Risk Management Using STPA
Restarting Widget Production

STAMP Workshop, MIT March 26, 2019

Gregory Pope CSQE
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 Responses 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 shutdown and start-up modes that could add risk to safe operation. Also, reduction in funds. | Identified | 4-Delay | 1-Multiple | Mitigate | Ensure 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 | Ensure that widget production funding is not impacted by competing priorities or interruptions in funding that is political in nature. |
| GR3 | 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 | Ensure 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-Infrquent | Mitigate | Ensure 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 | 2-Employee, Safety | 2-Infrquent | Mitigate | Select Secretary oversight employees that have experience in production methods used for widget production as well as domain expertise in widgets. |
| GR6 | Secretary/Overseers Turnover | Employees with experience in widget production are retiring or no longer living or are hard to relocate in plants. | Identified | 4-Delay | 2-Infrquent | 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 | Overseers 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 | 2-Employee, Safety | 2-Infrquent | Mitigate | Select Overseers oversight employees that have experience in production methods used for widget production as well as domain expertise in widgets. |
| GR8 | Overseers Budget Concerns | Funding cuts to Overseers may reduce ability to conduct comprehensive hazard analysis. | Identified | 4-Delay | 2-Infrquent | Mitigate | Ensure Overseers or other agencies will be supported adequately to oversee widget production. |
| GR9 | Overseers Differing Technical Opinion With CEO | Overseers and CEO may not be able to compromise on solutions and encourage lack of transparency. | Identified | 4-Delay | 1-Multiple | Mitigate | Ensure Overseers oversight personnel are experienced in the areas they are assessing. |
| GR10 | Personal Opinions Over Experience | Decisions are made based on organizational hierarchy of the CEO 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

<table>
<thead>
<tr>
<th>GPR1</th>
<th>Funding from Secretary, Oversight from Overtime</th>
<th>Opposed priorities for widget production. For instance, Secretary is schedule and budget driven, Oversight is safety driven leading to bureaucratic delays.</th>
<th>Identified</th>
<th>4 - Delay</th>
<th>2 - Infrequent</th>
<th>Mitigate</th>
<th>Emphasize advisory board concerns and advice when making policy, standards, budgetary, schedule, or procedural decisions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPR2</td>
<td>Taxes and Management Fee Increase</td>
<td>Corporate oversight are for profit companies and therefore subject to taxes. Additional risk of widget production may cause increases in management fees.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Plan for increased management fees in future budgets.</td>
</tr>
<tr>
<td>GPR3</td>
<td>Work to Performance Incentives</td>
<td>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.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>1 - Multiple</td>
<td>Mitigate</td>
<td>Tie incentives to safe operations rather than just schedule and budget performance.</td>
</tr>
<tr>
<td>GPR4</td>
<td>Corporate Management Experience</td>
<td>Corporations that manage site may not have experience in widget production or a production culture.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Assure site oversight management has experienced widget production staff.</td>
</tr>
<tr>
<td>GPR5</td>
<td>Private Oversight Firm Acquired</td>
<td>Oversight firm could be acquired or go out of business during widget production, if acquired the new management may not be experienced in widget production.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>2 - Infrequent</td>
<td>Monitor</td>
<td>Stipulate that any changes in site management companies must be requalified before being allowed to continue.</td>
</tr>
<tr>
<td>GPR6</td>
<td>Lack of Production Culture</td>
<td>The chosen widget production site must have experience in production and a production culture.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Assure that site management includes experienced production managers and key employees with experience in products similar to widgets.</td>
</tr>
</tbody>
</table>
## Site Management Risks

<table>
<thead>
<tr>
<th>SMR</th>
<th>Risk Description</th>
<th>Impact and Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMR1</td>
<td>Top Site Managers Corporate Employees</td>
<td>Corporate Management experience may not be in widget production.</td>
</tr>
<tr>
<td>SMR2</td>
<td>Recent Site Management Switch</td>
<td>Corporate Management is new to this site.</td>
</tr>
<tr>
<td>SMR3</td>
<td>Contending Priorities Make or Buy</td>
<td>Widget production equipment not available on commercial market may require special fabrication by a vendor or built by site.</td>
</tr>
<tr>
<td>SMR4</td>
<td>Compartmentation Culture</td>
<td>The site may have siloed departments that are not accustomed to working together. For example design and production.</td>
</tr>
<tr>
<td>SMR5</td>
<td>Safety/Security Culture Undervalued</td>
<td>The site may not have a strong safety culture required for the production of widgets.</td>
</tr>
</tbody>
</table>
## Development Risks

