Risk Management Using STPA Restarting Widget Production – V2.0

Virtual STAMP Workshop, MIT July 28th, 2020

Gregory Pope CSQE

Lawrence Livermore National Laboratory

LLNL-PRES-LLNL-PRES-812730

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

Background

- ✓ Government would like to restart the production of widgets which have not been produced for 30 years.
- ✓ Could STPA be useful for identification of risks on the production restart ?

Can the Risk Prediction process be improved?

Typical Risk Management Process

1. Identify the Risk
2. Assess the Risk
3. Develop Reponses to the Risk
4. Develop Contingency Plan, Preventive Measures

Identifying Risk

1. Brainstorming
2. Interviews (SMEs, Stakeholders)
3. Similar Projects (Historical Records, Lessons Learned)
4. Diagramming Techniques (Fish Bone, What if, Pictorial Modeling)
5. Risk Identification Checklist
6. STPA (Systemic Theoretic Process Assessment) ?

Assess the Risk

- Magnitude of Impact Detection/Effectiveness
  - Public Safety
  - Worker Safety
  - Financial Loss
  - Delay
  - Trivial

- Probability of Occurrence
  - Multiple
  - Infrequent
  - Not Yet

This is the area where improvement is needed.

Why?

- Traditional (consequence x likelihood) to quantify risk.
- Likelihood traces back to reliability failure rates for mechanical, electrical, and likelihood of environmental events. May still be useful there.
- Management may feel more comfortable with numbers.
- The likelihood of MS Power Point failing now is 10^{-7}.

Your PC ran into a problem that it couldn't handle, and now it needs to restart.

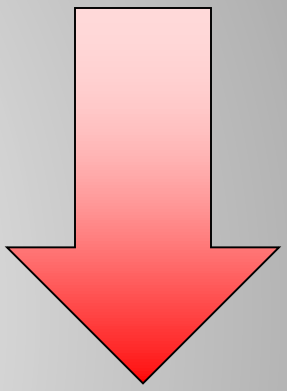
You can search for the error online: HAL_INITIALIZATION_FAILED

Software Controls Many Systems

- Software does not wear out
- If statement not limited to number of decisions
- Loops not limited to number of iterations

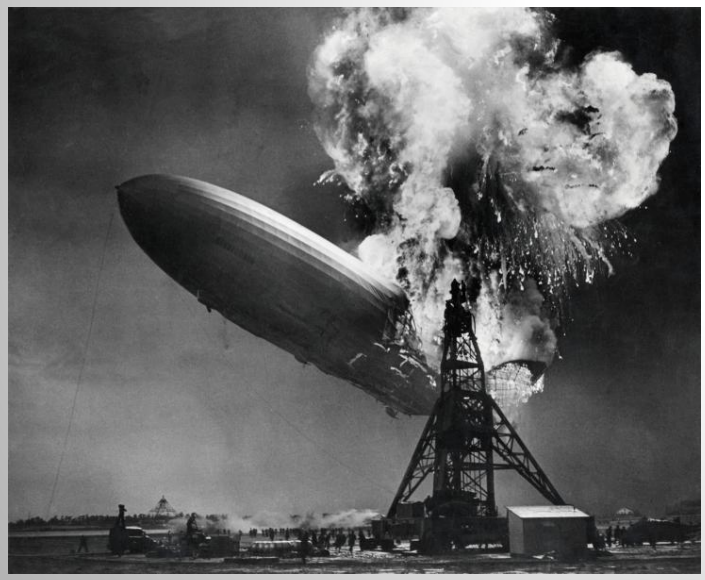
Last Year's Attempted Solution

- Probability of occurrence:
  - Never Happened Before (Least Likely)
  - Happened Once Before
  - Happened Multiple Times Before (Most Likely)



Fallacy

- If undesired consequence happened before we may have already created mitigations, so it won't happen again.



Hydrogen Filled

Helium Filled

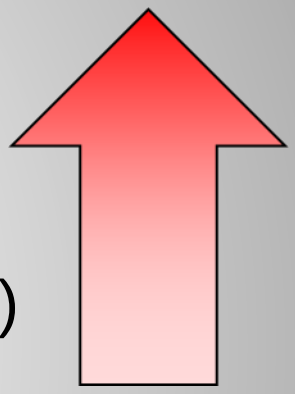
Guessing

- If something has never happened before how can we accurately predict its likelihood?

The results of the test, carried out early in 1964, calculated that the towers would handle the impact of a 707 traveling at 600 mph without collapsing.
https://www.ae911truth.org/evidence/faqs/360-faq-2-were-the-twin-towers-designed-to-withstand-the-impact-of-the-airplanes

Contra Fallacy

- Probability of occurrence:
  - Never Happened Before (More Likely)
  - Happened Once Before
  - Happened Multiple Times Before (Least Likely)



Contra Contra Fallacy

- Tires going flat
- School shootings
- Car accidents
- Terrorist acts
- Cyber hacking

Happened before many times but we have yet to mitigate these away.

Risk Confirmation Bias

- Bob likes his job at Colossaltron Inc.
- Bob likes his boss at Colossaltron
- Bob has stock options at Colossaltron
- Bob is due for a big promotion at Colossaltron
- Bob predicts likelihood of an undesired event at Colossaltron
- Can Bob be impartial?

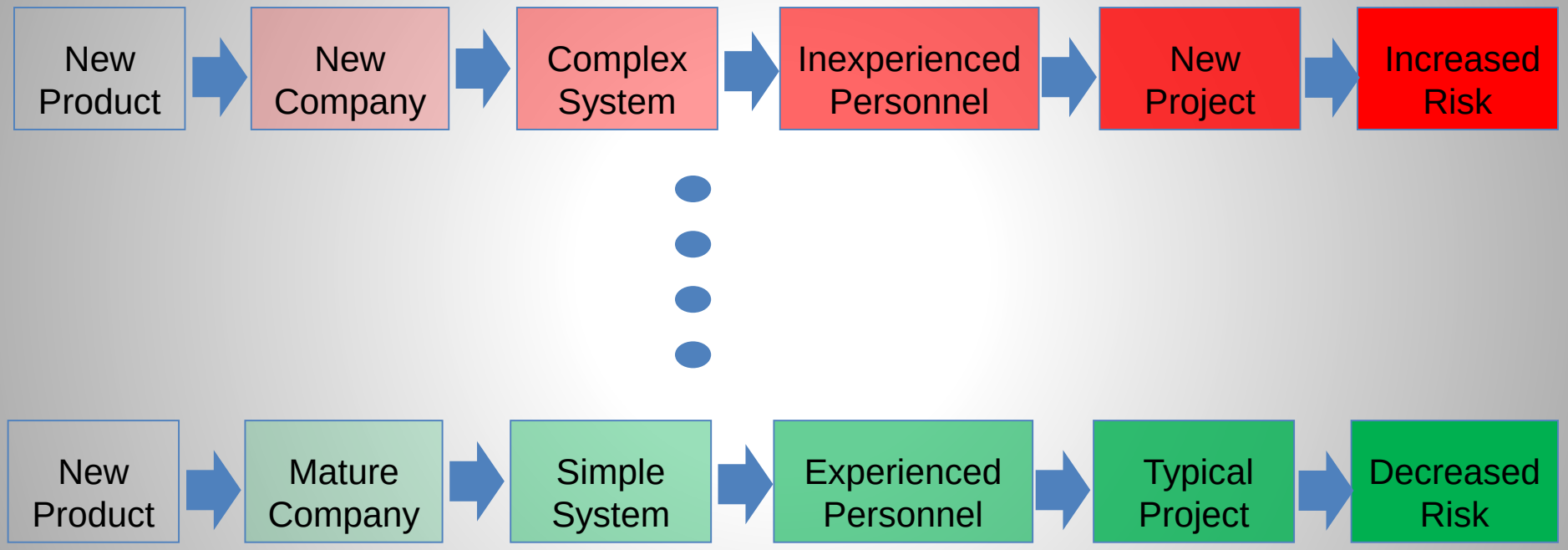
Confirmation Bias and Predictions

- 1876 “Telephones will never catch on” William Orton – Western Union
- 1927 “Who the hell wants to hear actors talk?” H.M. Warner – Warner Brothers
- 1946 “Television won’t last because people will soon get tired of staring at a plywood box every night.” Darryl Zanuck – 20th Century Fox
- 1977 “There is no reason for any individual to have a computer in his home.” Ken Olsen - Digital Equipment Corp
- 2007 “Especially phones that act like computers” Steve Ballmer - CEO Microsoft

Likelihood May Not Be the Best Indicator for Risk

- Hard to predict
- Confirmation bias
- Past does not assure the same future
- Political and economic factors can limit mitigations
- How to handle mechanical, electronics, environmental risks.

