Risk Management Using STPA Restarting Widget Production

STAMP Workshop, MIT March 26, 2019

Gregory Pope CSQE

Lawrence Livermore National Laboratory

LLNL-PRES-LLNL-PRES-770080

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

The Problem

- 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 ?

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
  - Public Safety
  - Worker Safety
  - Financial Loss
  - Delay
  - Trivial
- Probability of Occurrence
  - Multiple
  - Infrequent
  - Not Yet

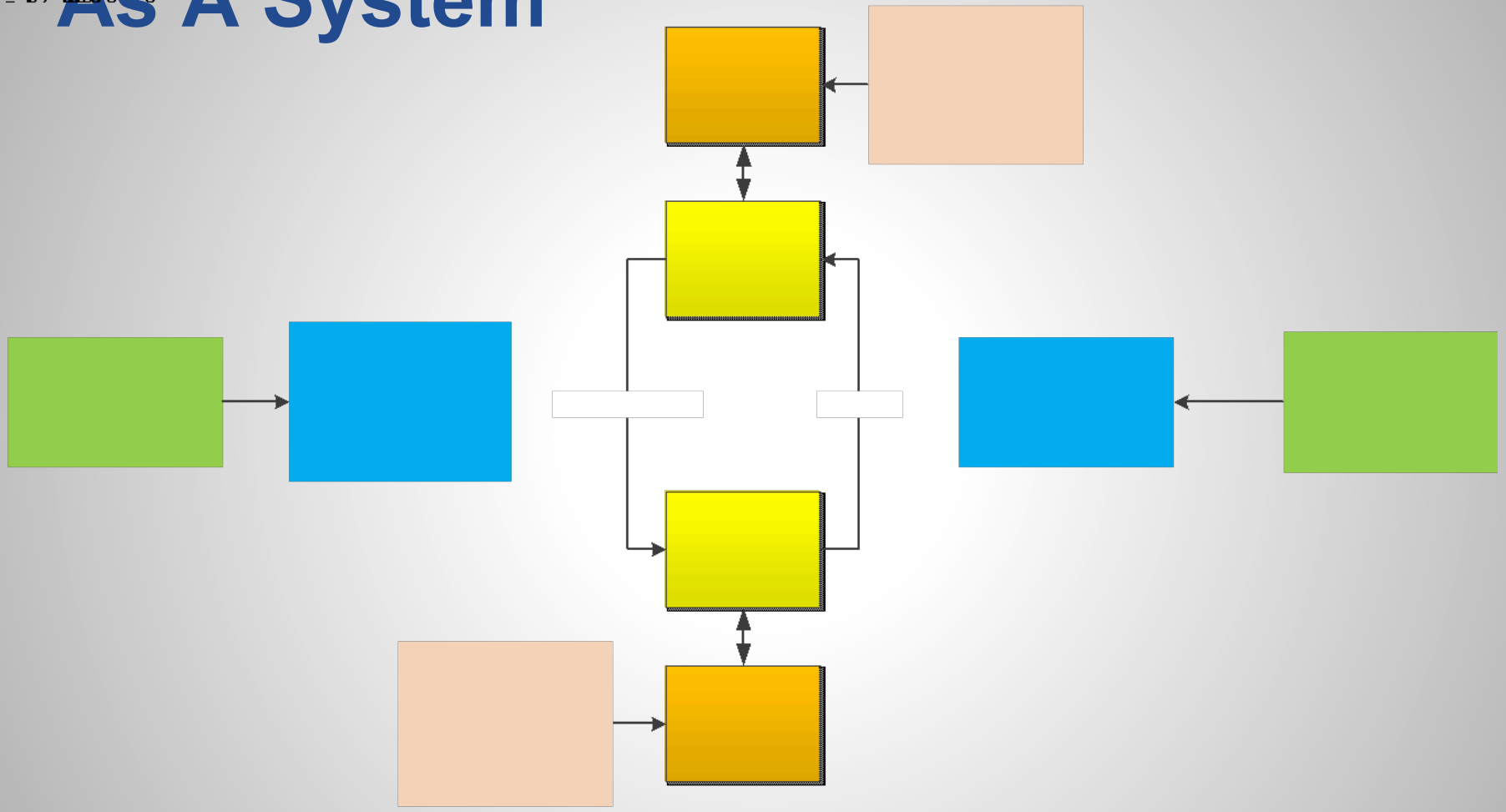
Develop Responses to the Risk

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

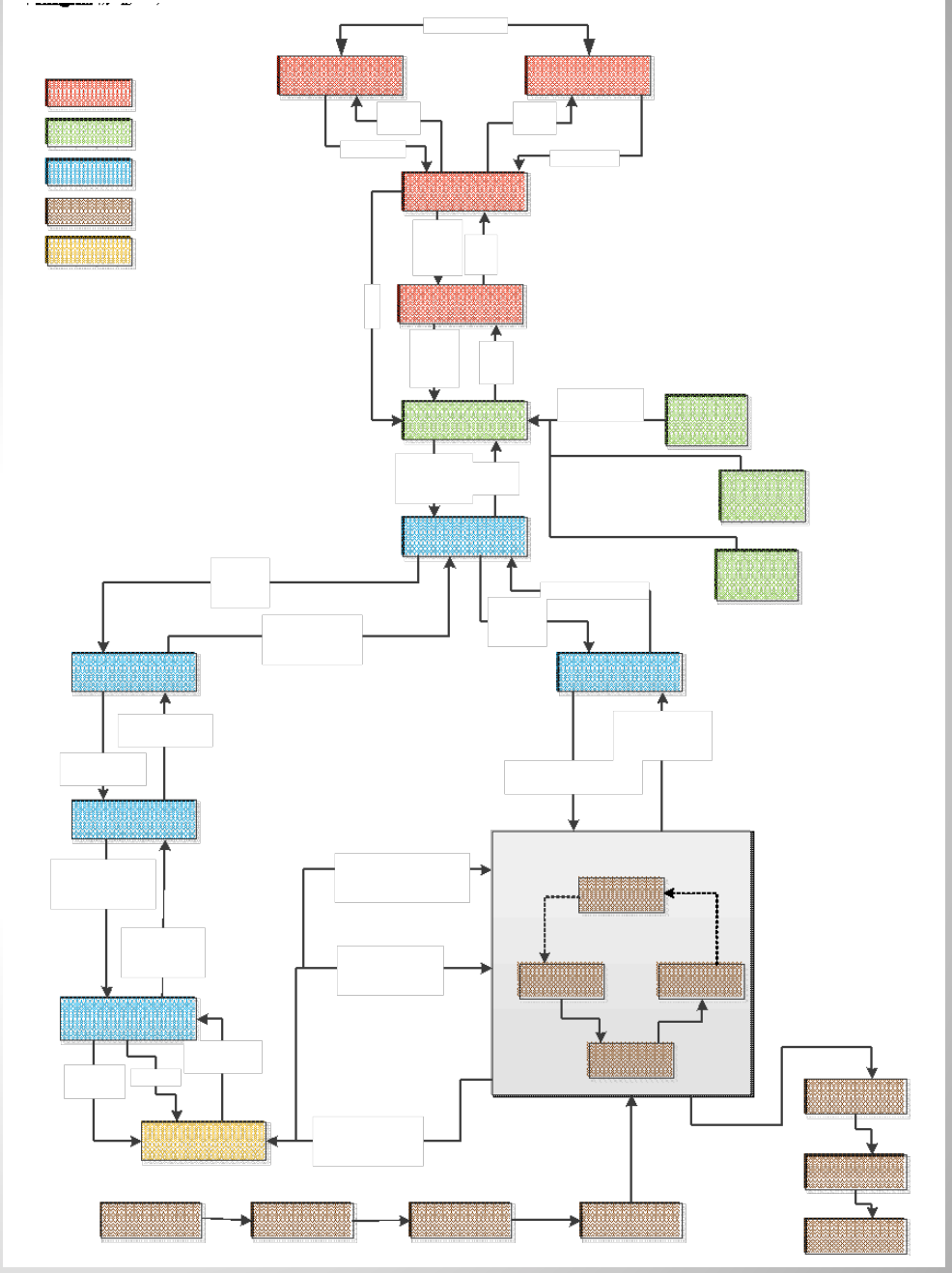
