduces the risk that the instruction was not understood. The pilot or co-pilot would then take the necessary actions to implement this control action.

Using the example above STPA can uncover some additional unsafe control actions:

- The controller forgets to ask for the altitude change (Control action not given)
- The controller sends the request to AA 237 (Control action is incorrect)
- The controller delays the request until the aircraft has crashed into the terrain (Control action is too late)
- The controller’s transmission is shortened due to radio static (Control action to short)

The guide phrases are also used on the feedback path uncovering additional risks:

- The pilot does not report back to the air traffic controller (Feedback not given)
- The pilot reports back he will climb to FL90 (Feedback is incorrect)
- The pilot does not report back until the plane encounters the terrain (Feedback given too late)
- The pilot’s report is shorted due to radio static (Report to short)

The basic technique used for STPA for management risk identification is to analyze each interaction between a supervisor and supervisee, the yellow boxes in figure 10. The supervisor is assumed to be a person(s) or entity in the organization that supervise or manage the person(s) or entity below them in an organization (supervisee). The supervisor and supervisee each have a mental model and a control algorithm (orange boxes) that will influence the actions issued and feedback given. The way the supervisor provides control actions (management of the supervisee) is by applying control actions in a management tasks context:

- Planning
- Organizing
- Staffing (Coordinating)
- Directing (Commanding, Leading)
- Controlling

Which are arguably the essential tasks of management[9]. In STPA for risk management these are the inputs to the supervised entity. In figure 10 the four guide phrases (left green box) can apply to any of the five tasks of management (left blue box) to create up to twenty questions that can be asked about (used to analyze) the control actions flowing from the supervisor to the supervised activity.

The supervised entity gives feedback to the supervising entity applying feedback in a management report context:

- Written

- Verbal
- By firsthand observation
- N hand observation

In figure 10 the guide phrases (right green box) can be applied to the four types of reports (right blue box) to create 16 questions that can be asked (used to analyze) the feedback loop.

STPA also considers the mental model (what the supervisor believes the supervisee is doing) and control algorithm (the correct constraint to issue for a perceived mental model) of the supervisor. Likewise, the process model of the supervisee (what the supervisee believes the supervisor wants done) and the control algorithm of the supervisee (the correct action to take given the perceived mental model) determine the reports sent back to the supervisor. The supervisor and supervisee mental models and control algorithms are shown in the orange boxes in figure 10. However, in the case of humans there may be pre-existing beliefs that can taint the belief models or influence the control algorithm of the supervisor and the supervisee. Pre-existing beliefs may come from:

- Training
- Experience
- Communication (verbal and non-verbal)
- Orientation (self-centered versus other-centered)
- Health (physical and mental)
- Attitude (emotional state, workload)

These pre-existing beliefs may influence the model or control algorithm of the supervisor or supervisee and in some cases even override the control actions given or feedback received. For instance, in the Asiana 214 crash[10] the pilot in command of the Boeing 777 was sure the auto pilot would not allow the airspeed to go below stall speed while landing and did not monitor the airspeed indicator which indicated the airspeed was much too slow. This pre-existing belief may well have come from flying an Airbus model and influenced the pilot's control algorithm for landing. Another pre-existing belief in the accident was the pilot's belief that if something was wrong the more senior pilots overseeing the training would notice and say something or intervene.

The five pre-existing beliefs (flesh colored boxes in figure 10) are used to evaluate external forces that could influence the supervisor and supervisee's mental model and control algorithm (orange boxes). Risks are most likely to occur when the mental models or control algorithms are not congruent with reality. The five pre-existing beliefs can alter the mental model and/or control algorithms of the supervisor and therefore impact the 20 combinations of control actions issued or interpretation of the 16 combinations of feedback received. Likewise, the five pre-existing beliefs can impact how the supervisee interprets the 20 combinations of control actions or sends back the 16 combinations of feedback.

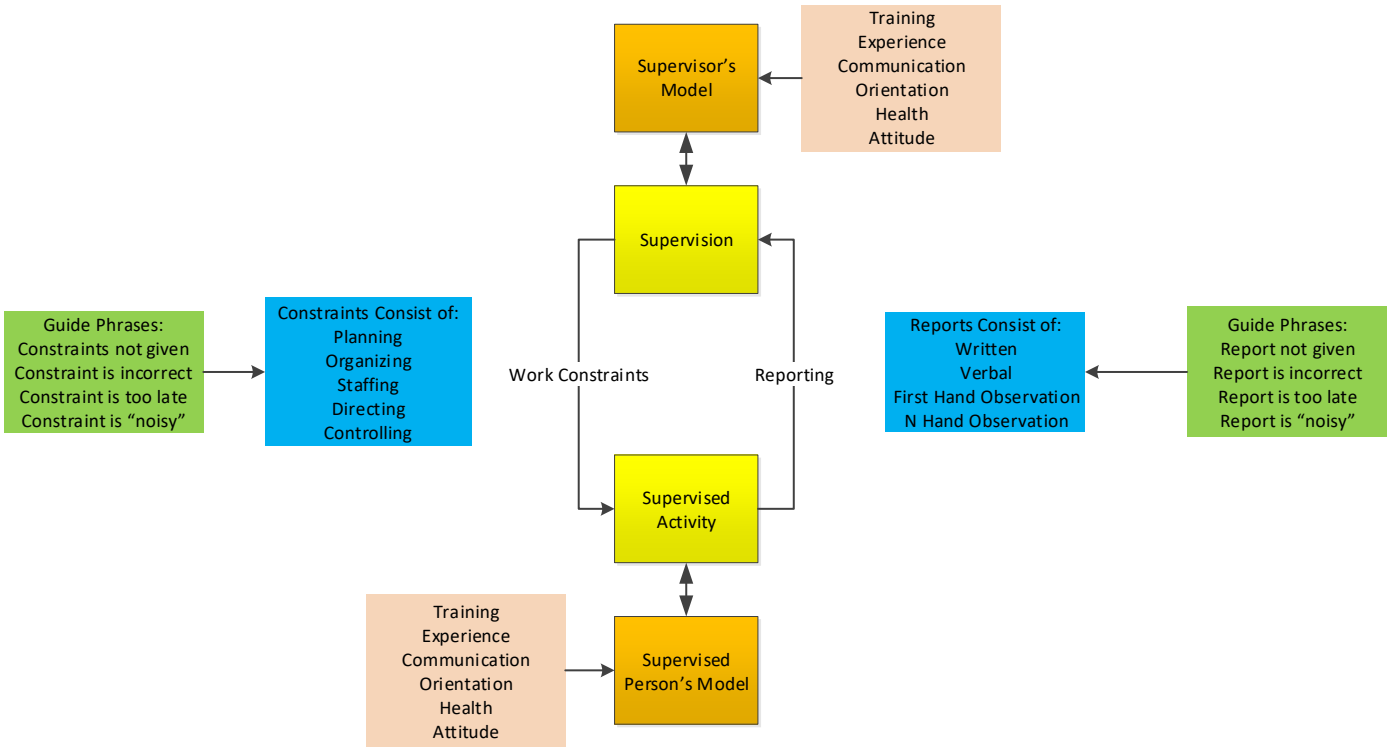

Figure 10 STPA for Risk Management: Organizational Components as a System

STPA in a management context uses the combinations of control actions, feedback, and pre-existing beliefs to structure numerous questions that can be used to analyze and identify risks, for example the 60 questions in Appendix A. The combinations of STPA for management questions act as triggers to help domain experts doing the analysis recall historical events or envision future situations that may lead to risks. During this case study, working with widget domain experts, the power of the technique was evident. The graphical nature and simplicity of the technique also made the results relatively easy to understand and review. As a result, reviewers were able to suggest additional risks that were triggered for them.

4.0 Case Study: Restarting Production of Widgets:

The case study used to illustrate an example of applying STPA for risk identification and management is contained in the remainder of this paper. The case study is the restarting of production of an item that has not been made for 30 years. This item is made by the government because it is high cost and uses materials that are hazardous. The materials needed to make the item (called a widget) has been in storage for 30 years.

The first step in performing STPA on this case study is to create a Hierarchal Control Structure Chart that depicts all the organizations involved in the decisions to produce the widgets. The Hierarchal

Control Structure Chart is shown in figure 11. Note that the chart indicates the control actions and feedback flowing between the various supervising and supervised entities. The entities are grouped as follows:

- Government
- Corporate
- Site
- Production
- Vendor

Creating the Hierarchal Control Structure Chart requires studying the organizations and organizational charts involved in the production of widgets. It required researching the staff involved and understanding the constraints and reports flowing between them. Creating the Hierarchal Control Structure Chart is an important part of doing the STPA for management analysis. It can also be one of the most time-consuming tasks. Drawing tools such as Visio can help automate the task and allow easier editing as new information becomes available.