Could Institutional Risk Be Better?



Alternative Names for Institutional Risk

- Inferred Risk
- Entity Risk
- Corporate Risk
- Organizational Risk
- Infrastructure Risk
- Operations Risk
- Agile Risk
- DevSecOps Risk

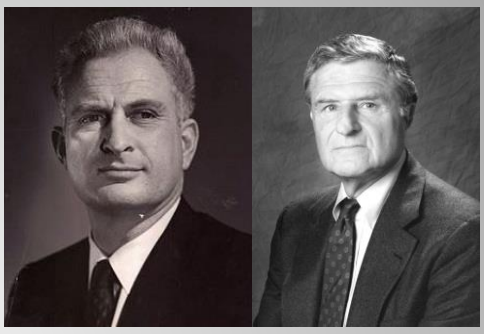
For Environmental Risk, Regional Factors, Assume Will Happen

- Meteor (1 in 250,000)[1]
- Earthquake (1 in 100)[3]
- Hurricane (Every N Years)[4]
- Strong Winds
- Tornado (1 in 60,000)[1]
- Lightning (1 in 17,241)[2]
- Tsunami
- Flood (1 in 27,000)[1]
- Wildfire
- Volcano

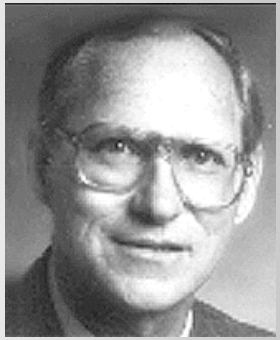
1. Dr. Stephen A Nelson, Tulane University
2. http://lightningsafety.com/nlsi_lhm/prbshort.html
3. https://pubs.usgs.gov/fs/old.1999/fs152-99/calcodds.html
4. https://www.noaa.gov/stories/what-are-chances-hurricane-will-hit-my-home

Reuse of Analysis Concepts

- Kepner Tregoe Decision Analysis



- Barry Boehm's COCOMO Model



- Nancy Leveson's STAMP

Institutional Categories

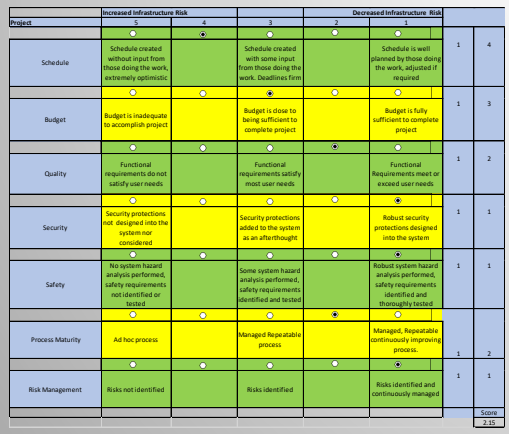
- Company
  - Experience of Management
  - Corporate Health
  - Competition
  - Cost of Entry
- Project
  - Schedule
  - Budget
  - Quality
  - Security
  - Safety
  - Process Maturity
  - Risk Management
- System
  - Complexity
  - Maturity
  - User Base
- Personnel
  - Relevant Experience
  - Staffing
  - Training and Education
  - Culture
  - Communications
  - Availability of Candidates

Magnitude X IR = Risk Score

- Magnitude of Impact
  - 5 - Highest
  - 4- High
  - 3 - Medium
  - 2 - Delay
  - 1 - Trivial

5 x 2.15 = 10.75

- Institutional Risk



Project	Increased Infrastructure Risk 5	4	3	Decreased Infrastructure Risk 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

Risk Score (w = 1)
1 (Lowest) – 25 (Highest)

Analyzing Institutional Risk (IR)

- Five Choices
- 1= Least IR,
- 5= Most IR
- Each category can be weighted (w)
- Score = choice x w
- Total IR = $\sum_1^n ir\ w$

Institutional Risk Factors							
	Increased Institutional Risk				Decreased Institutional 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

Company Institutional Risk Table

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

System Institutional Risk

	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

Personnel Institutional Risk

	Increased Infrastructure Risk			Decreased Infrastructure Risk			
Personnel	5	4	3	2	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	1
	○	○	◉	○	○		
Staffing	Projects are severely understaffed, continual overtime		Projects occasionally require overtime hours to meet deadlines		Projects staffed appropriately, overtime rare	1	3
	○	○	○	○	◉		
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	1
	○	○	◉	○	○		
Availability of Candidates	Qualified candidates are hard to recruit and hire		Some difficulty finding and hiring qualified candidates		Qualified candidates are readily available	1	3

Project Institutional Risk

	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

Three Institutions

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	4
Competition	Monopoly, only provider		Many competitors, customers have choices		Highly competitive marketplace	1	5
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
	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	4
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	3
	Increased Infrastructure Risk				Decreased Infrastructure Risk		
Personnel	5	4	3	2	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 to meet schedule		Projects staffed appropriately, overtime rare	1	4
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	4
Availability of Candidates	Qualified candidates are hard to recruit and hire		Some difficulty finding and hiring qualified candidates		Qualified candidates are readily available	1	4
	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	3
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	3
Process Maturity	Ad hoc process		Managed Repeatable process		Managed, Repeatable continuously improving process.	1	3
Risk Management	Risks not identified		Risks identified		Risks identified and continuously managed	1	3
							Score
							3.05

3.05

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	3
Corporate Health	Funding very restricted, start up, bankruptcy, merger		Successful track record of profitability		Industry leader, best in breed products, great reputation	1	2
Competition	Monopoly, only provider		Many competitors, customers have choices		Highly competitive marketplace	1	3
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	3
	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	3
	Increased Infrastructure Risk				Decreased Infrastructure Risk		
Personnel	5	4	3	2	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 to meet schedule		Projects staffed appropriately, overtime rare	1	3
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	2
Availability of Candidates	Qualified candidates are hard to recruit and hire		Some difficulty finding and hiring qualified candidates		Qualified candidates are readily available	1	3
	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	3
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
							2.4

2.4

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
	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
	Increased Infrastructure Risk				Decreased Infrastructure Risk		
Personnel	5	4	3	2	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	1
Staffing	Projects are severely understaffed, continual overtime		Projects occasionally require overtime to meet schedule		Projects staffed appropriately, overtime rare	1	3
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	1
Availability of Candidates	Qualified candidates are hard to recruit and hire		Some difficulty finding and hiring qualified candidates		Qualified candidates are readily available	1	3
	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

2.15

Institutional Risk by Supply Chain

Sacred Cow Inc.
Main Supplier

Trusty's Widgets
Sub-Contractor

Shifty's Used
Widgets
Sub-Sub-
Contractor

ebay

Handling Electrical, Mechanical, Environmental

- Electrical: If it can ever fail assume it will
- Mechanical: If it can ever fail assume it will
- Environmental: May be dependent on geographical region. If it has occurred in the geographical region assume it will happen.

Examples: Tornados in Midwest, earthquakes in west coast, hurricanes on gulf coast. Meteor strike can be ignored.