STPA Process

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

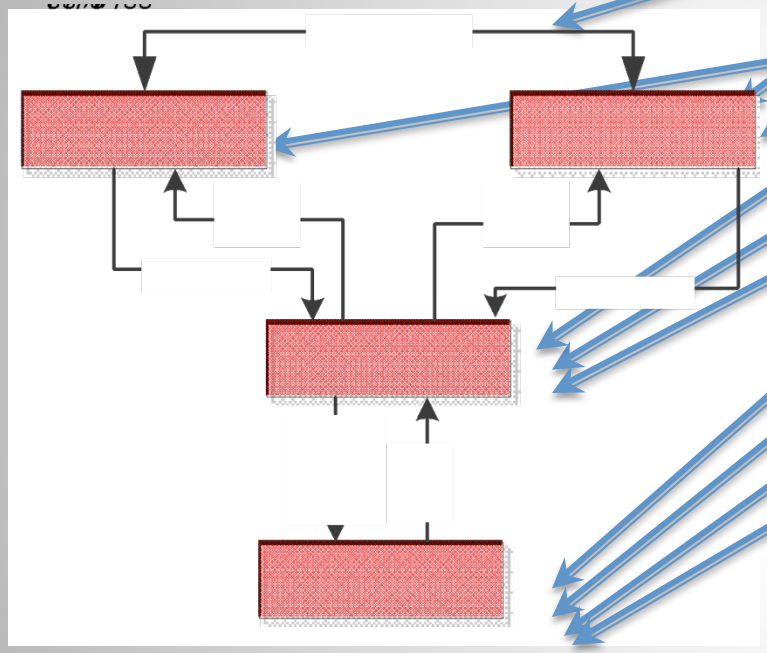
Organizational Components As A System



Hierarchical Control Structure Chart

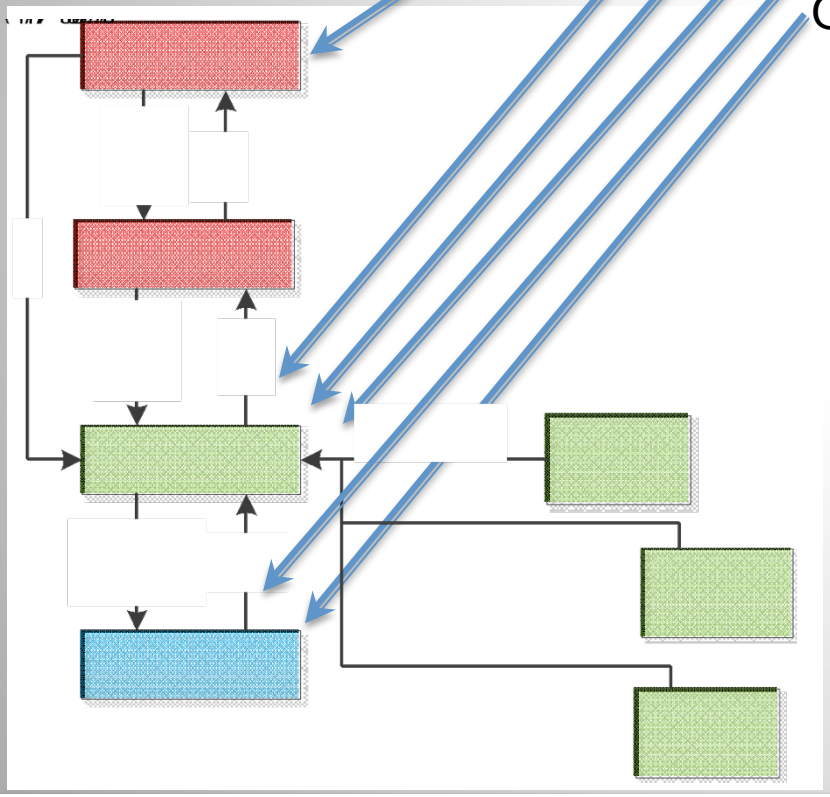


Government Entity Risks



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