For each of the five organizations named on the Hierarchal Control Structure Chart an Institutional Risk was created using the Institutional Risk spreadsheet shown in figures 2-5. The Institutional Risk number for each organization will be used in the Institutional Risk column on the Risk Spreadsheet.

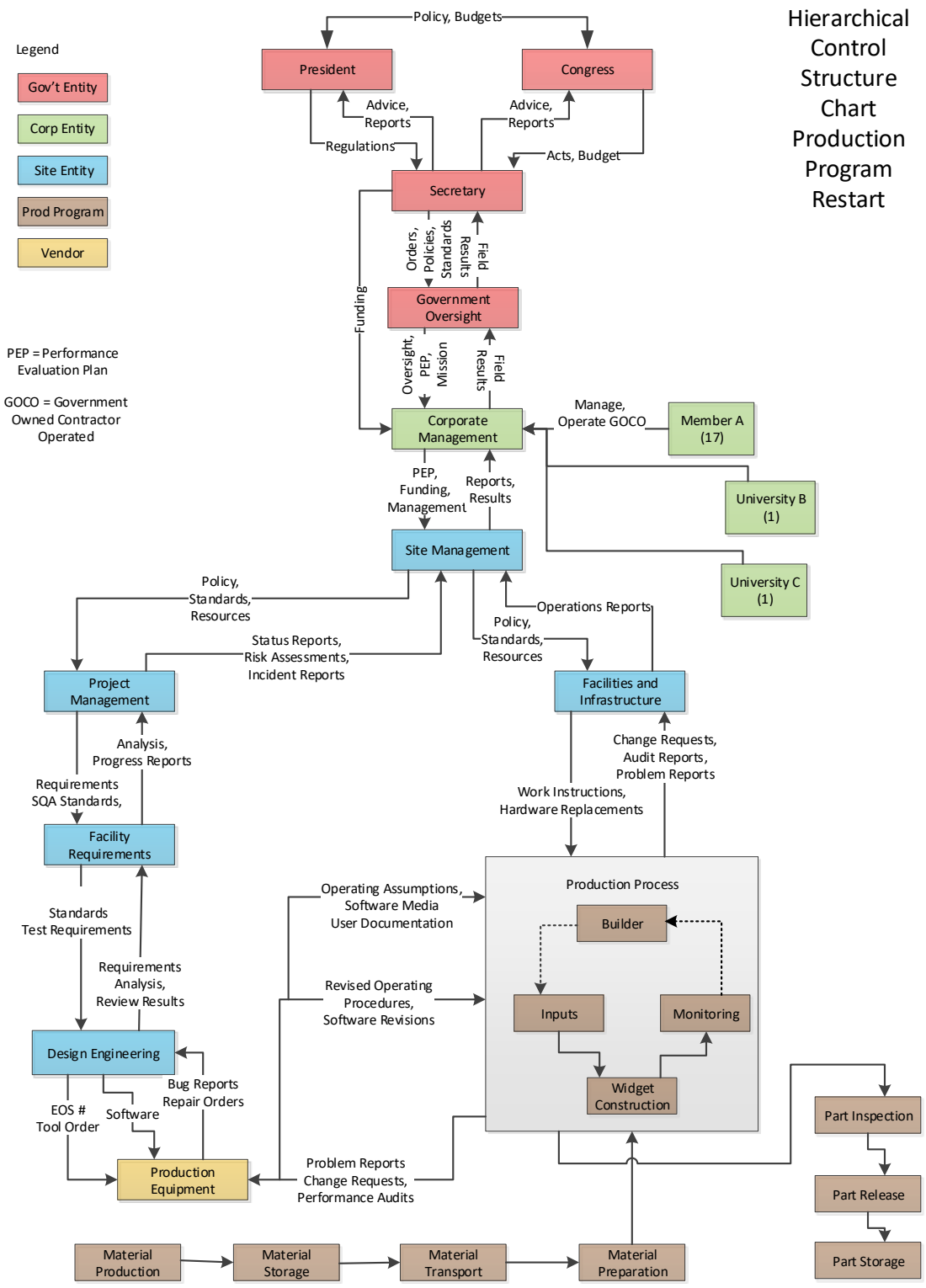

Figure 11 Widget Production Hierarchal Control Structure Chart

4.1 Government Entity Risks:

The STPA analysis was done on one entity grouping at a time. Starting top down with the government entity (figure 12). The relationships between the supervising and supervised entities are analyzed by asking the guide phrase questions about elements of management on the control actions path and the types of reports on the feedback path. Also considering the preconditions that might exist for the supervisor or supervisee entities. As a result of asking the questions possible risks emerge. The list of government risks has been enumerated with a GR prefix and sequential number to identify them. In this example analysis 10 risks are shown for the government sector with arrows pointing to the area where the risk was identified. Not all projects require government funding and oversight, however the case study does and lists some risks that could impact the success of the project because of government involvement.

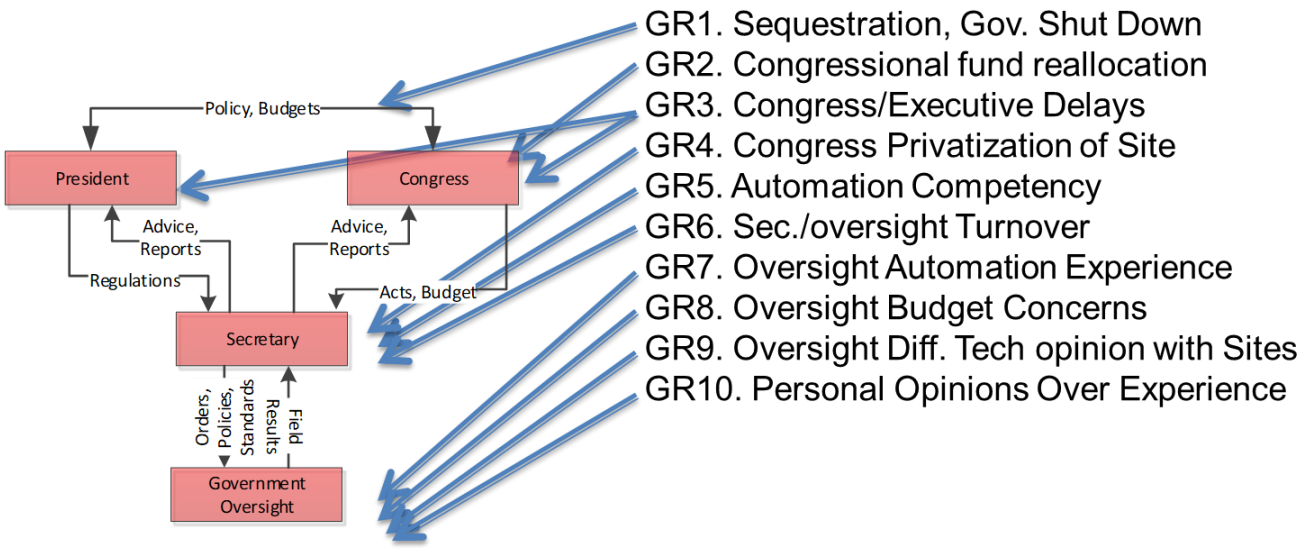

Figure 12 List of Government Risks

4.2 Government, Privatizing, Site Risks

In this case study the production is to be restarted at one (or more) of the government contractors' sites. These sites are managed by private corporations or holding companies consisting of multiple corporations and academic institutions (figure 13). The use of private for-profit entities managing the government contractor sites can be analyzed for risks using the same analysis technique applied to the government entity. The prefix for these six identified risks is GPSR.

