Are We Doing It Wrong?

Jim McGlone, MBA, GICSP
CMO, Kenexis
In my lifetime seatbelts, crumple zones, power windows, airbags, more airbags, door lock knobs disappeared, drive by wire technology made my emergency brake a pushbutton, and now automatic collision avoidance
• What if something goes wrong
• Patch Tuesday
• Never mind, just patch everyday!
• How are we supposed to run the plant if we are patching, updating firmware, updating antivirus signatures
• Routable protocols are appearing on everything, even pressure and temperature transmitters
• Everything is digital, remotely programmable or configurable
• Now we have wireless and IoT stuff appearing
• Communication stacks have been hacked
• Remote Access Trojans have compromised control
• Safety Instrumented Systems have been hacked
• When is the last time you felt like you had this under control
• If we are trying to protect information in the office, what are we protecting in the plant?
  • Production, process, safety, machines, environment
  • Can it be segmented and categorized differently
  • Are some parts of production more important than others
  • Are some processes more important or dangerous
  • Are service level requirements at risk
  • MTTR to long
  • Is life at risk
  • Can it go boom
• Is it statistically possible to measure the risk of being attacked or of a malware infestation
• How do I make the business case for management
• We already measure the risk of critical processes using Process Hazards Analysis (PHA)
  • Common method is HAZOP
  • Most wet processes use it today
  • Established ISA84 & IEC61511
    • We must understand the process under control
    • We must understand under what circumstances control can be lost
    • We must know the consequences, causes, and safeguards for each scenario
Once the SCENARIO is known that can compromise a critical process:
- We can assess the risk
- Evaluate the SAFEGUARDS
- Determine if improved security measures are necessary for that SCENARIO
• Network device vulnerabilities alone do not tell us what the risk is to the plant
• Looking at the design of the network to determine what hazards are present is backwards
• It’s like looking at the Safety Instrumented System (SIS) to determine what risk to the process exist, we do not do that
• Cybersecurity is important, but not specific unless attached to a specific SCENARIO
• Cyber PHA, Cyber HAZOP, CHAZOP (Computer Hazards & Operability)
• These methods focus on vulnerabilities in network devices
• These methods are more like Failure Modes & Effects Analysis (FMEA)
  • Great tool for identifying flaws in design, doesn’t identify process hazard scenarios
• They lack an Initiating Event
• Have Infinite Potential Outcomes
• Unknowable Frequency of Attack
• Failure to Consider Inherent Safety

1. Identify an ICS asset
2. Identify a threat employing that asset
3. Identify a vulnerability allowing that threat to occur
4. Determine likelihood of attack
5. Determine consequence
6. Calculate risk
• Maybe we should be analyzing the process to verify at least one layer of protection for a SCENARIO cannot be hacked like the car example.
• Maybe we should argue that any industrial cybersecurity effort that begins with the network devices is focused on the wrong thing.
Security PHA Review

• Designed to either generate the cybersecurity performance targets for a zone or specify the recommendations for inherently cyber-secure layers of protection

• Developed by technical safety practitioners with a strong background in industrial controls implementation and cybersecurity

• Designed to fit with existing project life cycles of design, implementation, and operation of process plants while leveraging existing engineering tasks and reports generated for process safety

• Makes SL-T (ISA/IEC62443) selection similar to LOPA for SIL selection targets for SIF
Security PHA Review

• Can be done after a PHA, or as a step during we check each SCENARIO
  • Is the initiating event hackable
  • Microprocessors are hackable
  • Control loops, SIS functions, operator interface actions are all micro-based
  • Human operation manually opening a valve are not hackable yet
  • Mechanical safety devices like pressure relief valves are not hackable

• If all layers are hackable
  • Assign Security Level (SL) or recommend inherently safe device
Security PHA Review Benefits

• Lower risk to tolerable level based on lowering consequence of event
• Better understanding of attack vectors
• Make the right choices for the design you have
• Increased efficiency by extending existing studies
• Standards compliance by building on recognized and generally accepted good engineering practices
- **ISA/IEC 62443 Industrial Automation and Control Systems Security**
  - Significant collection of documents to support various security aspects