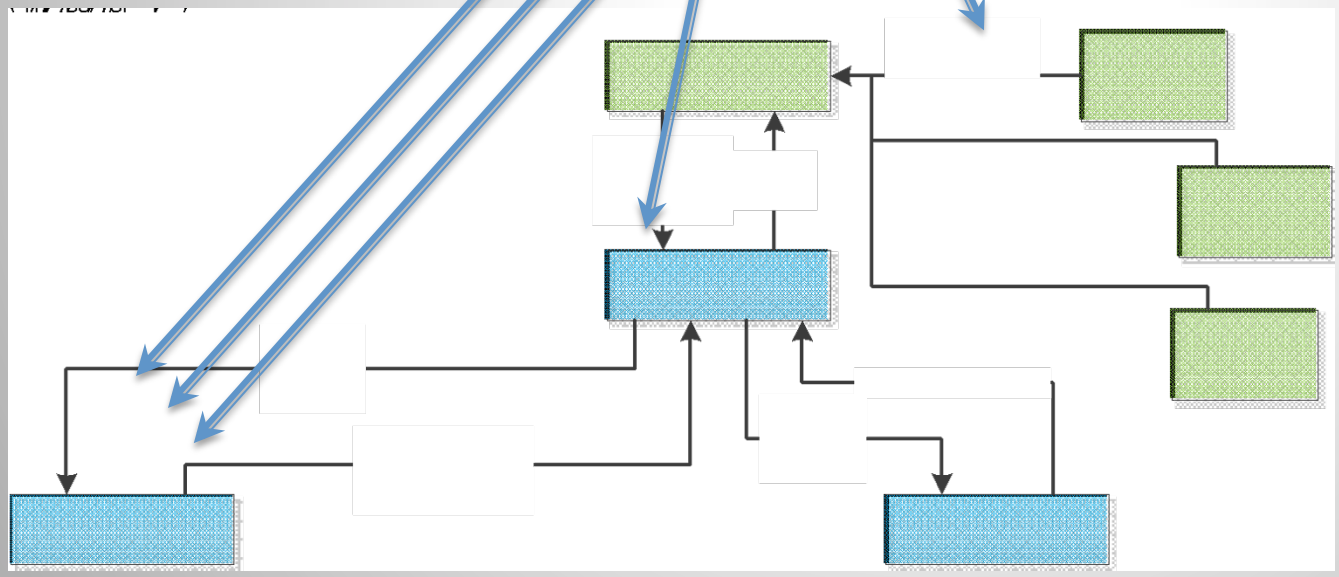
Government, Privatizing, Site Risks



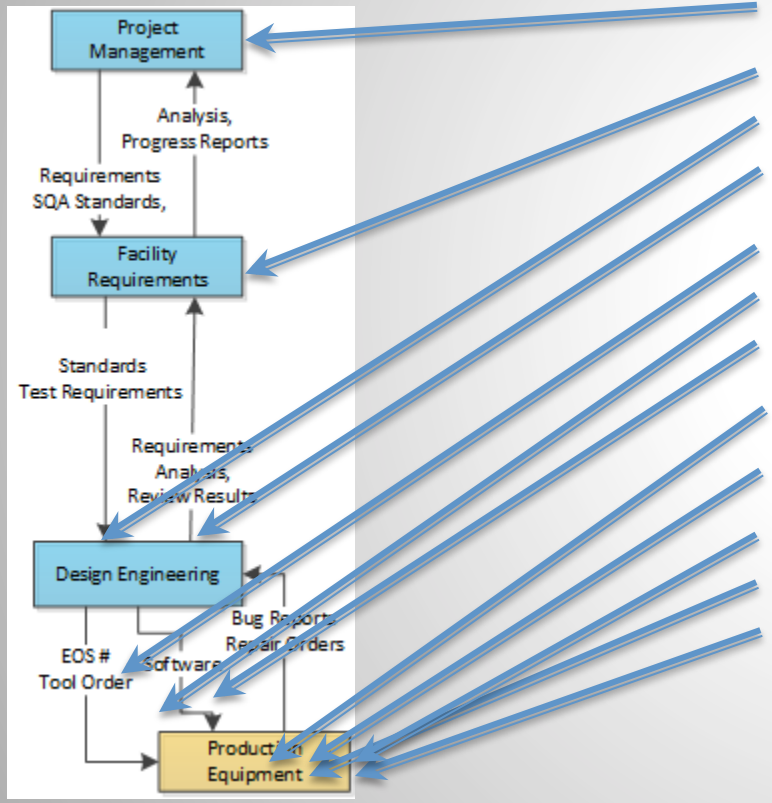
GPSR1. Funding from Secretary, Not oversight
GPSR2. Taxes, Management Fee Increase
GPSR3. Work to Performance Incentives
GPSR4. Corporate Management Experience
GPSR5. Private Oversight Firm Acquired
GPSR6. Lack of Production Culture