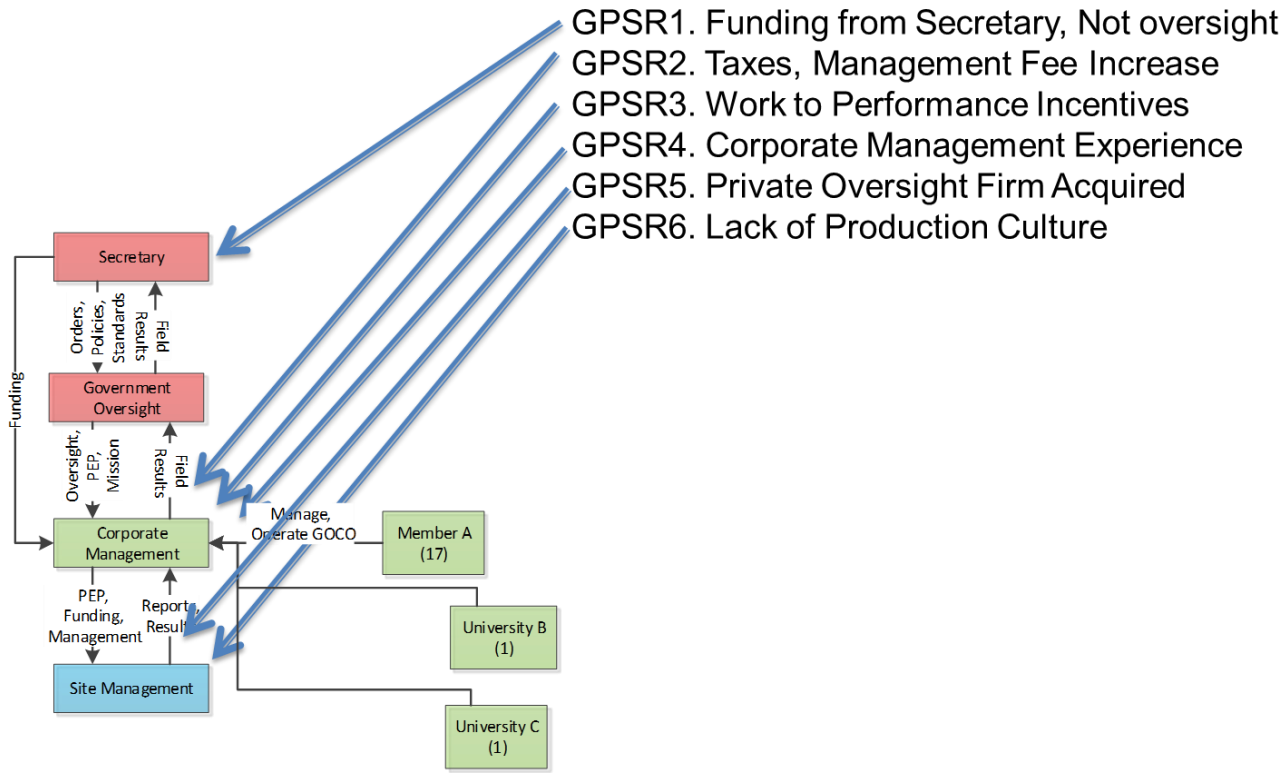

Figure 13 Government Privatization Risks

4.3 Site Management Risks:

The next entity analyzed for risks is the on-site management risks (figure 14). The five risks identified have the prefix SMR. So far, we have analyzed three distinct levels of management. The government is the top layer and provides the standards and orders for the contractor to follow. Corporations or holding companies consisting of multiple corporations manage each government owned site. Each site has its own set of managers who are responsible for all the different work going on at the site. At some sites the corporate managers are also the high-level site managers.

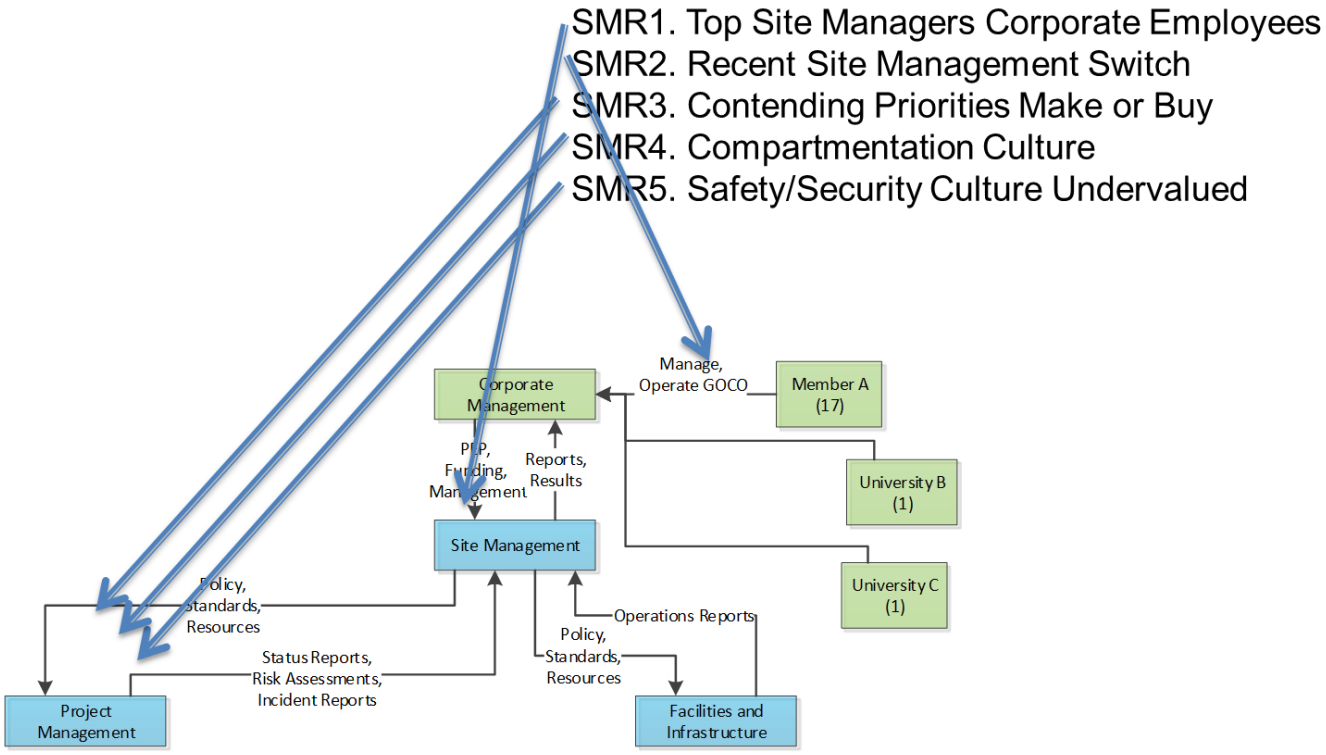

Figure 14 Site Management Risks

4.4 Development Risks:

The development risks (figure 15) are those associated with the project at the site that will be undertaking the restart of production of the widgets. This includes design and construction of the production facility and all the tools required to produce the widgets. The 12 risks associated with this activity have a DR prefix.

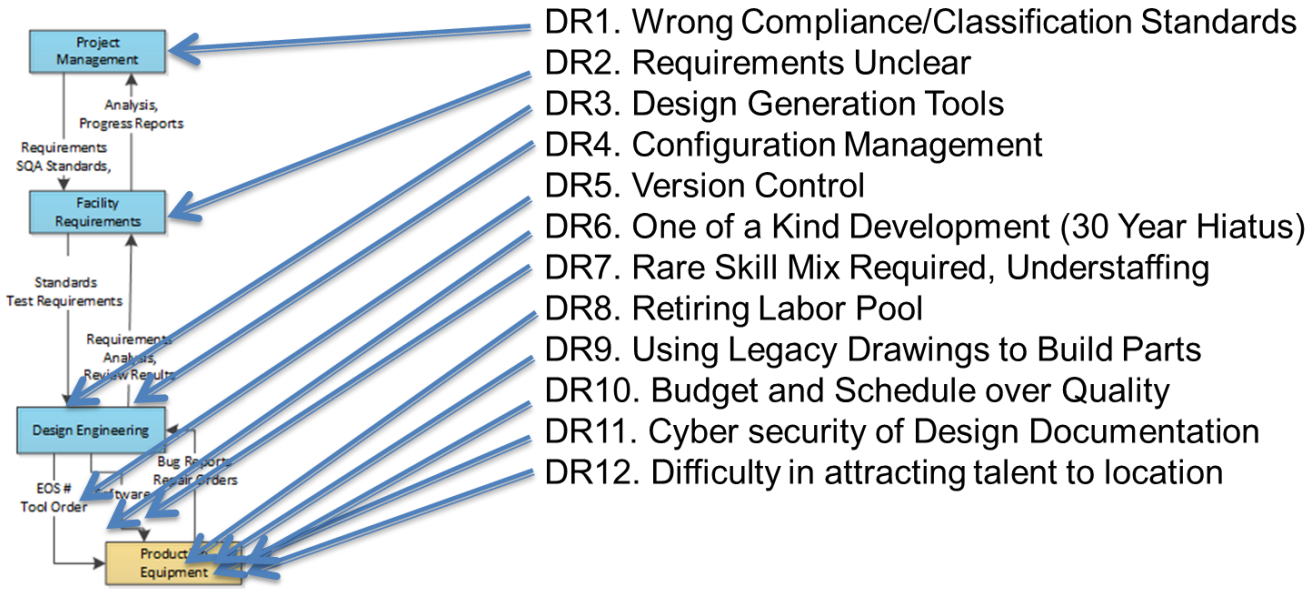

Figure 15 Development Risks

4.5 Production Risks:

The production risks (figure 16) are those associated with the widget production process. The list of 15 risks associated with the actual production have a PR prefix. This list of risks will be revisited and expanded as additional information becomes known about the production process and the tools that are used.