<table>
<thead>
<tr>
<th>DR1</th>
<th>Wrong Compliance /Classification Standards</th>
<th>Identified</th>
<th>Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR2</td>
<td>Requirements Unclear</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR3</td>
<td>Design Generation Tools</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR4</td>
<td>Configuration Management</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR5</td>
<td>Version Control</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR6</td>
<td>One of a Kind Development</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR7</td>
<td>Rare Skill Mix Required, Understaffing</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR8</td>
<td>Retiring Labor Pool</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DR9</td>
<td>Using Legacy Drawings to Build Parts</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DRL0</td>
<td>Budget and Schedule over Quality</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DRL1</td>
<td>Cyber security of Design Documentation</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
<tr>
<td>DRL2</td>
<td>Difficulty in Attracting talent to location.</td>
<td>Identified</td>
<td>Mitigate</td>
</tr>
</tbody>
</table>

- **DR1**: Wrong Compliance /Classification Standards - Existing current standards may not appropriately cover production of widgets.
  - Identified: 3. Financial Loss, 2. In frequent
  - Mitigate: Ensure 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 don't 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: Ensure tool software updates 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: Quality 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 workforce.

- **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.

- **DRL0**: 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.

- **DRL1**: Cyber security of Design Documentation - Electronic forms of design documentation susceptible to cyber theft.
  - Identified: 3. Financial Loss, 2. Infrequent
  - Mitigate: Ensure electronic documentation is airgapped to public networks and use biometric identification to minimize insider threat.

- **DRL2**: Difficulty in Attracting talent to location. - Location may be in rural areas without access to labor supply or industries needed to support needed technologies and skills.
  - Identified: 4. Delay, 2. Infrequent
  - Mitigate: Ensure electronic documentation is airgapped to public networks and use biometric identification to minimize insider threat.
# Production Risks

<table>
<thead>
<tr>
<th>PR</th>
<th>Description</th>
<th>Identified</th>
<th>Frequency</th>
<th>Mitigate</th>
<th>Mitigation Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR1</td>
<td>Tolerances not maintained</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Routine maintenance and periodic calibrations performed when required is enforced with oversight.</td>
</tr>
<tr>
<td>PR2</td>
<td>Drawing Correctness</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Verify and validate independently the original prints used against reproductions or digitizations.</td>
</tr>
<tr>
<td>PR3</td>
<td>Quantifying the Machines Uncertainty</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Independently verify machine tool tolerances meet or exceed required tolerances.</td>
</tr>
<tr>
<td>PR4</td>
<td>Validating Results (Inspections)</td>
<td>Identified</td>
<td>3-Financial Loss</td>
<td>2-In frequent</td>
<td>Provide independent inspections during production runs and independent sampling and test.</td>
</tr>
<tr>
<td>PR5</td>
<td>Workspace Control</td>
<td>Identified</td>
<td>2-Employee Safety</td>
<td>2-In frequent</td>
<td>Provide appropriate physical plant security in depth. Allow any production employee to call a stopwork.</td>
</tr>
<tr>
<td>PR6</td>
<td>Lack of Independent Oversight</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Oversight provided by entity that is not under the influence of the production site.</td>
</tr>
<tr>
<td>PR7</td>
<td>Repeatability of the Production Process</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Independently verify machine tool tolerances meet or exceed required tolerances. Replace equipment before end of life.</td>
</tr>
<tr>
<td>PR8</td>
<td>Welding Set Up</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Provide training for welders, consider some or all of the welding be done using automated techniques to improve repeatability.</td>
</tr>
<tr>
<td>PR9</td>
<td>Retiring Production Employees</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Provide salaries and benefits to attract and maintain top talent. Provide specialized training for welder.</td>
</tr>
<tr>
<td>PR10</td>
<td>Production Culture vs. Design Culture</td>
<td>Identified</td>
<td>4-Delay</td>
<td>1-Multiple</td>
<td>Collocate design and production facilities.</td>
</tr>
<tr>
<td>PR11</td>
<td>Spill Containment</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Provide a work environment which contains hazardous materials or atmosphere to strictly controlled enclosures or work areas.</td>
</tr>
<tr>
<td>PR12</td>
<td>Material Handling</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Create a production culture where reporting defects is rewarded and encouraged.</td>
</tr>
<tr>
<td>PR13</td>
<td>Raw Material Forming</td>
<td>Identified</td>
<td>4-Delay</td>
<td>2-In frequent</td>
<td>Assure incoming inspection can detect defects in material form and construction.</td>
</tr>
<tr>
<td>PR14</td>
<td>Volatility Considerations</td>
<td>Identified</td>
<td>2-Employee Safety</td>
<td>2-In frequent</td>
<td>Provide a work environment which contains hazardous materials or atmosphere to strictly controlled enclosures or work areas.</td>
</tr>
<tr>
<td>PR15</td>
<td>Toxic Scrap Disposition</td>
<td>Identified</td>
<td>1-Public Safety</td>
<td>2-In frequent</td>
<td>Assure inventory tracking of scrap material and safe disposal of hazardous scrap.</td>
</tr>
</tbody>
</table>
# Material Handling Risks