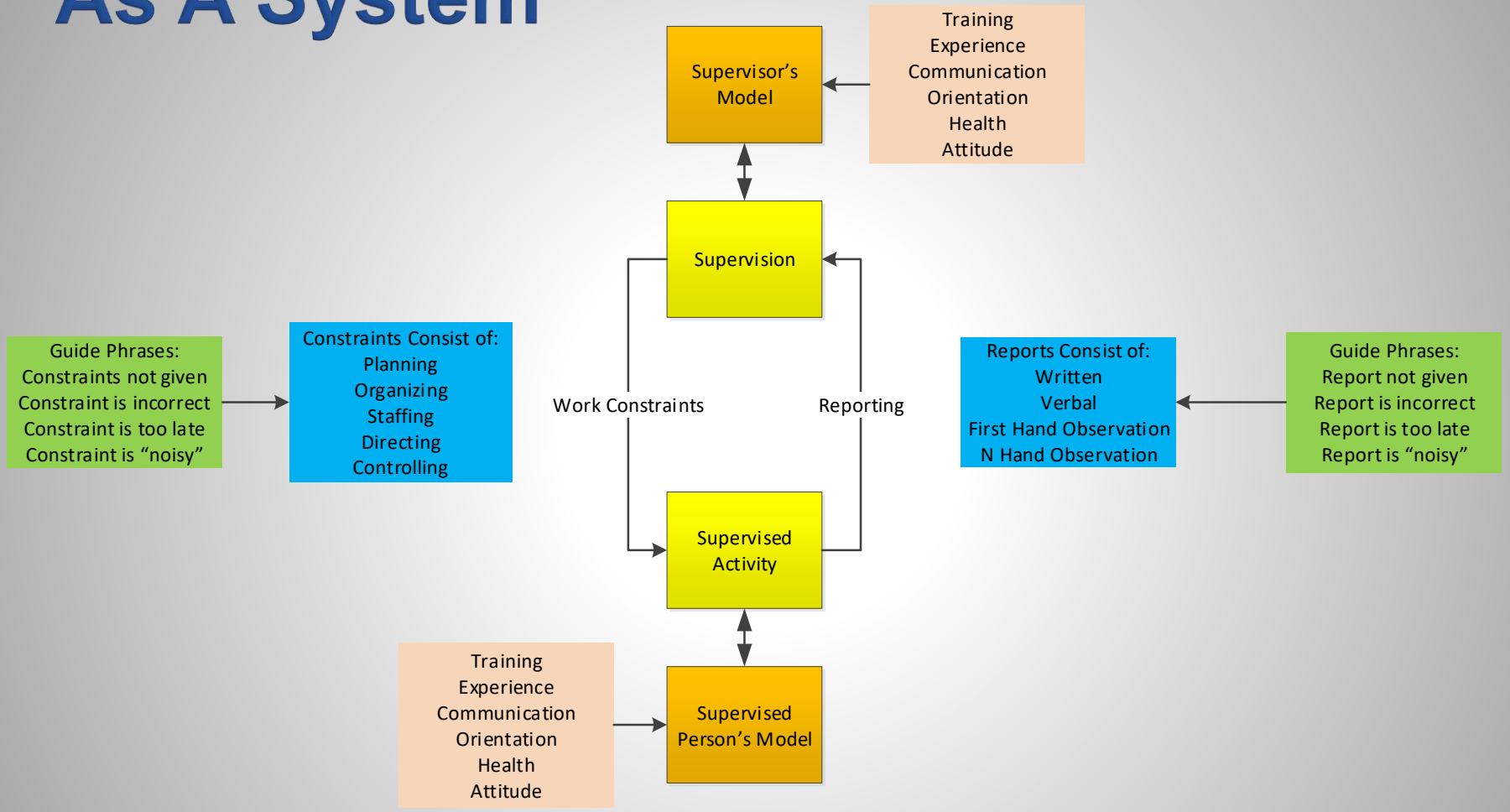
Develop Responses to the Risk

- Status
  - Identified
  - Active
  - Closed
  - Unassigned
- Risk Response
  - Leave It
  - Monitor
  - Avoid
  - Move
  - Mitigate
  - Unassigned

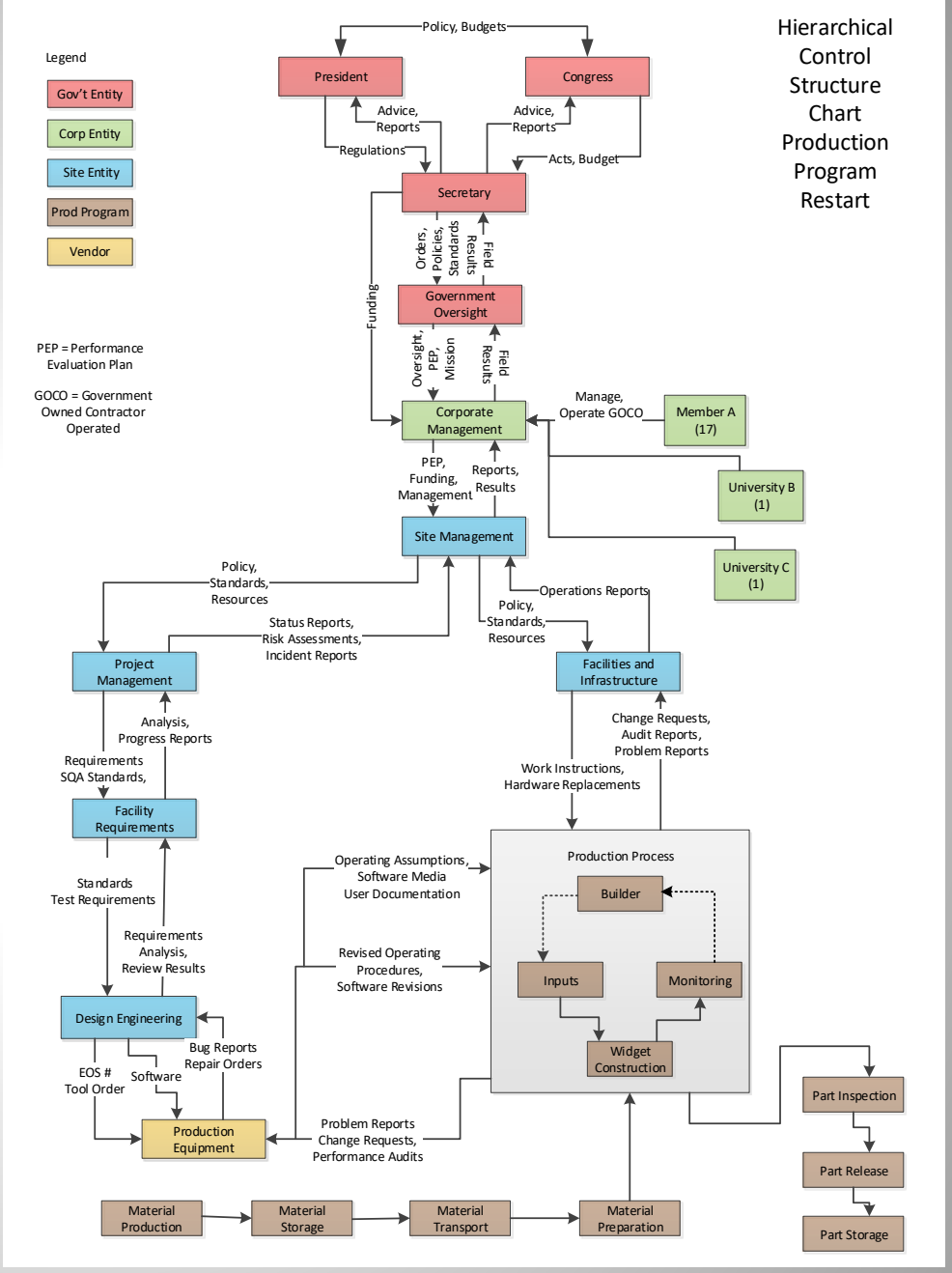
STPA Process

1. Find experienced domain experts in widget design, test, and production.
2. Create a Hierarchal Structure Chart for the organizations involved.
3. Apply guide phrases to each interface in the Hierarchal Structure Chart to identify risks.
4. Capture risks, prioritize, suggest mitigations.