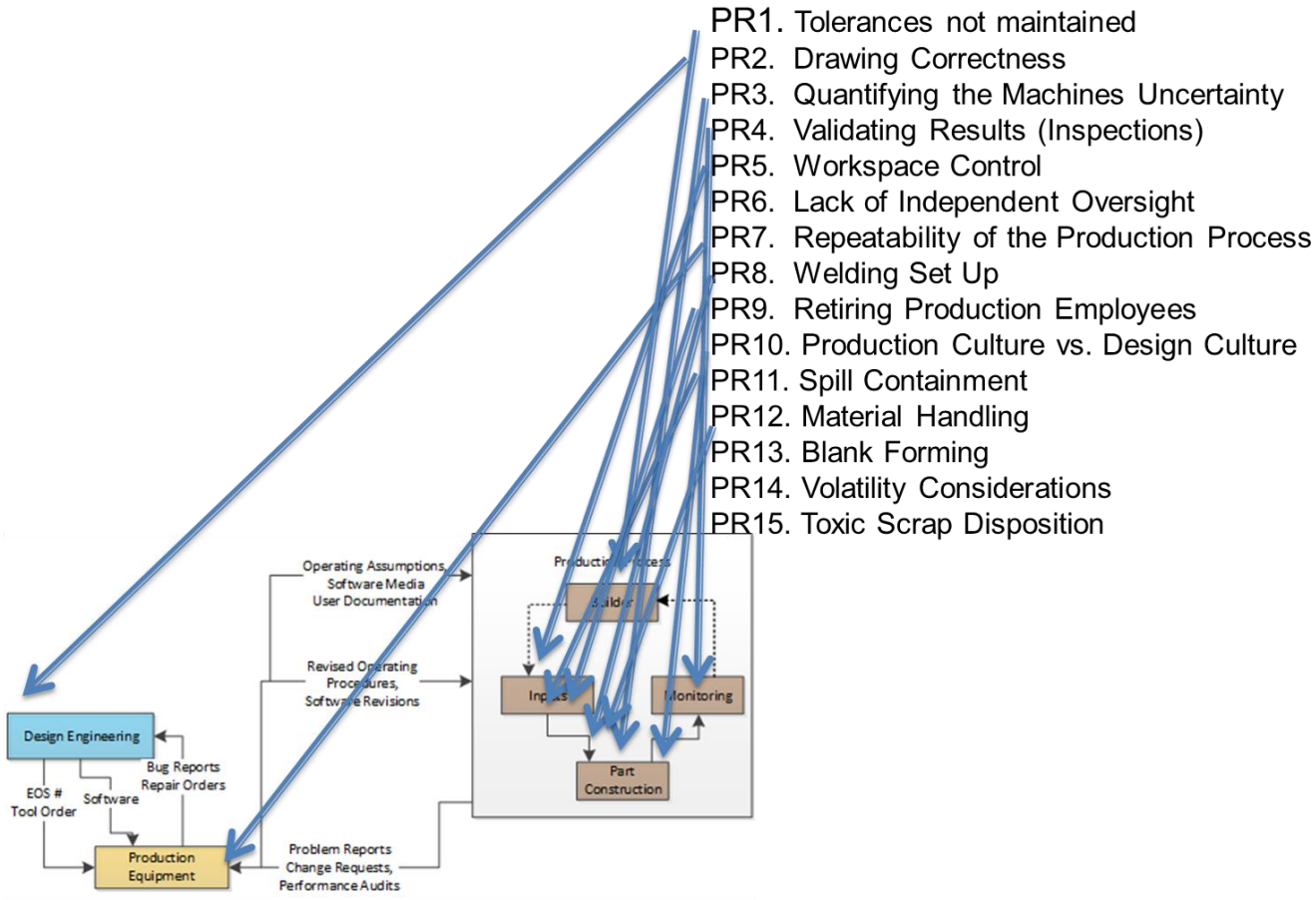

Figure 16 Production Risks

4.6 Material Handling Risks:

Material handling (figure 17) risks are those encountered when moving the widget raw material from long term storage to the production facility. The 8 risks listed assume the storage site for the raw material and the production site are not co-located so that the raw material must be transported to the production site. The prefix for the 8 material handling risks is MHR.

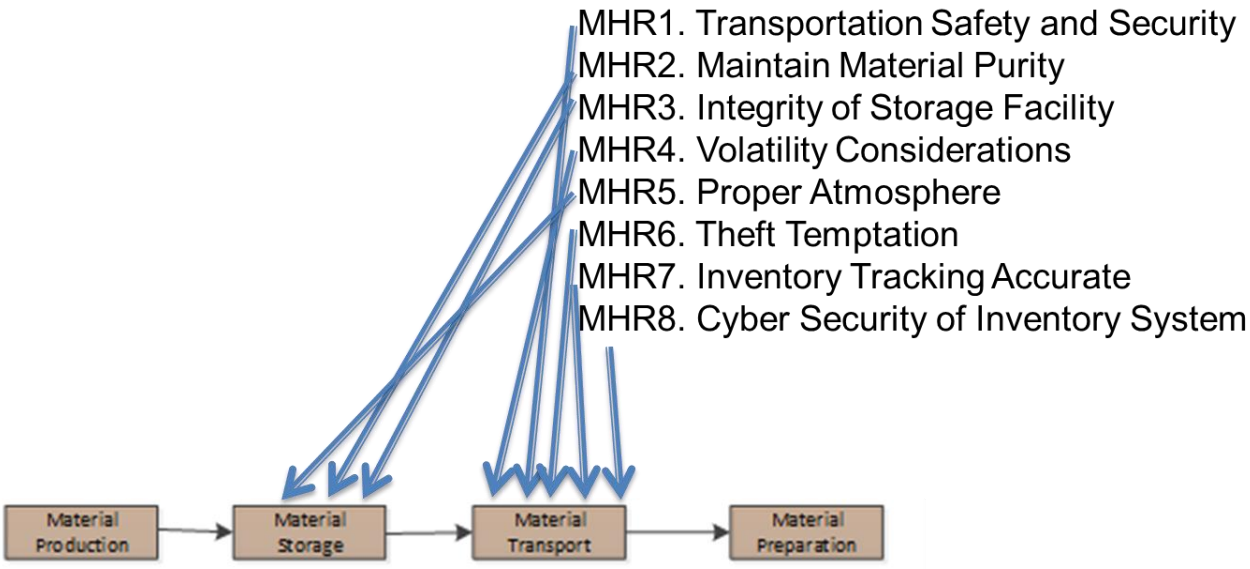

Figure 17 Material Handling Risks

4.7 Postproduction and Storage Risks:

The postproduction risks (figure 18 and storage include the disposition of the finished product and storage of finished goods. The 6 risks associated with this activity have a PPR prefix.

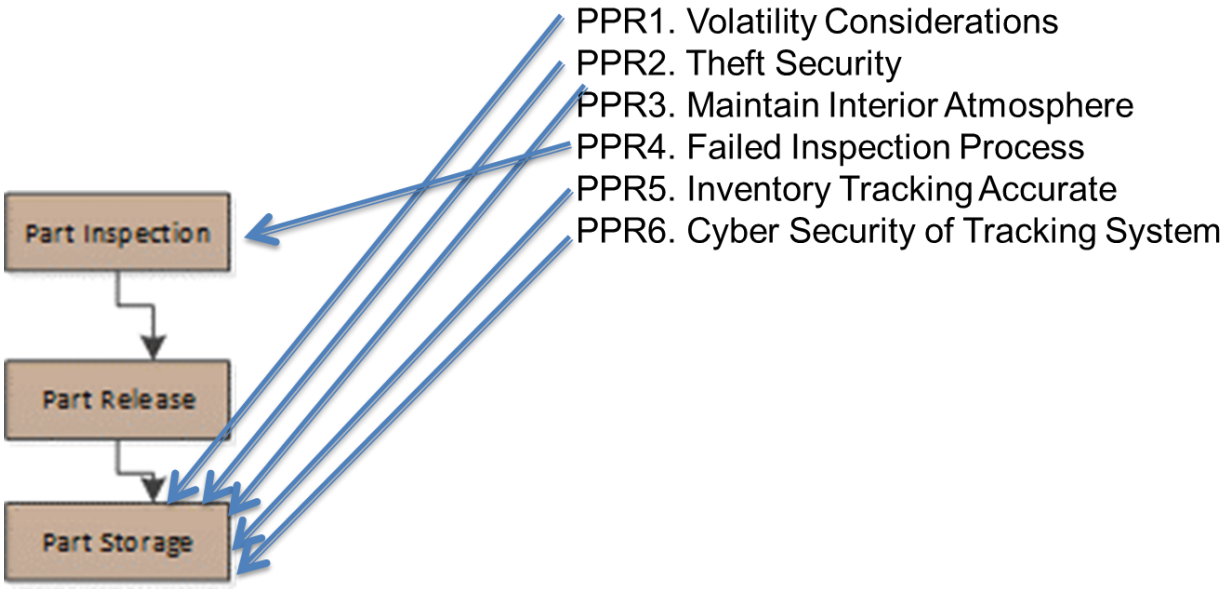

Figure 18 Postproduction and Storage Risks

4.8 Environmental Risks:

Environmental risks (figure 19) are external factors caused by naturally accruing events that could act upon the product facility. The list of 11 identified risks has the prefix ER.