<table>
<thead>
<tr>
<th>MHR</th>
<th>Description</th>
<th>Identify</th>
<th>Nature</th>
<th>Mitigate/Move</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MHR1</td>
<td>Transportation Safety and Security: Widget raw material is spilled, damaged, or stolen during transportation to production site.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>Mitigate</td>
<td>Provide secure transportation and accountability for materials from departure to arrival.</td>
</tr>
<tr>
<td>MHR2</td>
<td>Maintain Material Purity: Widget raw material has been degraded in storage and is not suitable for widget production.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>Move</td>
<td>Provide comprehensive incoming material inspection prior to use in widget production.</td>
</tr>
<tr>
<td>MHR3</td>
<td>Integrity of Storage Facility: The widget raw material storage facility has lost or misplaced widget raw material.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>Move</td>
<td>Assign law enforcement to investigate missing raw materials.</td>
</tr>
<tr>
<td>MHR4</td>
<td>Volatility Considerations: The widget raw material storage facility has stored raw material in a way that has allowed it to become volatile.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>Move</td>
<td>Assure storage of widgets is monitored and done following a safe method.</td>
</tr>
<tr>
<td>MHR5</td>
<td>Proper Atmosphere: The widget raw material must be transported by a conveyance that maintains a proper environment for the raw material.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>Mitigate</td>
<td>Widget materials must retain their integrity in the most severe accident conditions, including high impacts, explosion, and fire for air, land, or sea transport.</td>
</tr>
<tr>
<td>MHR6</td>
<td>Theft Temptation: Widget raw material is stolen during movement to production site.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>Mitigate</td>
<td>Comply with transportation requirements, provide secure transportation method.</td>
</tr>
<tr>
<td>MHR7</td>
<td>Inventory Tracking Accurate: Widget raw material is unaccounted for, the inventory records do not agree with physical inventory.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>Move</td>
<td>Employ independent audit to determine cause, involve law enforcement if appropriate.</td>
</tr>
<tr>
<td>MHR8</td>
<td>Cyber Security of Inventory System: The widget raw material inventory system has been compromised by a cyber security incident.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>Mitigate</td>
<td>Network and software inventory control systems are air gapped to the internet and multiple authentication is required internally.</td>
</tr>
</tbody>
</table>
# Post Production and Storage Risks

<table>
<thead>
<tr>
<th>PPR1</th>
<th>Volatility Considerations</th>
<th>Widgets become volatile during storage or while being transported.</th>
<th>Identified</th>
<th>1 - Public Safety</th>
<th>1 - Multiple</th>
<th>Mitigate</th>
<th>Widget quantity and packing density controlled in storage and transport.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPR2</td>
<td>Theft Security</td>
<td>Widgets are stolen during storage or transportation after production.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Physical plant security must control access to storage facility and provide adequate transportation security resources.</td>
</tr>
<tr>
<td>PPR3</td>
<td>Maintain Interior Atmosphere</td>
<td>Widgets damaged during storage.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Controlled storage environment must have power and other resource backup to maintain environment in case of power outage, act of nature, or national emergency.</td>
</tr>
<tr>
<td>PPR4</td>
<td>Failed Inspection Process</td>
<td>Widgets that fail inspection are not disposed of or reprocessed safely.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Plans for safe disposal of scrap materials and/or reprocessing of materials not passing inspections must assure public and worker safety.</td>
</tr>
<tr>
<td>PPR5</td>
<td>Inventory Tracking Accurate</td>
<td>Inventory tracking system Secretary's not include features required for safe movement and storage of widgets.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>1 - Multiple</td>
<td>Mitigate</td>
<td>Assure features for safe storage and movement of finished goods are included in tracking system.</td>
</tr>
<tr>
<td>PPR6</td>
<td>Cyber Security of Tracking System</td>
<td>The tracking system used to keep track of widget inventory must not be vulnerable to cyber attack.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>1 - Multiple</td>
<td>Mitigate</td>
<td>Air gap deployed inventory tracking system to outside world. Provide inside authentication that relies on biometric information.</td>
</tr>
</tbody>
</table>
## Environmental Risks