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



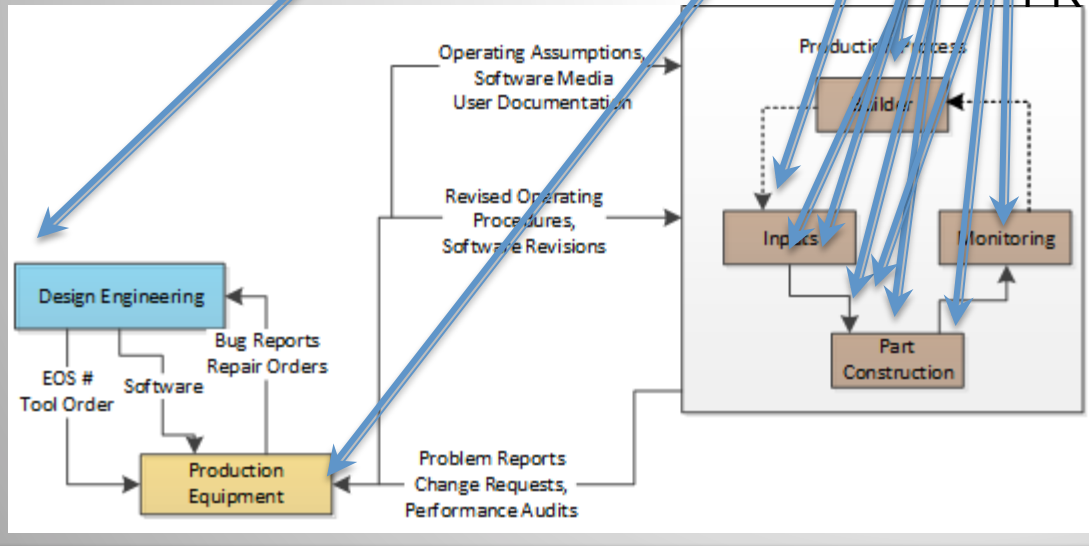
Development Risks



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

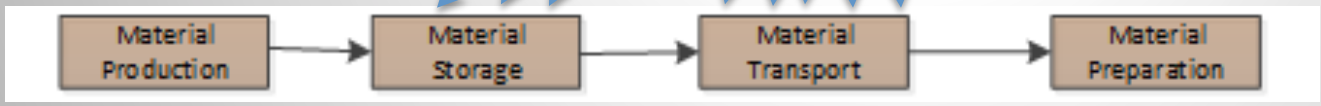
Production Risks

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

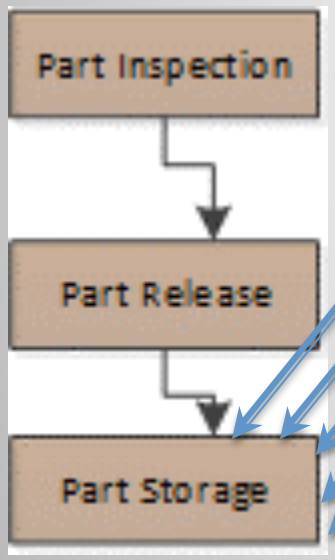


Material Handling Risks

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

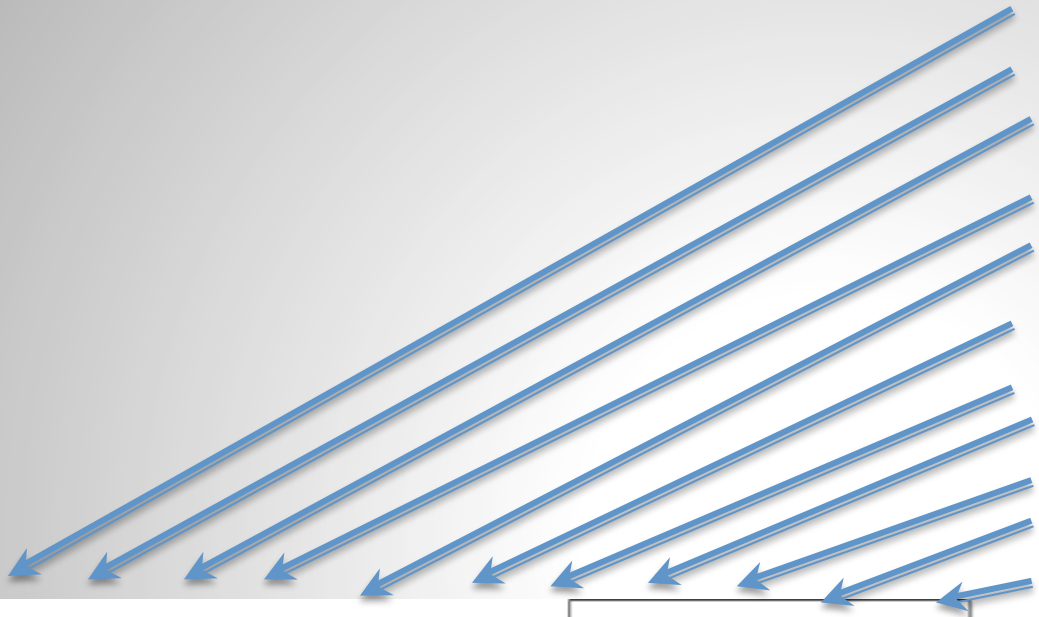


Post Production and Storage Risks