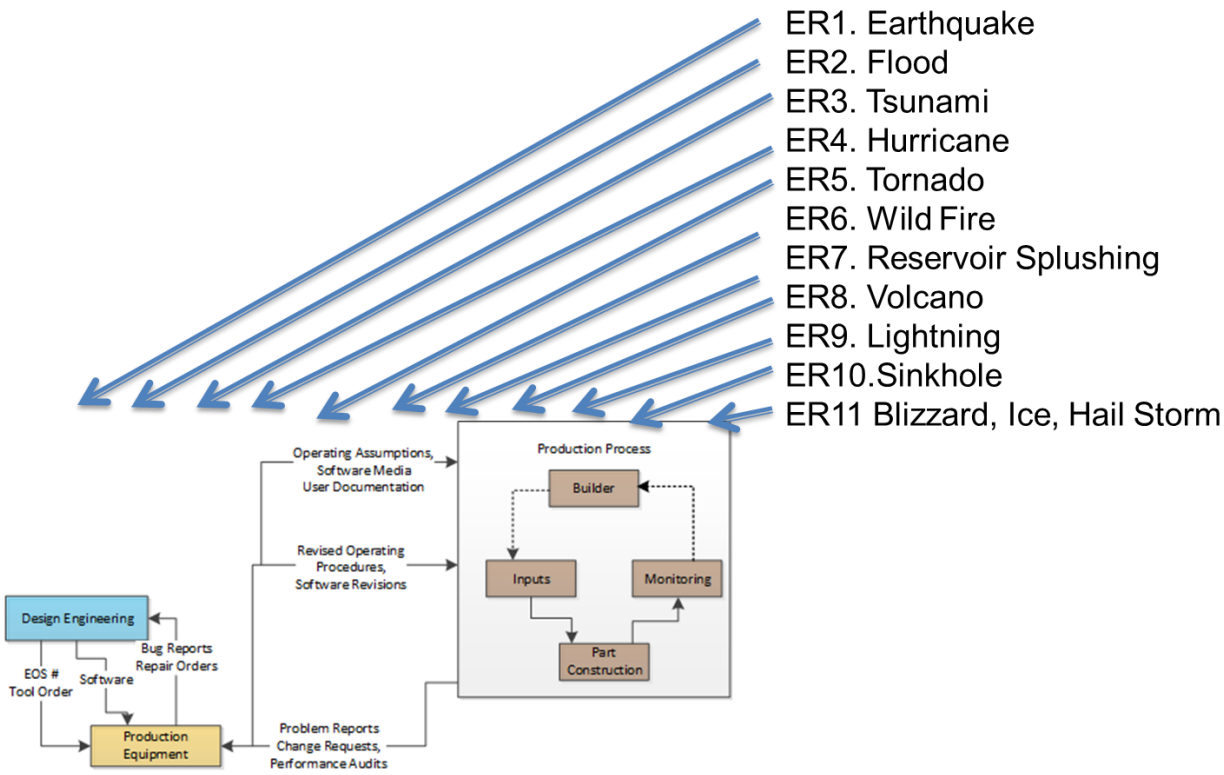

Figure 19 Environmental Risks

4.9 Human Generated Risks:

Human generated risks (figure 20) are forces that could act against the production facility that are caused by human actors with malicious intent or accidental malfunction. The 11 risks identified have the prefix HGR.

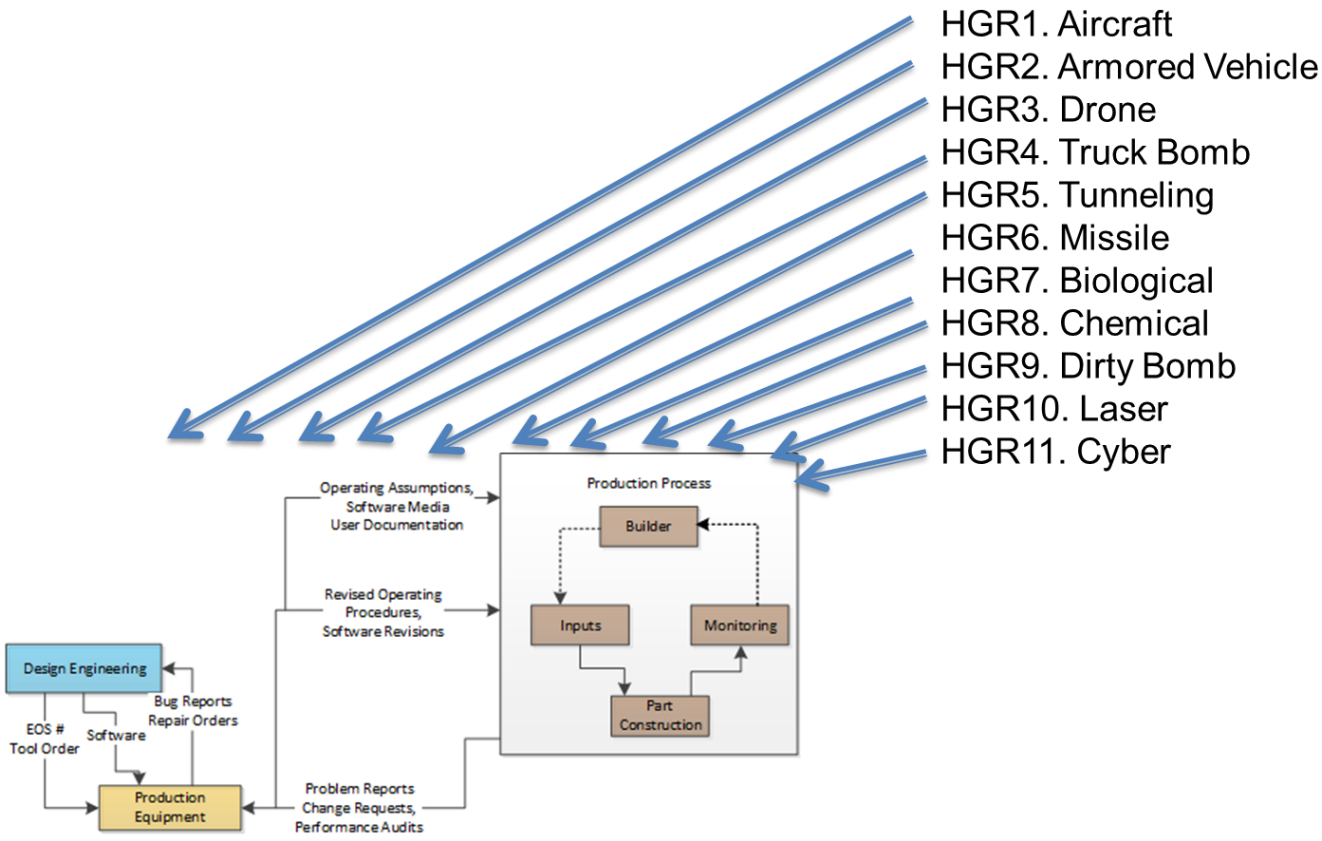

Figure 20 Human Generated Risks

5.0 Assessing the Identified Risks

The risks that have been identified using STPA are assessed and added to an Excel spreadsheet. Risks are identified by the prefix and risk numbers assigned in the identification process in chapter 4. A description is added to elaborate further on what could go wrong and cause the undesired outcome. The status of the risk is set to identified from the four choices described in chapter 2.3 using a pull-down menu. The magnitude of impact of the risk and Institutional risk (from figures 2-5) are selected via pull down menu from the choices described in chapter 2.2. The magnitude of the impact is also color coded:

- Magnitude of Impact
    - 5 -Public Safety - Red
    - 4 - Employee Safety - Orange
    - 3 - Financial Loss - Yellow
    - 2 - Delay - Light Green
    - 1 - Trivial –Green

The Risk Inference number (after using the Risk Inference Spreadsheet in figures 2-5) is selected using a pull-down menu of items from section 2.2 and is also color coded:

- Institutional Risk
    - 5 - Highest – Red
    - 4 – High - Orange
    - 3 - Moderate – Yellow
    - 2 – Low Light Green
    - 1 – Lowest – Dark Green

The risk score (1-25) is the product of the magnitude of impact (1-5) and institutional risk (1-5). The color coding for Risk score starts at dark green for lowest score and transitions to red for the highest scores. The risk response is selected from the 6 choices described in chapter 2.3. The last column on the risk management spreadsheet is the action to be taken on the identified risk. The most common action is to mitigate the risk and this column allows a description of what the mitigation action will be. The following chapters give examples of the risk management spreadsheet for the case study divided up by the same groupings used for analysis of the Hierarchal Process Structure Chart.