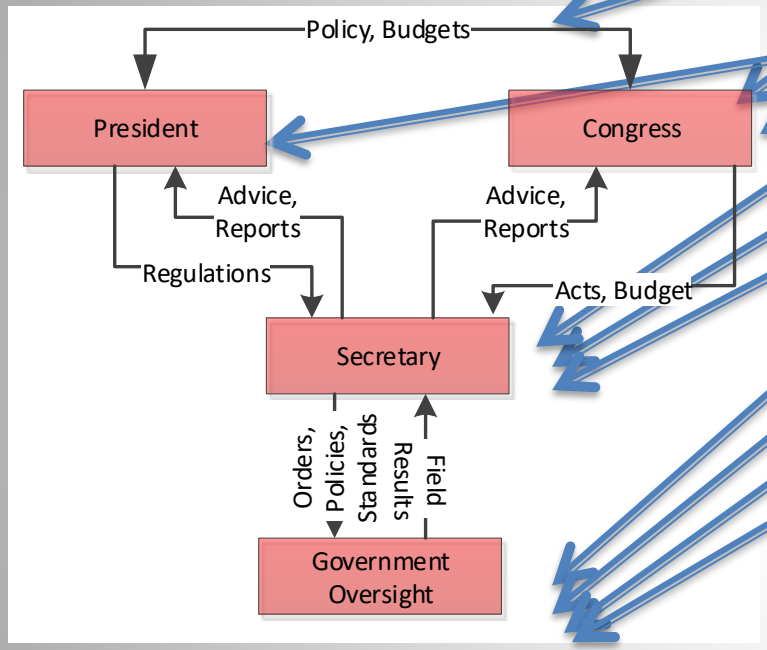
Organizational Components As A System



Hierarchical Control Structure Chart



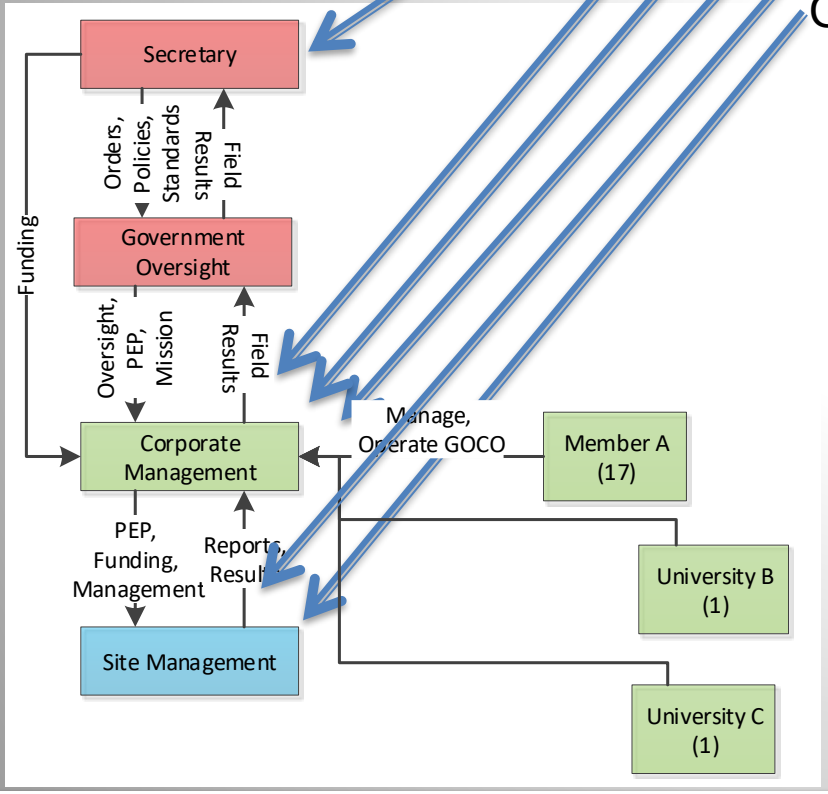
Government Entity Risks



GR1. Sequestration, Gov. Shut Down
GR2. Congressional fund reallocation
GR3. Congress/Executive Delays
GR4. Congress Privatization of Site
GR5. Automation Competency
GR6. Sec./oversight Turnover
GR7. Oversight Automation Experience
GR8. Oversight Budget Concerns
GR9. Oversight Diff. Tech opinion with Sites
GR10. Personal Opinions Over Experience

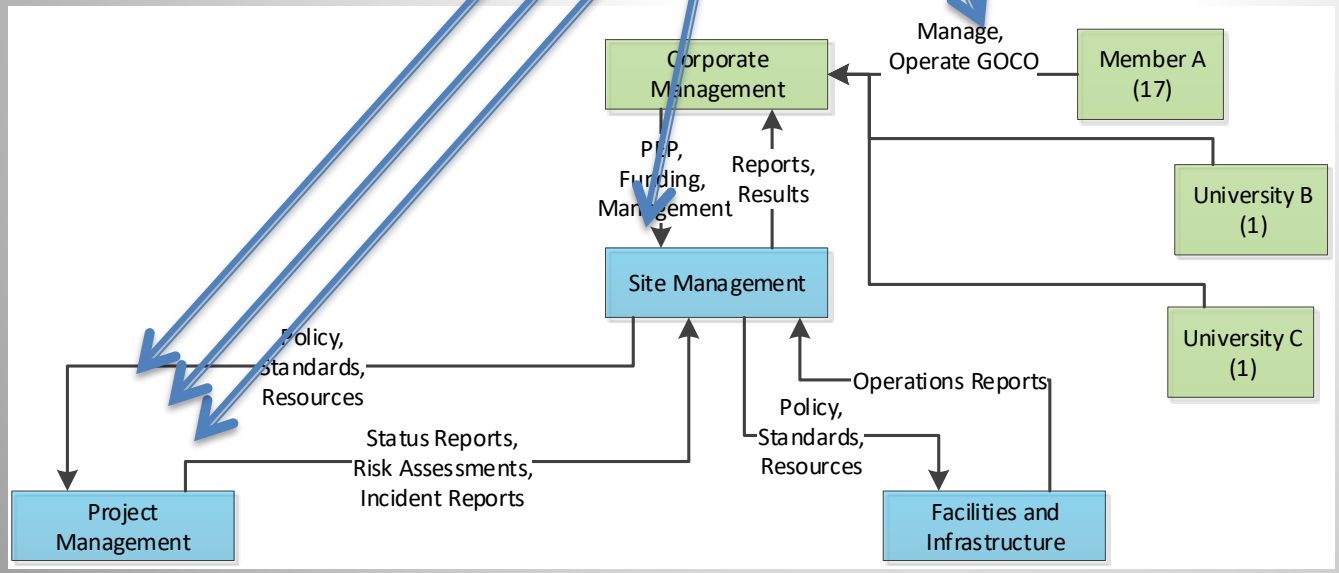
Government, Privatizing, Site Risks

GPSR1. Funding from Secretary, Not oversight
GPSR2. Taxes, Management Fee Increase
GPSR3. Work to Performance Incentives
GPSR4. Corporate Management Experience
GPSR5. Private Oversight Firm Acquired
GPSR6. Lack of Production Culture