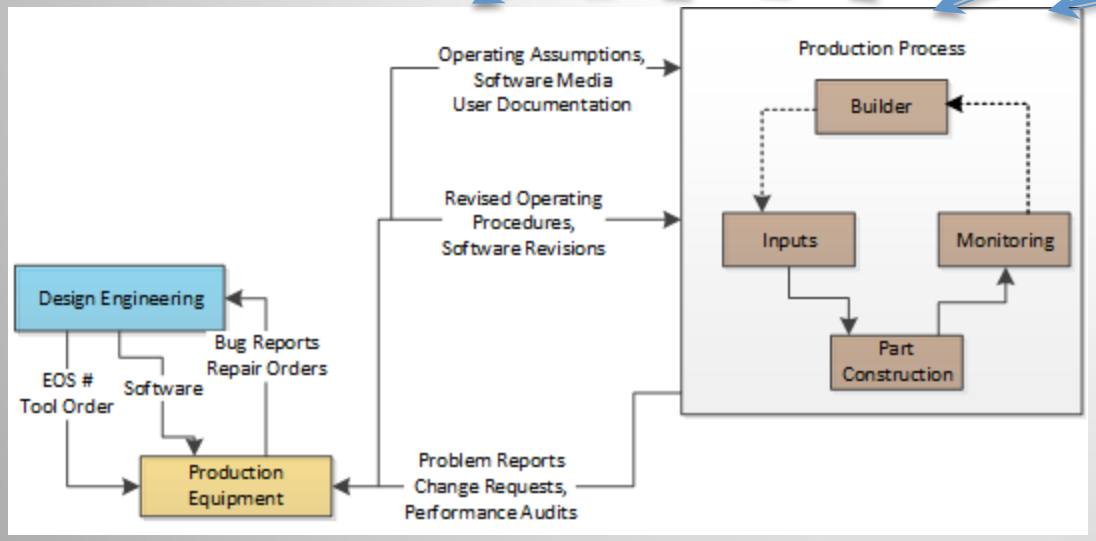


PPR1. Volatility Considerations
PPR2. Theft Security
PPR3. Maintain Interior Atmosphere
PPR4. Failed Inspection Process
PPR5. Inventory Tracking Accurate
PPR6. Cyber Security of Tracking System

Environmental Risks

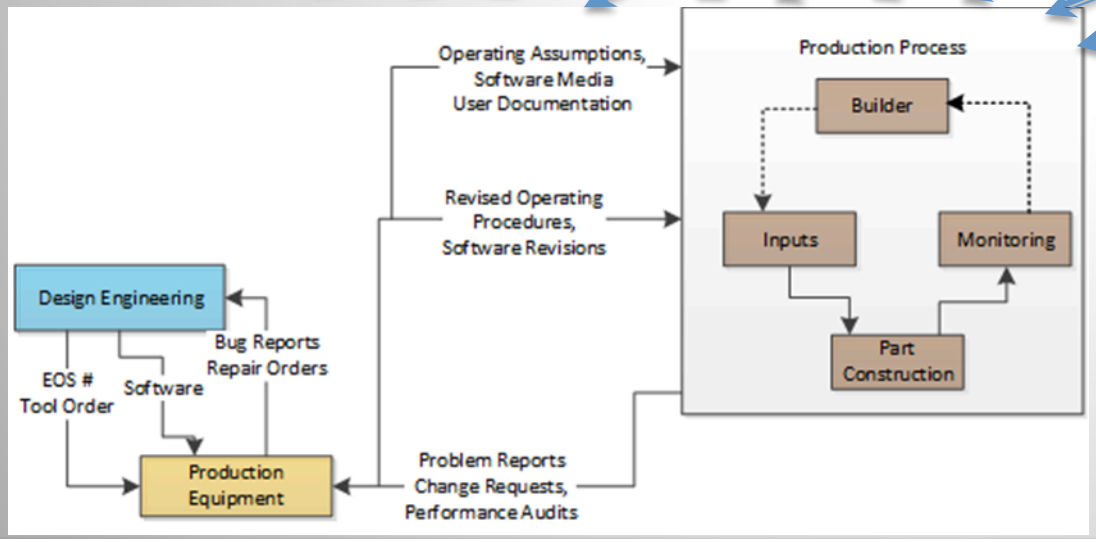


ER1. Earthquake
ER2. Flood
ER3. Tsunami
ER4. Hurricane
ER5. Tornado
ER6. Wild Fire
ER7. Reservoir Splushing
ER8. Volcano
ER9. Lightning
ER10.Sinkhole
ER11 Blizzard, Ice, Hail Storm