5.1 Government Entity Risks:

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
GR1.	Sequestration, Government Shut Down	Unexpected cessation of funds needed for widget production could cause shut down and start up modes that could add risk to safe operation. Also reduction in funds could impact safety measures as well	Identified	2 - Delay	3.05	6.1	Mitigate	Assure that widget production funding is not impacted by sequestration or interruptions in funding that is political in nature.
GR2	Congressional fund reallocation	Other congressional priorities could divert funds for widget production to other programs, reducing funding for widget production and impacting safety and schedule.	Identified	2 - Delay	3.05	6.1	Mitigate	Assure that widget production funding is not impacted by competing priorities or interruptions in funding that is political in nature..
GR 3	Congress/Executive Delays	Delays caused by the slow legislative process or inability to get required votes to pass required legislation could encourage unrealistically short schedules to compensate	Identified	2 - Delay	3.05	6.1	Mitigate	Assure that legislative or executive delays do not compromise schedules required to safely produce widgets.
GR4	Congress Privatization of Site	Privatization of sites for widget production creates the possibility that executives in charge of widget production do not have experience in widget production and will	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Assure private corporate executives include those with widget production experience and create advisory boards made up of retired employees who have lesson learned experience from previous production efforts.
GR5	Secretary Automation Experience	Reliance on modern production automation will require oversight with experience in areas such as CAD/CAM, robotics, software, networks, CM factory automation, etc.	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Select Secretary oversight employees that have experience in production methods used for widget production as well as domain expertise in widgets.
GR6	Secretary/Oversite Turnover	Employees with experience in widget production are retiring or no longer living or are hard to relocate to plant site.	Identified	2 - Delay	3.05	6.1	Mitigate	Interview experienced retirees and form advisory boards of experienced former employees to pass on relevant experience in widget production. Use simulation techniques to help train replacement employees.
GR7	Oversite Automation Experience	Reliance on modern production automation will require oversight with experience in areas such as CAD/CAM, robotics, software, networks, CM factory automation, etc.	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Select Oversite oversight employees that have experience in production methods used for widget production as well as domain expertise in widgets.
GR8	Oversite Budget Concerns	Funding cuts to Oversite may reduce ability to conduct comprehensive hazard analysis	Identified	2 - Delay	3.05	6.1	Mitigate	Assure Oversite or other agency will be supported adequately to oversee widget production.
GR9	Oversite Differing Technical Opinion With Sites	Oversite and site may not be able to compromise on solutions and encourage lack of transparency.	Identified	2 - Delay	3.05	6.1	Mitigate	Assure Oversite oversight personnel are experienced in the areas they are assessing.
GR10	Personal Opinions Over Experience	Decisions are made based on organizational hierarchy of the decider rather than taking into account experience of lower level employees.	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgets, schedule, or procedural decisions.

5.2 Government, Privatizing, Site Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
GPSR1	Funding from Secretary, Oversight from Oversite	Opposed priorities for widget production. For instance Secretary is schedule and budget driven, Oversite is safety driven leading to bureaucratic delays.	Identified	2 - Delay	3.05	6.1	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.
GPSR2	Taxes and Management Fee Increase	Corporate oversight are for profit companies and therefore subject to taxes. Additional risk of widget production may cause increases in management fees.	Identified	2 - Delay	3.05	6.1	Mitigate	Plan for increased management fees in future budgets.
GPSR3	Work to Performance Incentives	If management oversight is tied to performance bonuses and If this extends to widget production it could influence site management to take risks to receive bonuses.	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Tie incentives to safe operations rather than just schedule and budget performance.
GPSR4	Corporate Management Experience	Corporations that manage site may not have experience in widget production or a production culture.	Identified	4 - Employee Safety	3.05	12.2	Mitigate	Assure site oversight management has experienced widget production staff.
GPSR5	Private Oversight Firm Acquired	Oversight firm could be acquired or go out of business during widget production, if acquired the new management may not be experienced in widget	Identified	2 - Delay	3.05	6.1	Monitor	Stipulate that any changes in site management companies must be requalified before being allowed to continue.
GPSR6	Lack of Production Culture	The chosen widget production site must have experience in production and a production culture.	Identified	2 - Delay	3.05	6.1	Mitigate	Assure that site management includes experienced production managers and key employees with experience in products similar to widgets.

5.3 Site Management Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
SMR1	Top Site Managers Corporate Employees	Corporate Management experience may not be in widget production.	Identified	4 - Employee Safety	2.40	9.6	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.
SMR2	Recent Site Management Switch	Corporate Management is new to this site.	Identified	2 - Delay	2.40	4.8	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.
SMR3	Contending Priorities Make or Buy	Widget production equipment not available on commercial market may require special fabrication by a vendor or built by site.	Identified	2 - Delay	2.40	4.8	Mitigate	For vendor built equipment for manufacturing assure rigorous vendor qualification process.
SMR4	Compartmentation Culture	The site may have siloed departments that are not accustomed to working together. For example design and production.	Identified	2 - Delay	2.40	4.8	Mitigate	Organize the widget production into multi-disciplined teams so that design and production can work together to optimize production.
SMR5	Safety/Security Culture Undervalued	The site may not have a strong safety culture required for the production of widgets.	Identified	5 - Public Safety	2.40	12	Mitigate	Supply training and create processes that embrace safety as the primary priority. Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.

5.4 Development Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
DR1	Wrong Compliance /Classification Standards	Existing current standards may not appropriately cover production of widgets.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Assure that appropriate existing and legacy widget making standards and classification guides are followed using training along with oversight audits and assessments for compliance to the standards.
DR2	Requirements Unclear	Lack of recent experience in widget production leads to unclear requirements for production facility or processes or staff.	Identified	2 - Delay	2.15	4.3	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.
DR3	Design Generation Tools	New tools designed for widget production do not function as desired.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Plan for significant time to test and evaluate new tools prior to use in production.
DR4	Configuration Management	Design software for new widget production tools contains errors or security vulnerabilities.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Protect design software from network intrusions, place tool design under configuration management.
DR5	Version Control	Errors or vulnerabilities in tool design software not updated.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Assure tool software updates to fix vulnerabilities are accomplished and retest is performed.
DR6	One of a Kind Development	Tools needed for widget production may not be available from commercial vendors.	Identified	2 - Delay	2.15	4.3	Mitigate	Qualify commercial tools or software for designing tools for widget production prior to use. Limit sources of commercial tools to trusted and qualified vendors.
DR7	Rare Skill Mix Required, Understaffing	Skills needed to produce widgets are rare and require extensive training and experience.	Identified	2 - Delay	2.15	4.3	Mitigate	Identify sources of qualified widget production skills and recruit them for widget production.
DR8	Retiring Labor Pool	Staff with widget production skills have retired or are retiring soon or hard to attract to location of production plant	Identified	2 - Delay	2.15	4.3	Mitigate	Offer incentives for retired widget production workers to re enter the work force.
DR9	Using Legacy Drawings to Build Parts	Legacy drawings for building widgets may contain errors or be hard to interpret.	Identified	2 - Delay	2.15	4.3	Mitigate	Allow time to make corrections or improve quality of legacy drawings for widget parts.
DR10	Budget and Schedule over Quality	Pressure on production to meet schedule milestones or budget constraints may create unrealistic deadlines or resource constraints.	Identified	2 - Delay	2.15	4.3	Mitigate	Keep safety and quality as the top priority, relegating cost and schedule to secondary considerations.
DR11	Cyber security of Design Documentation	Electronic forms of design documentation susceptible to cyber theft.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Assure electronic documentation is air gapped to public networks and use biometric identification to minimize insider threat.
DR12	Difficulty in Attracting talent to location.	Location may be in rural area without access to labor supply or industries needed to support needed technologies and skills	Identified	2 - Delay	2.15	4.3	Mitigate	Assure electronic documentation is air gapped to public networks and use biometric identification to minimize insider threat.