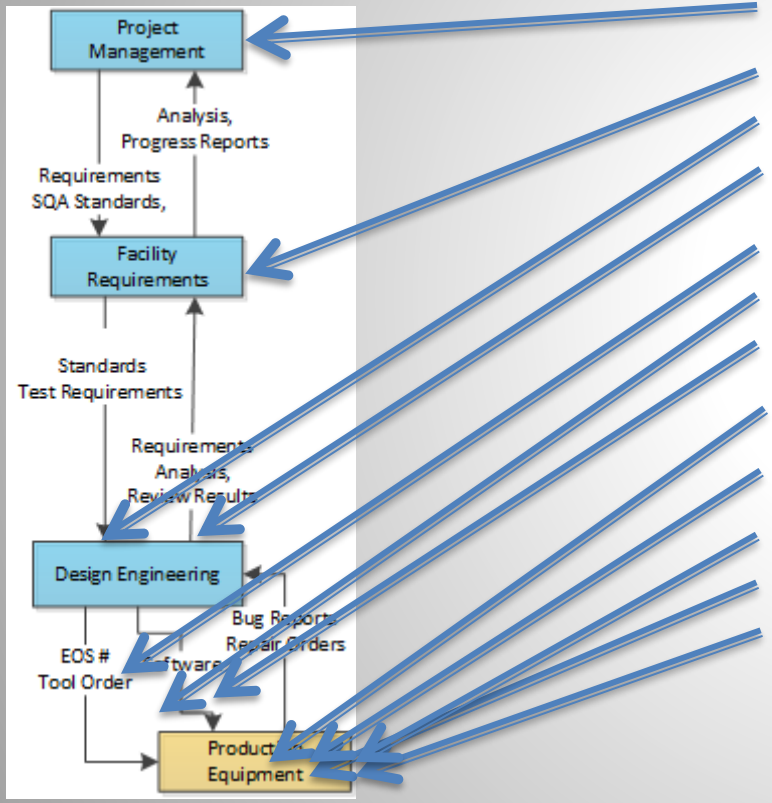


Site Management Risks

SMR1. Top Site Managers Corporate Employees
SMR2. Recent Site Management Switch
SMR3. Contending Priorities Make or Buy
SMR4. Compartmentation Culture
SMR5. Safety/Security Culture Undervalued



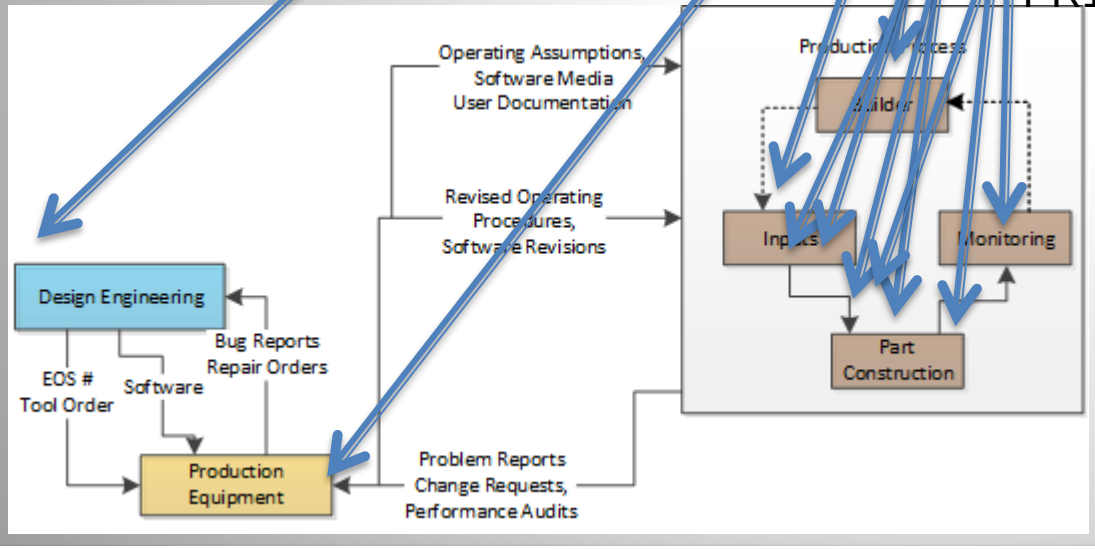
Development Risks



DR1. Wrong Compliance/Classification Standards
DR2. Requirements Unclear
DR3. Design Generation Tools
DR4. Configuration Management
DR5. Version Control
DR6. One of a Kind Development (30 Year Hiatus)
DR7. Rare Skill Mix Required, Understaffing
DR8. Retiring Labor Pool
DR9. Using Legacy Drawings to Build Parts
DR10. Budget and Schedule over Quality
DR11. Cyber security of Design Documentation
DR12. Difficulty in attracting talent to location

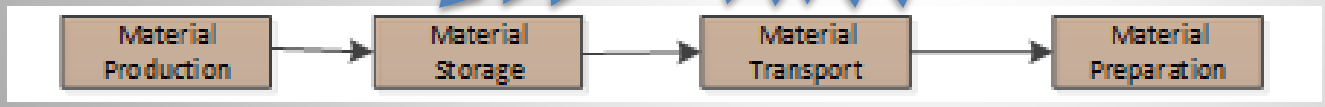
Production Risks

PR1. Tolerances not maintained
PR2. Drawing Correctness
PR3. Quantifying the Machines Uncertainty
PR4. Validating Results (Inspections)
PR5. Workspace Control
PR6. Lack of Independent Oversight
PR7. Repeatability of the Production Process
PR8. Welding Set Up
PR9. Retiring Production Employees
PR10. Production Culture vs. Design Culture
PR11. Spill Containment
PR12. Material Handling
PR13. Blank Forming
PR14. Volatility Considerations
PR15. Toxic Scrap Disposition

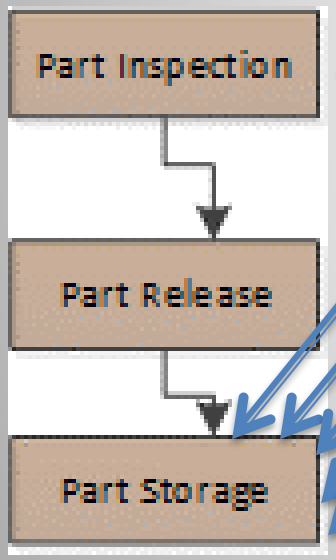


Material Handling Risks

MHR1. Transportation Safety and Security
MHR2. Maintain Material Purity
MHR3. Integrity of Storage Facility
MHR4. Volatility Considerations
MHR5. Proper Atmosphere
MHR6. Theft Temptation
MHR7. Inventory Tracking Accurate
MHR8. Cyber Security of Inventory System