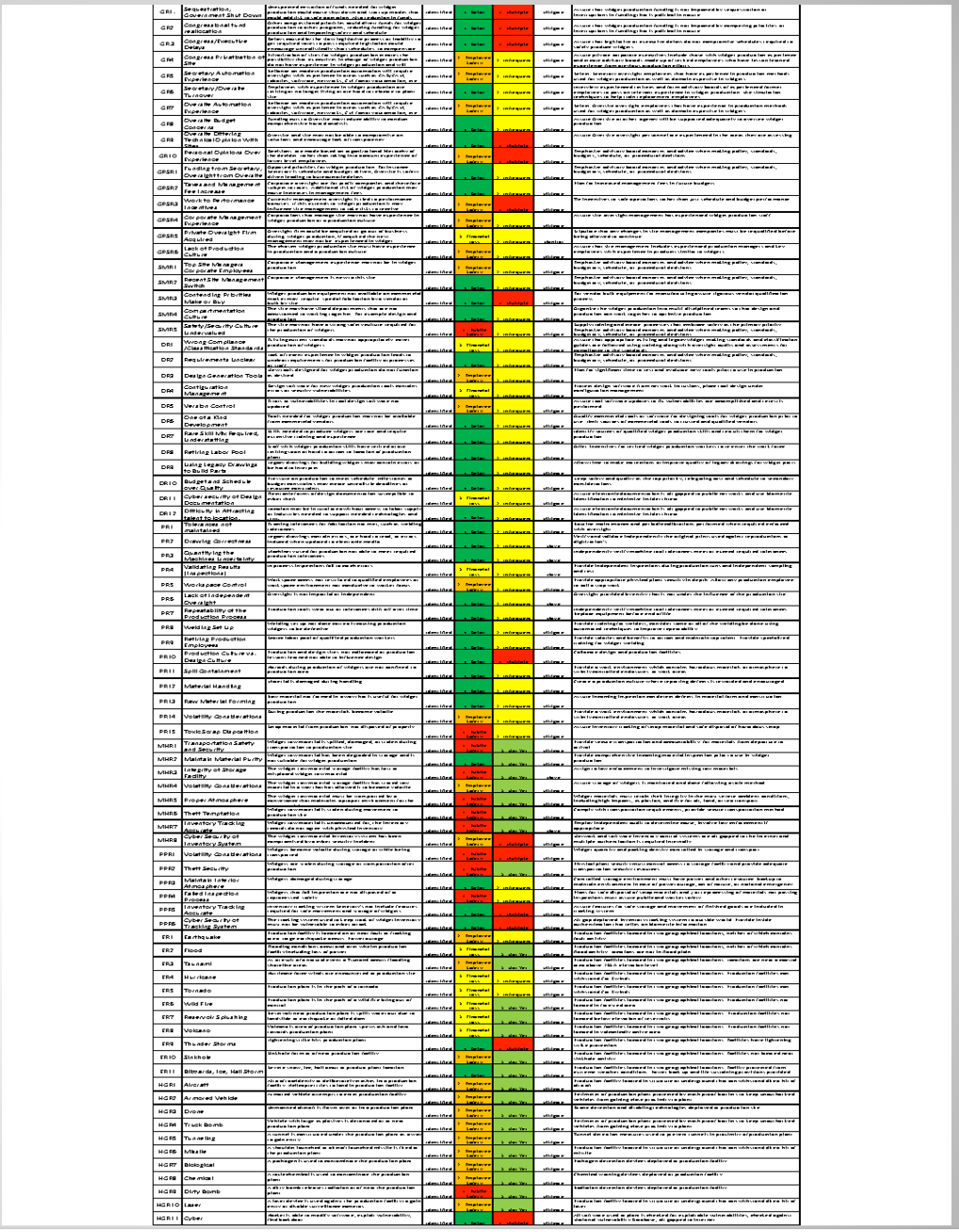


Human Generated Risks

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



Risk Tracker for 84 Risks



Government Entity Risks

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	Identified	4- Delay	1 - Multiple	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	4- Delay	1 - Multiple	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	4- Delay	1 - Multiple	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	2- Employee Safety	2- Infrequent	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, CIM factory automation, etc	Identified	2- Employee Safety	2- Infrequent	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	4- Delay	2- Infrequent	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, CIM factory automation, etc	Identified	2- Employee Safety	2- Infrequent	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	4- Delay	2- Infrequent	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	4- Delay	1 - Multiple	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	2- Employee Safety	1 - Multiple	Mitigate	Emphasize advisory board concerns and advice when making policy, standards, budgets, schedule, or procedural decisions.

Government, Privatizing, Site Risks

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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	Mitigate	Plan for increased management fees in future budgets.
GPSR3	Work to Performance Incentives	If management oversight is tied to performance bonuses If and this extends to widget production it could influence site management to take risks to receive bonuses.	Identified	2 - Employee Safety	1 - Multiple	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	2 - Employee Safety	2 - Infrequent	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	3 - Financial Loss	2 - Infrequent	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 - Employee Safety	2 - Infrequent	Mitigate	Assure that site management includes experienced production managers and key employees with experience in products similar to widgets.

Site Management Risks

SMR1	Top Site Managers Corporate Employees	Corporate Management experience may not be in widget production.	Identified	2 - Employee Safety	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	1 - Multiple	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	4 - Delay	2 - Infrequent	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	1 - Public Safety	2 - Infrequent	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

DR1	Wrong Compliance /Classification Standards	Existing current standards may not appropriately cover production of widgets.	Identified	3- Financial Loss	2- Infrequent	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	4 - Delay	2- Infrequent	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	2- Employee Safety	2- Infrequent	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- Infrequent	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	2- Employee Safety	2- Infrequent	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	4 - Delay	2- Infrequent	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	4 - Delay	2- Infrequent	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	4 - Delay	2- Infrequent	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	4 - Delay	2- Infrequent	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	4 - Delay	2- Infrequent	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- Infrequent	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	4 - Delay	2- Infrequent	Mitigate	Assure electronic documentation is air gapped to public networks and use biometric identification to minimize insider threat.