5.5 Production Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
PR1	Tolerances not maintained	Exacting tolerances for fabrication not met, such as welding tolerances.	Identified	2 - Delay	2.15	4.3	Mitigate	Routine maintenance and periodic calibrations performed when required enforced with oversight.
PR2	Drawing Correctness	Legacy drawings contain errors, are hard to read, or errors induced when updated to electronic media.	Identified	3 - Financial Loss	2.15	6.45	Move	Verify and validate independently the original prints used against reproductions or digitization's.
PR3	Quantifying the Machines Uncertainty	Machinery used for production not able to meet required production tolerances.	Identified	2 - Delay	2.15	4.3	Move	Independently verify machine tool tolerances meet or exceed required tolerances.
PR4	Validating Results (Inspections)	In process inspections fail to catch errors.	Identified	3 - Financial Loss	2.15	6.45	Move	Provide independent inspections during production runs and independent sampling and test.
PR5	Workspace Control	Workspace access not restricted to qualified employees or workspace environment not conducive to worker focus.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Provide appropriate physical plant security in depth. Allow any production employee to call a stop work.
PR6	Lack of Independent Oversight	Oversight is not impartial or independent.	Identified	2 - Delay	2.15	4.3	Move	Oversight provided by entity that is not under the influence of the production site.
PR7	Repeatability of the Production Process	Production tools wear out or tolerances drift off over time.	Identified	2 - Delay	2.15	4.3	Move	Independently verify machine tool tolerances meet or exceed required tolerances. Replace equipment before end of life..
PR8	Welding Set Up	Welding set up not done correctly causing production widgets to be defective.	Identified	2 - Delay	2.15	4.3	Mitigate	Provide training for welders, consider some or all of the welding be done using automated techniques to improve repeatability.
PR9	Retiring Production Employees	Scarce labor pool of qualified production workers.	Identified	2 - Delay	2.15	4.3	Mitigate	Provide salaries and benefits to attract and maintain top talent. Provide specialized training for widget welding.
PR10	Production Culture vs. Design Culture	Production and design sites not collocated or production lessons learned not able to influence design.	Identified	2 - Delay	2.15	4.3	Mitigate	Collocate design and production facilities.
PR11	Spill Containment	Hazards during production of widgets are not confined to production area.	Identified	2 - Delay	2.15	4.3	Mitigate	Provide a work environment which contains hazardous materials or atmosphere to strictly controlled enclosures or work areas.
PR12	Material Handling	Material is damaged during handling.	Identified	2 - Delay	2.15	4.3	Mitigate	Create a production culture where reporting defects is rewarded and encouraged.
PR13	Raw Material Forming	Raw material not formed in a way that is useful for widget production.	Identified	2 - Delay	2.15	4.3	Mitigate	Assure incoming inspection can detect defects in material form and construction.
PR14	Volatility Considerations	During production the materials become volatile.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Provide a work environment which contains hazardous materials or atmosphere to strictly controlled enclosures or work areas.
PR15	Toxic Scrap Disposition	Scrap material from production not disposed of properly.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Assure inventory tracking of scrap material and safe disposal of hazardous scrap.

5.6 Material Handling Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
MHR1	Transportation Safety and Security	Widget raw material is spilled, damaged, or stolen during transportation to production site.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Provide secure transportation and accountability for materials from departure to arrival.
MHR2	Maintain Material Purity	Widget raw material has been degraded in storage and is not suitable for widget production.	Identified	2 - Delay	2.15	4.3	Mitigate	Provide comprehensive incoming material inspection prior to use in widget production.
MHR3	Integrity of Storage Facility	The widget raw material storage facility has lost or misplaced widget raw material.	Identified	5 - Public Safety	2.15	10.75	Move	Assign to law enforcement to investigate missing raw materials
MHR4	Volatility Considerations	The widget raw material storage facility has stored raw material in a way that has allowed it to become volatile.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Assure storage of widgets is monitored and done following a safe method.
MHR5	Proper Atmosphere	The widget raw material must be transported by a conveyance that maintains a proper environment for the raw materials	Identified	5 - Public Safety	2.15	10.75	Mitigate	Widget materials must retain their integrity in the most severe accident conditions, including high impacts, explosion, and fire for air, land, or sea transport.
MHR6	Theft Temptation	Widget raw material is stolen during movement to production site.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Comply with transportation requirements, provide secure transportation method.
MHR7	Inventory Tracking Accurate	Widget raw material is unaccounted for, the inventory records do not agree with physical inventory.	Identified	5 - Public Safety	2.15	10.75	Move	Employ independent audit to determine cause, involve law enforcement if appropriate.
MHR8	Cyber Security of Inventory System	The widget raw material inventory system has been compromised by a cyber security incident.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Network and software inventory control systems are air gapped to the internet and multiple authentication is required internally.

5.7 Postproduction and Storage Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
PPR1	Volatility Considerations	Widgets become volatile during storage or while being transported.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Widget quantity and packing density controlled in storage and transport.
PPR2	Theft Security	Widgets are stolen during storage or transportation after production.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Physical plant security must control access to storage facility and provide adequate transportation security resources.
PPR3	Maintain Interior Atmosphere	Widgets damaged during storage.	Identified	2 - Delay	2.15	4.3	Mitigate	Controlled storage environment must have power and other resource backup to maintain environment in case of power outage, act of nature, or national emergency.
PPR4	Failed Inspection Process	Widgets that fail inspection are not disposed of or reprocessed safely.	Identified	5 - Public Safety	2.15	10.75	Mitigate	Plans for safe disposal of scrap materials and / or reprocessing of materials not passing inspections must assure public and worker safety.
PPR5	Inventory Tracking Accurate	Inventory tracking system Secretary's not include features required for safe movement and storage of widgets.	Identified	2 - Delay	2.15	4.3	Mitigate	Assure features for safe storage and movement of finished goods are included in tracking system.
PPR6	Cyber Security of Tracking System	The tracking system used to keep track of widget inventory must not be vulnerable to cyber attack.	Identified	2 - Delay	2.15	4.3	Mitigate	Air gap deployed inventory tracking system to outside world. Provide inside authentication that relies on biometric information.

5.8 Environmental Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
ER1	Earthquake	Production facility is located on or near fault or fracking area. Large earthquake occurs. Power outage	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Production facilities located in two geographical locations, one is located near a known fault, so construcution must assume a Mag 7.5 earthquake.
ER2	Flood	Flooding conditions occur and over whelm production facility including loss of power.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations, neighter located in a flood plain.
ER3	Tsunami	As a result of a natural event a Tsunami occurs flooding shoreline areas.	Unassigned	4 - Employee Safety	2.15	8.6	Mitigate	Production facilities located in two geographical locations. Locations are not near a coastal area below 250 ft elevation level.
ER4	Hurricane	Hurricane force winds are encountered at production site.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations. Production facilities can withstand Cat 5 winds.
ER5	Tornado	Production plant is in the path of a tornado..	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations. Production facilities can withstand Cat 5 winds.
ER6	Wild Fire	Production plant is in the path of a wild fire bring out of control.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations. Production facilities in forested areas. Fire breaks put in to stop wildfires from reaching plant.
ER7	Reservoir Splushing	Reservoir near production plant is spills water out due to landslide or earthquake or failed dam.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations. Production facilities not located below elevation of reservoirs.
ER8	Volcano	Volcano is area of production plant spews ash and lava towards production plant.	Unassigned	3 - Financial Loss	2.15	6.45	Mitigate	Production facilities located in two geographical locations.Neigher is in active volcano region.
ER9	Thunder Storms	Lightening strike hits production plant	Identified	2 - Delay	2.15	4.3	Mitigate	Production facilities located in two geographical locations. Facilities have lightening strike protection.
ER10	Sinkhole	Sinkhole form at of near production facility	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Production facilities located in two geographical locations. Facilities not located near sinkhole activity.
ER11	Blizzards, Ice, Hail Storm	Severe snow, ice, hail occur at product plant location	Identified	2 - Delay	2.15	4.3	Mitigate	Production facilities located in two geographical locations. Facility protected from extreme weather conditions. Power back up and life sustaining provisions provided.

5.9 Human Generated Risks

	Risk	Description	Status	Magnitude of Impact	Institutional Risk	Risk Score	Risk Reponses	Mitigation Actions
HGR1	Aircraft	Aircraft accidently or deliberately crashes into production facility. Helicopter tries to land in production facility.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Production facility located in structure or underground that can withstand direct hit of aircraft.
HGR2	Armored Vehicle	Armored vehicle attempts to enter production facility	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Perimeter of production plant protected by crash proof barriers to keep unauthorized vehicles from gaining close proximity to plant.
HGR3	Drone	Unmanned aircraft is flown over or into production plant	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Drone detection and disabling technologies deployed at production site.
HGR4	Truck Bomb	Vehicle with large explosives is detonated at or near production plant.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Perimeter of production plant protected by crash proof barriers to keep unauthorized vehicles from gaining close proximity to plant.
HGR5	Tunneling	A tunnel is constructed under the production plant as a way to gain entry	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Tunnel detection measures used to prevent tunnels in proximity of production plant.
HGR6	Missile	A shoulder launched or aircraft launched missile is fired at the production plant	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Production facility located in structure or underground that can withstand direct hit of missile.
HGR7	Biological	A pathogen is used to contaminate the production plant.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Pathogen detection devices deployed at production facility.
HGR8	Chemical	A toxic chemical is used to contaminate the production plant	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Chemical warning devices deployed at production facility.
HGR9	Dirty Bomb	A dirty bomb releases radiation at of near the production plant	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Radiation detection devices deployed at production facility.
HGR10	Laser	A laser device is used against the production facility to gain entry or disable surveillance cameras.	Identified	4 - Employee Safety	2.15	8.6	Mitigate	Production facility located in structure or underground that can withstand direct hit of laser.
HGR11	Cyber	Hacker is able to modify software, exploit vulnerability, find backdoor.	Identified	3 - Financial Loss	2.15	6.45	Mitigate	All software used at plant is checked for exploitable vulnerabilities, checked against National vulnerability Database, air gapped to internet.