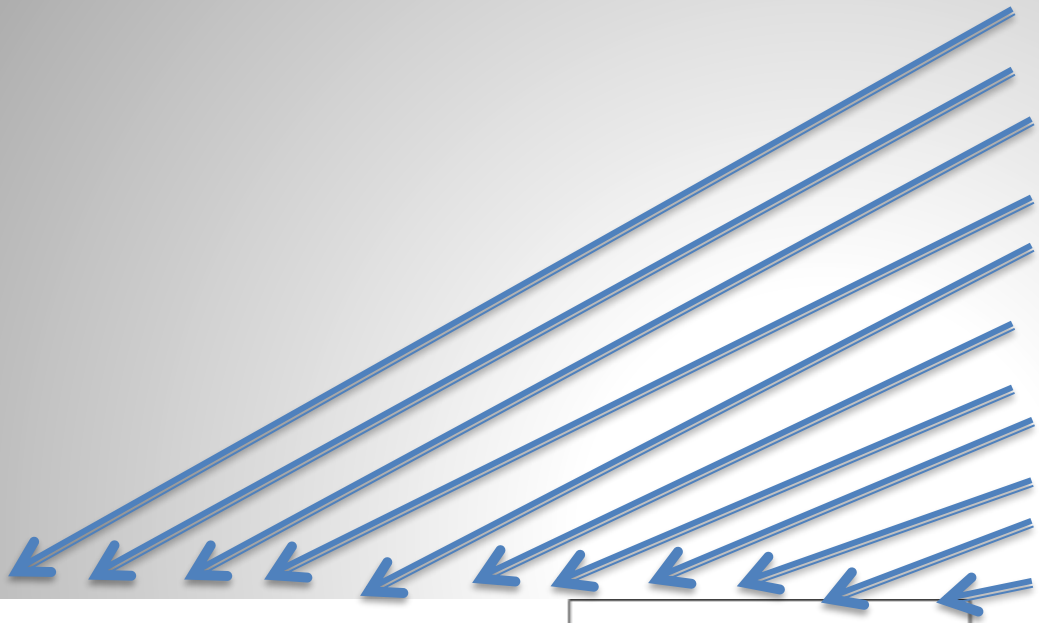


Post Production and Storage Risks

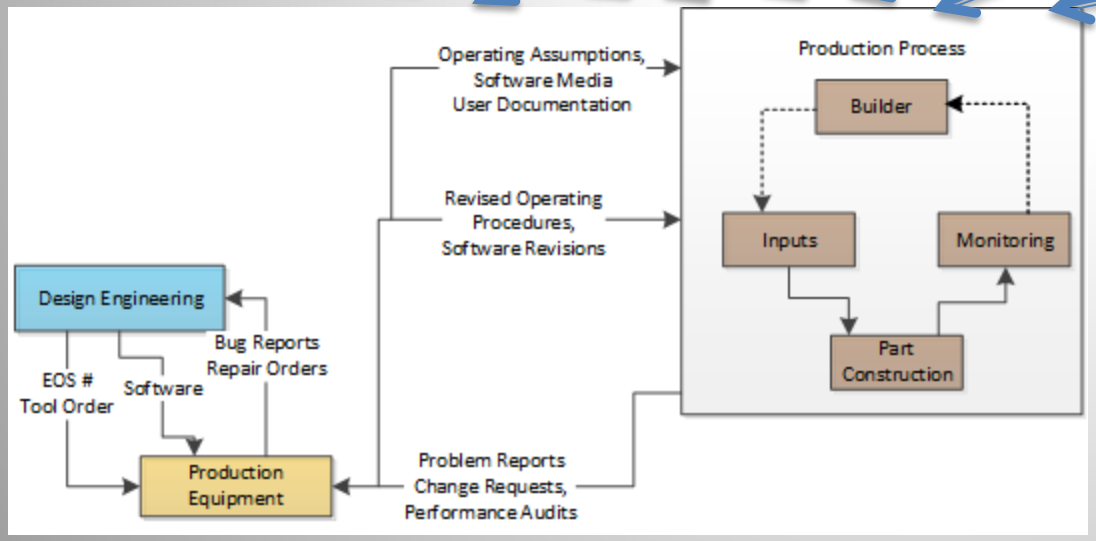


PPR1. Volatility Considerations
PPR2. Theft Security
PPR3. Maintain Interior Atmosphere
PPR4. Failed Inspection Process
PPR5. Inventory Tracking Accurate
PPR6. Cyber Security of Tracking System

Environmental Risks

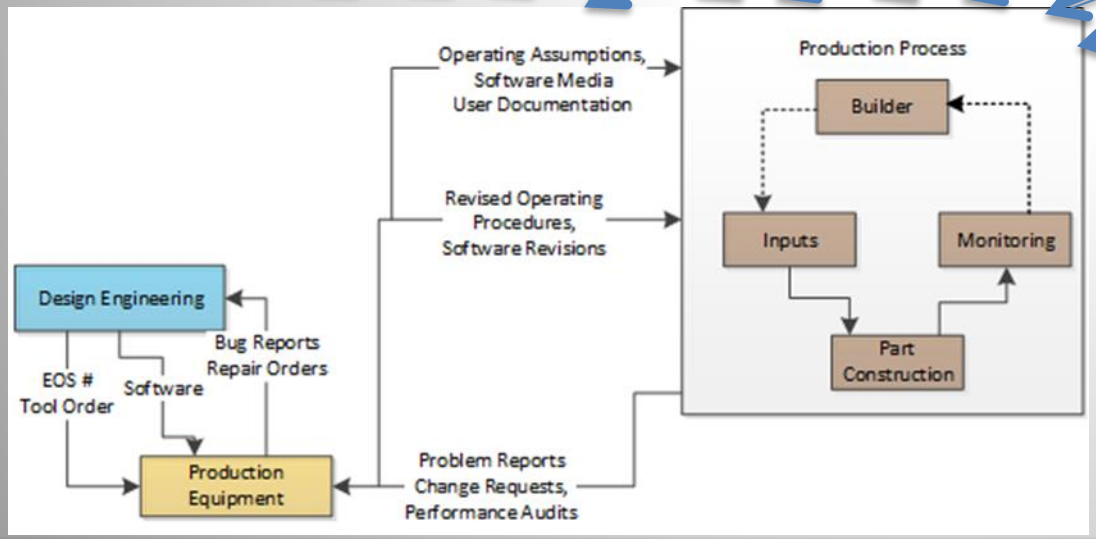


ER1. Earthquake
ER2. Flood
ER3. Tsunami
ER4. Hurricane
ER5. Tornado
ER6. Wild Fire
ER7. Reservoir Splushing
ER8. Volcano
ER9. Lightning
ER10.Sinkhole
ER11 Blizzard, Ice, Hail Storm