Production Risks

PR1	Tolerances not maintained	Exacting tolerances for fabrication not met, such as welding tolerances.	Identified	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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 - Infrequent	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	2- Employee Safety	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	1 - Multiple	Mitigate	Collocate design and production facilities.
PR11	Spill Containment	Hazards during production of widgets are not confined to production area.	Identified	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	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	4 - Delay	2 - Infrequent	Mitigate	Assure incoming inspection can detect defects in material form and construction.
PR14	Volatility Considerations	During production the materials become volatile.	Identified	2- Employee Safety	2 - Infrequent	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	1 - Public Safety	2 - Infrequent	Mitigate	Assure inventory tracking of scrap material and safe disposal of hazardous scrap.

Material Handling Risks

MHR1	Transportation Safety and Security	Widget raw material is spilled, damaged, or stolen during transportation to production site.	Identified	1 - Public Safety	3 - Not Yet	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	4 - Delay	3 - Not Yet	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	1 - Public Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	1 - Public Safety	3 - Not Yet	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	1 - Public Safety	3 - Not Yet	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	1 - Public Safety	3 - Not Yet	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	2 - Employee Safety	1 - Multiple	Mitigate	Network and software inventory control systems are air gapped to the internet and multiple authentication is required internally.

Post Production and Storage Risks

PPR1	Volatility Considerations	Widgets become volatile during storage or while being transported.	Identified	1 - Public Safety	1 - Multiple	Mitigate	Widget quantity and packing density controlled in storage and transport.
PPR2	Theft Security	Widgets are stolen during storage or transportation after production.	Identified	1 - Public Safety	3 - Not Yet	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	4 - Delay	2 - Infrequent	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	1 - Public Safety	2 - Infrequent	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	4 - Delay	1 - Multiple	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	4 - Delay	1 - Multiple	Mitigate	Air gap deployed inventory tracking system to outside world. Provide inside authentication that relies on biometric information.

Environmental Risks

ER1	Earthquake	Production facility is located on or near fault or fracking area. Large earthquake occurs. Power outage	Identified	2 - Employee Safety	2 - Infrequent	Mitigate	Production facilities located in two geographical locations, neither of which contains fault activity.
ER2	Flood	Flooding conditions occur and over whelm production facility including loss of power.	Identified	3 - Financial Loss	3 - Not Yet	Mitigate	Production facilities located in two geographical locations, neither of which contains flood activity. Locations are not in flood plain.
ER3	Tsunami	As a result of a natural event a Tsunami occurs flooding shoreline areas.	Identified	2 - Employee Safety	3 - Not Yet	Mitigate	Production facilities located in two geographical locations. Locations are near a coastal area above 250ft elevation level.
ER4	Hurricane	Hurricane force winds are encountered at production site.	Identified	3 - Financial Loss	2 - Infrequent	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 - Infrequent	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	3 - Not Yet	Mitigate	Production facilities located in two geographical locations. Production facilities not located in forested area.
ER7	Reservoir Splushing	Reservoir near production plant is spills water out due to landslide or earthquake or failed dam.	Identified	3 - Financial Loss	3 - Not Yet	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.	Identified	3 - Financial Loss	3 - Not Yet	Mitigate	Production facilities located in two geographical locations. Production facilities not located in volcanically active area.
ER9	Thunder Storms	Lightening strike hits production plant	Identified	4 - Delay	1 - Multiple	Mitigate	Production facilities located in two geographical locations. Facilities have lightening strike protection.
ER10	Sinkhole	Sinkhole form at of near production facility	Identified	2 - Employee Safety	3 - Not Yet	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	4 - Delay	3 - Not Yet	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

HGR1	Aircraft	Aircraft accidently or deliberately crashes into production facility. Helicopter tries to land in production facility.	Identified	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	Mitigate	Pathogen detection devices deployed at production facility.
HGR8	Chemical	A toxic chemical is used to contaminate the production plant	Identified	2 - Employee Safety	3 - Not Yet	Mitigate	Chemical warning devices deployed at production facility.
HGR9	Dirty Bomb	A dirty bomb releases radiation at of near the production plant	Identified	1 - Public Safety	3 - Not Yet	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	2 - Employee Safety	3 - Not Yet	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	4 - Delay	1 - Multiple	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.