6.0 Example Major Risks

An example set of major risks is shown by taking the highest risk scores. The highest risk scores occur in the Government Risks section (12.2), Government, Privatization of Sites Risk (12.2), Site Management (12), Production (10.75), Postproduction (10.75), and Material Handling Risks (10.75). Some examples below are:

LLNL-CONF-812813

1. GR4: Privatization of sites for widget production creates the possibility that executives in charge of widget production do not have experience in widget production and will make poor decisions in leading widget production efforts.

2. GR5 and GR7: Reliance on modern production automation will require oversight with experience in areas such as CAD/CAM, robotics, software, networks, CM factory automation, etc. which may be scarce in the government sector.

3. GPSR3: If management oversight is tied to performance bonuses and if this extends to widget production it could influence site management to take risks to receive bonuses. Widget raw material is spilled, damaged, or stolen during transportation to production site.

4. GPSR4: Corporations that manage site may not have experience in widget production or a production culture.

5. MHR3: The widget raw material storage facility has lost or misplaced widget raw material.

7.0 Example Risks by Category

This example set of risks contain a top risk from each risk category.

1. GR4 - Privatization of sites for widget production creates the possibility that executives in charge of widget production do not have experience in widget production and will make poor decisions in leading widget production efforts (12.4).
2. GPSR3 – If management oversight is tied to performance bonuses and this extends to widget production it could influence site management to take risks to receive bonuses (12.2).
3. SMR5 - The site may not have a strong safety culture required to produce widgets (12).
4. DR3 - New tools designed for widget production do not function as desired (8.6).
5. PR15 – Scrap material from production not disposed of properly (10.75).
6. MHR1 - Widget raw material is spilled, damaged, or stolen during transportation to production site (10.75).
7. PPR1 - Widgets become volatile during storage or while being transported (10.75).
8. ER1 - Production facility is located on or near fault or fracking area. Large earthquake occurs and power outage (8.6).
9. HGR1 - Aircraft accidently or deliberately crashes into production facility. Helicopter tries to land in production facility (8.6).

LLNL-CONF-812813

8.0 Remaining Work

This white paper is a first attempt to utilize STPA for Risk Identification and Management. It is not a complete and thorough analysis but instead a start and template to use to do further analysis. The analysis did identify risks which were not present 30 years ago. For instance, the widespread availability of drones, use of large tunnel networks for smuggling, cyber security attacks, and the popularity of gas and oil fracking and its effects on geologic stability. To finish this analysis, at a minimum, the following four steps should be taken. SME refers to subject matter experts in widget production, storage, transportation, and handling.

1. Additional SME review of Hierarchical Structure Chart
2. Additional SME review of identified risks
3. Additional SME review of risk magnitudes and probability of occurrence
4. Additional SME review of mitigations

9.0 STPA Summary

There are hazard analysis techniques which have been successfully used in the past for making widgets. STPA for management is a contemporary hazard analysis technique which focuses on risks derived from the organization structures and interactions. It did not exist 30 years ago. Since no hazard analysis technique can prove that it has identified all hazards, using as many techniques as practical may be the best solution. Therefore, STPA can be used to enhance legacy hazard analysis techniques. In the research conducted for this white paper no previous risk identification process used analysis of organizational interaction as a source of risks. However, as we study past accidents and apply lessons learned from them, we find that organizational structure and interactions can play a major role in creating risks that may not be detectable when individual components of the system are analyzed separately.

As part of the research and review process for this white paper the risk presentation was shown to widget experts and hazard analysis experts. Their consensus was that the STPA technique does produce useful results and is relatively easy to review.

A partial review of the previous version of this case study by Nancy Leveson pointed out several terminology errors that have been corrected. Also, that the use of history to determine likelihood of future events was a flawed approach, so the case study was revised to incorporate institutional risk. As a result of using institutional risk in lieu of likelihood, risks are more driven by consequence of the undesired event.

10.0 Appendix A: Example Question Matrix

	Supervisor Inadaquate control action			Supervisor Beliefs		
1	Planning	Constraint not Given	21	Control Algorithm	influenced by	Training
2	Planning	Constraint is Incorrect	22	Control Algorithm	influenced by	Experience
3	Planning	Constraint is Too Late	23	Control Algorithm	influenced by	Communication
4	Planning	Constraint is too long or too short	24	Control Algorithm	influenced by	Orientation
5	Organizing	Constraint not Given	25	Control Algorithm	influenced by	Health
6	Organizing	Constraint is Incorrect	26	Control Algorithm	influenced by	Attitude
7	Organizing	Constraint is Too Late	27	Mental Model	influenced by	Training
8	Organizing	Constraint is too long or too short	28	Mental Model	influenced by	Experience
9	Staffing	Constraint not Given	29	Mental Model	influenced by	Communication
10	Staffing	Constraint is Incorrect	30	Mental Model	influenced by	Orientation
11	Staffing	Constraint is Too Late	31	Mental Model	influenced by	Health
12	Staffing	Constraint is too long or too short	32	Mental Model	influenced by	Attitude
13	Directing	Constraint not Given				
14	Directing	Constraint is Incorrect				
15	Directing	Constraint is Too Late				
16	Directing	Constraint is too long or too short				
17	Controlling	Constraint not Given				
18	Controlling	Constraint is Incorrect				
19	Controlling	Constraint is Too Late				
20	Controlling	Constraint is too long or too short				

	Supervisee Inadaquate feedback			Supervisee Beliefs		
33	Written Report	Not Given	49	Control Algorithm	influenced by	Training
34	Written Report	Incorrect	50	Control Algorithm	influenced by	Experience
35	Written Report	Too Late	51	Control Algorithm	influenced by	Communication
36	Written Report	too long or too short	52	Control Algorithm	influenced by	Orientation
37	Verbal Report	Not Given	53	Control Algorithm	influenced by	Health
38	Verbal Report	Incorrect	54	Control Algorithm	influenced by	Attitude
39	Verbal Report	Too Late	55	Mental Model	influenced by	Training
40	Verbal Report	too long or too short	56	Mental Model	influenced by	Experience
41	Direct Observation	Not Given	57	Mental Model	influenced by	Communication
42	Direct Observation	Incorrect	58	Mental Model	influenced by	Orientation
43	Direct Observation	Too Late	59	Mental Model	influenced by	Health
44	Direct Observation	too long or too short	60	Mental Model	influenced by	Attitude
45	Indirect Observation	Not Given				
46	Indirect Observation	Incorrect				
47	Indirect Observation	Too Late				
48	Indirect Observation	too long or too short				

11.0 End Notes

[1] GIlb, Tom. 1988, *Principles of Software Engineering Management*, Workingham, England; Addison-Westley.
[2] Nancy G. Leveson, *Engineering a Safer World*, MIT Press (2012)
[3] Bowander, B, "An Analysis of the Bhopal accident".page 166, **Project** Appraisal, volume 2, number 3, September 1987, pages 157-168. Beech Tree Publishing, 10 Watford Close, Guildford, Surrey GUl 2EP, England.
[4] Lance Spitzner, "The Congressional Report on Equifax Hack", page 1, SANS Security Awareness. December 17, 2018
[5] https://en.wikipedia.org/wiki/Risk Def 3. The probability of something happening multiplied by the resulting cost or benefit if it does. (This concept is more properly known as the 'Expectation Value' or 'Risk Factor' and is used to compare levels of risk)
[6] Nancy Leveson: Without a crystal ball, nobody can know the risk of something happening in the future.

- Most risk estimates are based on past performance. But technology is changing rapidly. The past use of different systems doing the same thing may not be a good predictor of the future. So, where do we get the estimates from?
- Most software is brand new in each case. Even reused software is used in different environments. The safety of software is only a relevant concept with respect to the controlled system and the environment. Both change over time, which is why software that has executed safely in hundreds or thousands of cases suddenly causes an accident, think of the reused Ariane 4 software in the Ariane 5. This is not an unusual case.

They are not "determining" anything. At best they are estimating future risk. A less charitable wording would be that they are "guessing" the risk.

[7] Leveson and Thomas, STPA Handbook, 2018, page 9
[8] Leveson and Thomas, STPA Handbook, 2018, page 22
[9] Koontz and Weihrich, "Essentials of Management", page 26 Tata McGraw-Hill Publishing Company Limited, 7 West Patel Nager, New Delhi, copyright 2007, ISBN 978---07-062030-8
[10] Accident Report NTSB/AAR-14/01 PB2014-105984, Descent Below Visual Glidepath and Impact With Seawall, Asiana Airlines Flight 214, Boeing 777-200ER, HL7742 San Francisco, California, July 6, 2013.

LLNL-CONF-812813