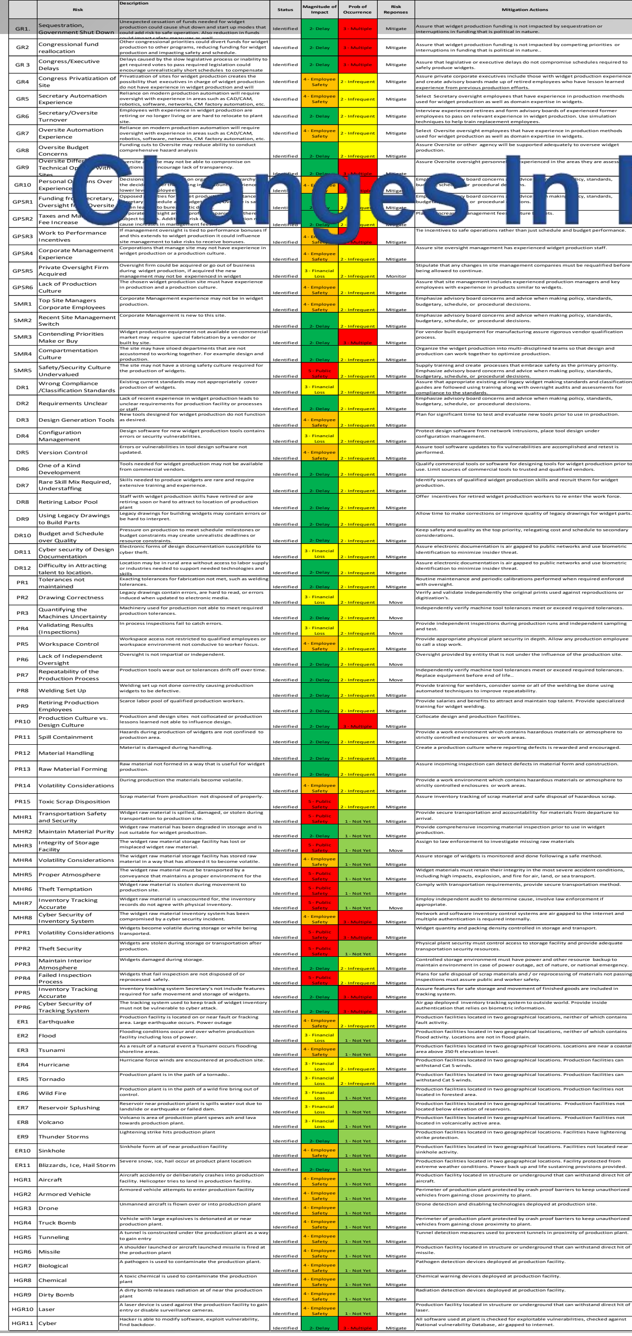


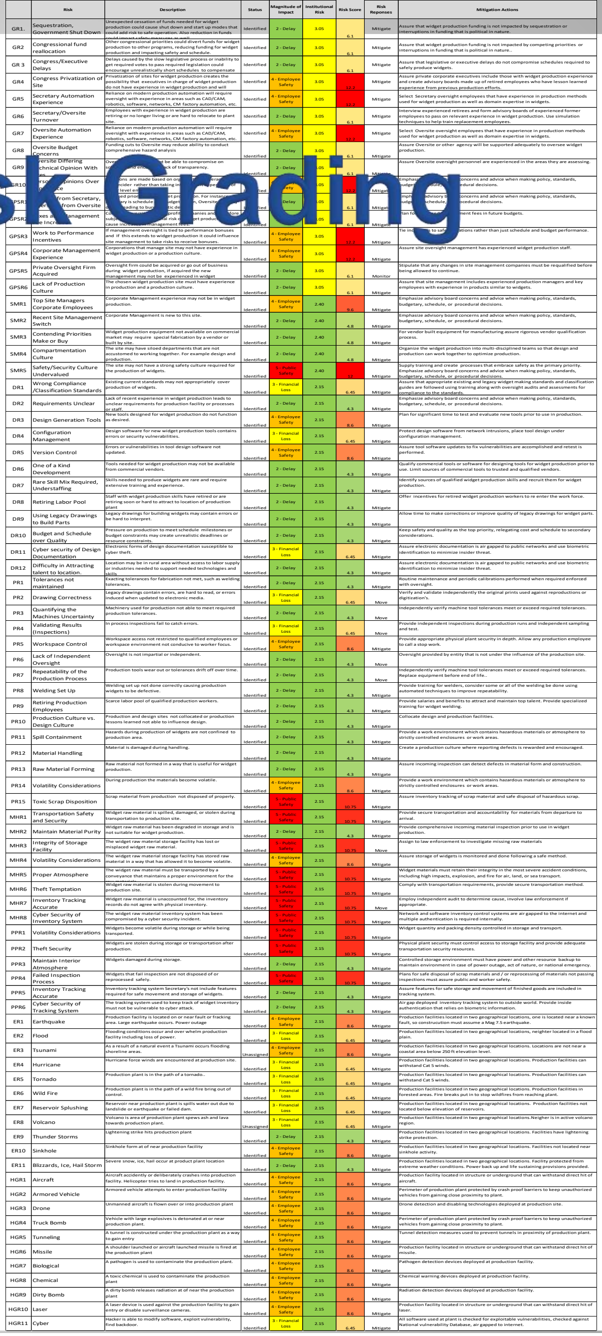
Human Generated Risks

HGR1. Aircraft
HGR2. Armored Vehicle
HGR3. Drone
HGR4. Truck Bomb
HGR5. Tunneling
HGR6. Missile
HGR7. Biological
HGR8. Chemical
HGR9. Dirty Bomb
HGR10. Laser
HGR11. Cyber



Changes In Risk Grading





Comparison Between Methods

Risk ID	Risk	Description	Status	Magnitude of Impact	Prob of Occurrence	Risk Reponses	Mitigation Actions
1	Hero Mode Development	One team member becomes indispensable to the team because of knowledge of sections of the code. Modifications of sections of the code can only be done by	Active	5 - Highest	5 - Highest	Mitigate	Recorded code walkthroughs by Dan to acquaint team with frontend code. Training materials or classes from EDG for their portion of the front end code.
2	No System Level Testing	Code going directly from researcher/developer to user without any independent system testing. Documentation not verified.	Active	5 - Highest	5 - Highest	Mitigate	Independent system testers added, funded by ISCP, documentation versions synchronized to versions.
3	Funding for hardening, productizing, and maintaining tools Is not available	System testing not planed of included in ROSE development model.	Active	5 - Highest	5 - Highest	Mitigate	ISCP funding covers 1.5 FTE for system testing and documentation verification. All tools built for users form the ROSE framework will require independent system level testing.
4	Unhappy users	Deliverable [illegible]estones missed [illegible]or ca[illegible]ty [illegible]oo[illegible] does not me[illegible]stome[illegible]pec[illegible]ns. To[illegible]ool[illegible]d to install and/or use.	Active	5 - Highest	5 - Highest	Mitigate	The customer based ROSE masterplan to be reviewed on a weekly basis detecting problems, identifying obstacles, and setting work arounds into place at the earliest point.
5	Chasing Shiny Objects	Team or team members attracted to new and exciting sounding code challenges diverting resources and causing longer term project milestone slip right.	Active	5 - Highest	4 - High	Mitigate	Limit annual time budget for Bluebird requests to a capped amount. Some of these efforts are useful (eat your own dog food) and important , so do not want to eliminate them entirely.
6	Level of rigor too high or too low	Do not want to retard research and exploration, want to have more rigorous code tools built from ROSE.	Active	5 - Highest	5 - Highest	Mitigate	Dual track risk levels in SQAP. RL 4 for ROSE framework (core) for researchers, RL 3 for tools built with ROSE framework for application developers.
7	Too many parallel projects	Rose managed as one large project with various add-ons for versus customers.	Active	5 - Highest	4 - High	Monitor	ROSE master plan breaks out ROSE work by customer projects.
8	Funding Continuity	ROSE has historically been funded from various sources without long term continuity. This has made the team leadership conservative about growth and support and	Active	5 - Highest	5 - Highest	Mitigate	Additional LLNL internal funding applied to help fill in the funding GAPS. Expansion of number of tasks for GS using planning, hiring, and contracting to supplement ROSE.
9	Test Platforms Aging	Platforms used for testing ROSE are aging and need to be upgraded to be more consistent with customer platforms.	Active	4 - High	4 - High	Mitigate	Use a portion of the project funds to purchase new platforms.
10	Insufficient resources to support user needs	User support is handled by asking developers for help directly which may distract them from other commitments.	Active	4 - High	4 - High	Mitigate	System testers will be used as the first level of user support. If system testers can not help the user then they will talk with developers to get additional information to help users. In this way user support time should be minimal for all but the most complex
11	Customer Experience	ROSE users may not think like compiler specialists	Active	4 - High	4 - High	Mitigate	Orient documentation to support application developers that are not compiler experts
12	Documentation Verbose	Documentation is immense and hard to find specific topics	Active	4 - High	4 - High	Mitigate	Create cookbook instructions for tools and a knowledge base forcommon user problems
13	Too much software in install packages	The ROSE install packages includes ROSE tests which use up a majority of the users time loading and a large amount of platform memory.	Active	4 - High	4 - High	Move	Tests will be removed from user install media. The tests can still be obtained but only if the user wants to have them.
14	Too many tools	The ROSE tool folder contains dozens of different tools collected over the years. Supporting all of these tools is very time consuming.	Identified	4 - High	4 - High	Avoid	Pair the tool folder down to less than a dozen useful tools. Use the system testers to validate the tools work correctly.
15	Lack of SE experience	ROSE using best SE practices	Active	4 - High	4 - High	Mitigate	Need to continue to encourage and incentivize ROSE staff to use SE best practices, reviews, and robustification funds
16	Too many platform types supported	There are 14 x 35 variations of BOOST and Compilers which are currently tested in the matrix testing	Active	3 - Medium	4 - High	Avoid	Consider reducing the number of combinations based on market analysis and customer requests.
17	Latest compilers, Libraries and operating systems not available or supported	LC does not support all the platforms that customers require ROSE to run on.	Active	3 - Medium	4 - High	Move	Out source to cloud vendors.
18	Large Platform Combonations	Versions of EDG, BOOST, Compilers, Operating Systems, Compiler Standards, and language popularity changing impacts ROSE performance.	Active	4 - High	4 - High	Mitigate	Automated testing reduces necessary to adapt to new condition. Previously released ROSE tool impacts considered. Updates to new version only done when enhanced functionality benefits users.
19	EDG goes out of business	EDG is the C,C++ parser for ROSE	Active	4 - High	2 - Low	Mitigate	ROSE demonstrated to work with LLVM (CLANG) for C.
20			Unassigned	1 - Lowest	1 - Lowest	Unassigned	