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Risk Description</th>
<th>Identified</th>
<th>2 - Employee Safety</th>
<th>2 - Infrequent</th>
<th>Mitigate</th>
<th>Production Facility Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER1</td>
<td>Earthquake. Production facility is located on or near fault or fracking area.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Located in two geographical locations, neither of which contains fault activity.</td>
</tr>
<tr>
<td>ER2</td>
<td>Flood. Flooding conditions occur and overwhelm production facility including loss of power.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations, neither of which contains flood activity. Locations are not in floodplain.</td>
</tr>
<tr>
<td>ER3</td>
<td>Tsunami. As a result of a natural event, a tsunami occurs flooding shoreline areas.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Locations are near a coastal area above 250 ft elevation level.</td>
</tr>
<tr>
<td>ER4</td>
<td>Hurricane. Hurricane force winds are encountered at production site.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Production facilities can withstand Cat 5 winds.</td>
</tr>
<tr>
<td>ER5</td>
<td>Tornado. Production plant is in the path of a tornado.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>2 - Infrequent</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Production facilities can withstand Cat 5 winds.</td>
</tr>
<tr>
<td>ER6</td>
<td>Wild Fire. Production plant is in the path of a wild fire bringing out of control.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Production facilities not located in forested area.</td>
</tr>
<tr>
<td>ER7</td>
<td>Reservoir Sploshing. Reservoir near production plant spills water out due to landslide or earthquake or failed dam.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Production facilities not located below elevation of reservoirs.</td>
</tr>
<tr>
<td>ER8</td>
<td>Volcano. Volcano is area of production plant spews ash and lava towards production plant.</td>
<td>Identified</td>
<td>3 - Financial Loss</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Production facilities not located in volcanically active area.</td>
</tr>
<tr>
<td>ER9</td>
<td>Thunder Storms. Lightning strikes hit production plant.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>1 - Multiple</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Facilities have lightning strike protection.</td>
</tr>
<tr>
<td>ER10</td>
<td>Sinkhole. Sinkhole forms at near production facility.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Facilities not located near sinkhole activity.</td>
</tr>
<tr>
<td>ER11</td>
<td>Blizzards, Ice, Hail Storm. Severe snow, ice, hail occur at production plant location</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>3 - Not Yet</td>
<td>Mitigate</td>
<td>Located in two geographical locations. Facility protected from extreme weather conditions. Power back up and life sustaining provisions provided.</td>
</tr>
</tbody>
</table>
# Human Generated Risks

<table>
<thead>
<tr>
<th>HGR</th>
<th>Type</th>
<th>Description</th>
<th>Identified</th>
<th>Mitigate</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>HGR1</td>
<td>Aircraft</td>
<td>Aircraft accidently or deliberately crashes into production facility. Helicopter tries to land in production facility.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR2</td>
<td>Armored Vehicle</td>
<td>Armored vehicle attempts to enter production facility.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR3</td>
<td>Drone</td>
<td>Unmanned aircraft is flown over or into production plant.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR4</td>
<td>Truck Bomb</td>
<td>Vehicle with large explosives is detonated at or near production plant.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR5</td>
<td>Tunneling</td>
<td>A tunnel is constructed under the production plant as a way to gain entry.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR6</td>
<td>Missile</td>
<td>A shoulder launched or aircraft launched missile is fired at the production plant.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR7</td>
<td>Biological</td>
<td>A pathogen is used to contaminate the production plant.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR8</td>
<td>Chemical</td>
<td>A toxic chemical is used to contaminate the production plant.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR9</td>
<td>Dirty Bomb</td>
<td>A dirty bomb releases radiation at or near the production plant.</td>
<td>Identified</td>
<td>1 - Public Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR10</td>
<td>Laser</td>
<td>A laser device is used against the production facility to gain entry or disable surveillance cameras.</td>
<td>Identified</td>
<td>2 - Employee Safety</td>
<td>3 - Not Yet</td>
</tr>
<tr>
<td>HGR11</td>
<td>Cyber</td>
<td>Hacker is able to modify software, exploit vulnerability, find backdoor.</td>
<td>Identified</td>
<td>4 - Delay</td>
<td>1 - Multiple</td>
</tr>
</tbody>
</table>

- **Production facility located in structure or underground that can withstand direct hit of aircraft.**
- **Perimeter of production plant protected by crash-proof barriers to keep unauthorized vehicles from gaining close proximity to plant.**
- **Drones detection and disabling technologies deployed at production site.**
- **Tunnel detection measures used to prevent tunnels in proximity of production plant.**
- **Production facility located in structure or underground that can withstand direct hit of missile.**
- **Pathogen detection devices deployed at production facility.**
- **Chemical warning devices deployed at production facility.**
- **Radiation detection devices deployed at production facility.**
- **Production facility located in structure or underground that can withstand direct hit of laser.**
- **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.