Risk ID	Risk	Description	Status	Magnitude of Impact	Infrastructure Risk	Risk Score	Risk Reponses	Mitigation Actions
1	Hero Mode Development	One team member becomes indispensable to the team because of knowledge of sections of the code. Modifications of sections of the code can only be done by	Active	5 - Highest	2.85	14.25	Mitigate	Increased responsibility for Marcus, Liao, Tristen. Training materials or classes from EDG for their portion of the front end code.
2	No System Level Testing	Code going directly from researcher/developer to user without any independent system testing. Documentation not verified.	Active	5 - Highest	2.85	14.25	Mitigate	Independent system testers added, funded by ISCP, documentation versions synchronized to versions. Move to sponsor funded.
3	Funding for hardening, productizing, and maintaining tools Is not available	System testing not planed or included in ROSE development model.	Active	5 - Highest	2.85	14.25	Mitigate	ISCP funding covers improvements in Testing frameworks, Juliet Test Suite, Plum Hall Tests suite. Cost moving to sponsors.
4	Unhappy users	Deliverable [illegible]estones missed and/or capability of tool does n[illegible]t cu[illegible]expectations. Too[illegible]hard install [illegible]	[illegible]tive	5 - [illegible]	2.8	[illegible]	Mitigate	The customer based ROSE masterplan to be reviewed on a weekly basis detecting problems, identifying obstacles, and setting work arounds into place at the earliest point.
5	Chasing Shiny Objects	Team or team members attracted to new and exciting sounding code challenges diverting resources and causing longer term project milestone slip right.	Active	5 - Highest	2.85	14.25	Mitigate	Limit annual time budget for Bluebird requests to a capped amount. Some of these efforts are useful (eat your own dog food) and important , so do not want to
6	Level of rigor too high or too low	Do not want to retard research and exploration, want to have more rigorous code tools built from ROSE.	Active	5 - Highest	2.85	14.25	Unassigned	Prioritize and repair most all high priority defects in backlog
7	Too many parallel projects	Rose managed as one large project with various add-ons for versus customers.	Active	5 - Highest	2.85	14.25	Mitigate	Dual track risk levels in SQAP. RL 4 for ROSE framework (core) for researchers, RL 3 for tools built with ROSE framework for application developers.
8	Funding Continuity	ROSE has historically been funded from various sources without long term continuity. This has made the team leadership conservative about growth and support and	Active	5 - Highest	2.85	14.25	Mitigate	Additional LLNL internal funding applied to help fill in the funding GAPS. Expansion of number of tasks for GS using planning, hiring, and contracting to supplement
9	Test Platforms Aging	Platforms used for testing ROSE are aging and need to be upgraded to be more consistent with customer platforms.	Active	4 - High	2.85	11.4	Monitor	Use a portion of the project funds to purchase new platforms.
10	Insufficient resources to support user needs	User support is handled by asking developers for help directly which may distract them from other commitments.	Active	4 - High	2.85	11.4	Mitigate	System testers will be used as the first level of user support. If system testers can not help the user then they will talk with developers to get additional information to
11	Customer Experience	ROSE users may not think like compiler specialists	Active	4 - High	2.85	11.4	Mitigate	Orient documentation to support application developers that are not compiler experts
12	Documentation Verbose	Documentation is immense and hard to find specific topics	Active	4 - High	2.85	11.4	Mitigate	Create cookbook instructions for tools and a knowledge base for common user problems
13	Too much software in install packages	The ROSE install packages includes ROSE tests which use up a majority of the users time loading and a large amount of platform memory.	Active	4 - High	2.85	11.4	Mitigate	Tests will be removed from user install media. The tests can still be obtained but only if the user wants to have them.
14	Too many tools	The ROSE tool folder contains dozens of different tools collected over the years. Supporting all of these tools is very time consuming.	Active	4 - High	2.85	11.4	Mitigate	Pair the tool folder down to less than a dozen useful tools. Use the system testers to validate the tools work correctly.
15	Lack of SE experience	ROSE using best SE practices	Active	4 - High	2.85	11.4	Mitigate	Need to continue to encourage and incentivize ROSE staff to use SE best practices, reviews, and robustification funds
16	Too many platform types supported	There are 14 x 35 variations of BOOST and Compilers which are currently tested in the matrix testing	Active	3 - Medium	2.85	8.55	Mitigate	Consider reducing the number of combinations based on market analysis and customer requests.
17	Latest compilers, Libraries and operating systems not available or supported	LC does not support all the platforms that customers require ROSE to run on.	Active	3 - Medium	2.85	8.55	Mitigate	Pare the tool folder down to less than a dozen useful tools. Use the system testers to validate the tools work correctly.
18	Large Platform Combinations	Versions of EDG, BOOST, Compilers, Operating Systems, Compiler Standards, and language popularity changing impacts ROSE performance.	Active	4 - High	2.85	11.4	Move	Out source to cloud vendors.
19	EDG goes out of business	EDG is the C,C++ parser for ROSE	Active	4 - High	2.85	11.4	Mitigate	ROSE demonstrated to work with LLVM (CLANG) for C.
20	OSS Users	Open Source Users consume time of senior developers seeking help. This creates unplanned work.	Active	3 - Medium	2.85	8.55	Mitigate	Set up help desk, FAQ, and a priority escalation schema to release senior developers from helping users except in rare cases.
21	Proposals and load leveling of staff	Proposals submitted primarily to secure funding may not agree with what ROSE sources can do in the time frame given.	Active	3 - Medium	2.85	8.55	Mitigate	Going forward assure proposals also support the master plan and directions, focus on beefing up previous research work.
22	Accumulated Technical Debt	Technical debt has accumulated in ROSE code over the past 15 years making it harder to trouble shoot and maintain.	Active	4 - High	2.85	11.4	Mitigate	Make bug fixing a top priority. From Plum Hall suite and Klowork, and ASC reproducers.
23			Unassigned	1 - Lowest	2.85	2.85	Unassigned	

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.

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.

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.

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.

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.

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.

Post-Production 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.

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.

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.

Example Major Risks

- PPR1 - Widgets become volatile during storage or while being transported.
- PPR4 - Widgets that fail inspection are not disposed of or reprocessed safely.
- MH1 -Widget raw material is spilled, damaged, or stolen during transportation to production site.
- PPR2 - Widgets are stolen during storage or transportation after production.
- MH7 - Widget raw material is unaccounted for, the inventory records do not agree with physical inventory.

Example Risks by Category

- GR3 - Delays caused by the slow legislative process or inability to get required votes to pass required legislation could encourage unrealistically short schedules to compensate for a late start due to legislative or executive delays.

- 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.

Example Risk by Category

- SMR5 - The site may not have a strong safety culture required for the production of widgets.
- DR3 - New tools designed for widget production do not function as desired.
- PR9 - Scarce labor pool of qualified production workers.
- MHR8 - The widget raw material inventory system has been compromised by a cyber security incident.

Example Risk by Category

- PPR1 - Widgets become volatile during storage or while being transported.
- ER1 - Unmanned aircraft is flown over or into production plant.
- HGR3 - Production facility is located on or near fault or fracking area. Large earthquake occurs. Power outage.

Remaining Work

- SME review of Hierarchical Structure Chart
- SME review of identified risks
- SME review of risk magnitudes and probability of occurrence.
- SME review of mitigations.

STPA Summary

- There are hazard analysis techniques which have been successfully used in the past for making widgets.
- STPA found contemporary risks.
  - Government, Privatization, Cyber, Drones, etc.
- STPA can be combined with other types of hazard analysis.
- Widget experts were receptive to approach, no one technique can prove it considers everything.