<table>
<thead>
<tr>
<th>General</th>
<th>Policies &amp; Procedures</th>
<th>System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>IEC 62443-1-1</strong> Concepts, and Models</td>
<td>• <strong>IEC 62443-2-1</strong> Requirements for an IACS Security Management System</td>
<td>• <strong>IEC 62443-3-1</strong> Security Technologies for IACS</td>
<td>• <strong>IEC 62443-4-1</strong> Product Development Requirements</td>
</tr>
<tr>
<td>• <strong>IEC 62443-1-2</strong> Master Glossary of Terms and Abbreviations</td>
<td>• <strong>IEC 62443-2-2</strong> Implementation Guidance for an IACS Security Management System</td>
<td>• <strong>IEC 62443-3-2</strong> Security Risk Assessment and System Design</td>
<td>• <strong>IEC 62443-4-2</strong> Technical Security Requirements for IACS Components</td>
</tr>
<tr>
<td>• <strong>IEC 62443-1-3</strong> System Security Compliance Metrics</td>
<td>• <strong>IEC 62443-2-3</strong> Patch Management in the IACS Environment</td>
<td>• <strong>IEC 62443-3-3</strong> System Security Requirements and Security Levels</td>
<td></td>
</tr>
<tr>
<td>• <strong>IEC 62443-1-4</strong> IACS Security Lifecycle and Use-Case</td>
<td>• <strong>IEC 62443-2-4</strong> Requirements for IACS Solution Suppliers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Process Hazards Analysis
- ~50 years old
- HAZOP is the most common method
- Facility is broken down into Nodes and every deviation like High Pressure, Low Temperature, Reverse Flow is considered
- If safeguards are inadequate, recommendations are made
Let’s Look at HAZOP quickly for those who might not be familiar...

1. Collect Process Safety Information (PSI)
   A. Piping and Instrumentation Diagrams (P&IDs)
   B. Process Flow Diagrams (PFDs)
   C. Process Block Flow Diagrams
   D. Material and Energy Balance (including stream compositions, temperatures, pressures, flow rates, etc.)
   E. Equipment Specification Sheets
   F. Instrumentation Specification Sheets
   G. Relief System Design Basis Documentation
   H. Cause-and-Effect Diagrams
2. Assess Deviations from Design Intent

A. Four deviations and eight process parameters (32 combinations) are common

B. It is possible to apply this to each piece of equipment, but it is impractical

C. Facilitators group equipment together into “Nodes” where the operating conditions of the equipment are similar

<table>
<thead>
<tr>
<th>Description</th>
<th>Intention</th>
<th>Session</th>
<th>Revision</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Operator Station</td>
<td>Allow the operators to interact with the process and view its operating condition.</td>
<td>Day 1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2 Safety PLC</td>
<td>Monitor the safety critical parameters of the plant and take action to move the process to a safe state if critical parameters are violated.</td>
<td>Day 1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3 Plant DCS</td>
<td>Take regulatory control actions to maintain the process in its normal operating condition, accept inputs from the operator station regarding state changes, and provide operating data to the plant historian</td>
<td>Day 2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4 Plant Historian</td>
<td>Obtain and record plant data. Communicate with operator stations and external devices to provide historical plant data</td>
<td>Day 2</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
3. P&IDs Marked to Provide a Visual Extent of a Node
4. HAZOP Team

A. Facilitator (a.k.a., leader or chairman)
B. Scribe (a.k.a, technical support engineer)
C. Operations
D. Operations Management
E. Process Engineering
F. Maintenance (including specific
G. Process Safety Management
H. Instrumentation and Controls Engineering
I. Specialty Equipment Engineering (e.g., rotating equipment, fired heaters)
5. Deviations

A. Analyze each deviation for each node and document the results of the discussion

B. Deviations vary for different industries

C. Process industries commonly use
   i. Pressure
   ii. Temperature
   iii. Level
   iv. Flow
   v. Composition
   vi. Viscosity

D. Guide words are used to drive deviations from design intent
   i. High (More)
   ii. Low (Less)
   iii. Reverse
   iv. Misdirected
   v. Other than
   vi. Abnormal
6. Scenarios & Consequences

A. Facilitator leads the team through a discussion about the first deviation, high pressure in this case
B. Team considers if there is a way to achieve high pressure above the design capabilities of the Node
C. If not, then it is documented and the team moves on
D. If it is possible to exceed maximum allowable working pressure, potential rupture of vessel, release of flammable material, potential fire or explosion, potential for single fatality for exposed personnel”

A. Then it is documented and assigned a Consequence Category based on the severity
7. Safeguards

A. Cause of high pressure might be excessive upstream pressure feeding into this process section, or an external fire near process equipment

B. All applicable safeguards are listed

<table>
<thead>
<tr>
<th>Safeguard</th>
<th>Safeguard Type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Relief valve PSV-101 opens to flare</td>
<td></td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>2 PT-101D high pressure shutdown closes HP separator inlet valve SDV-101</td>
<td></td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>3 Control valve PV-101B will open to flare</td>
<td></td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>4 Fire detection system allowing time for personnel evacuation</td>
<td></td>
<td>1.1.1.2</td>
</tr>
<tr>
<td>5 Control valve PV-101B will open to flare. No credit taken for this IPL due to inadequate sizing</td>
<td></td>
<td>1.1.1.2</td>
</tr>
<tr>
<td>6 PT-101D low pressure shutdown mitigates hazard by closing SDV-101</td>
<td></td>
<td>1.2.1.1</td>
</tr>
<tr>
<td>7 Automated low pressure shutdown upstream of the production header</td>
<td></td>
<td>1.2.1.1</td>
</tr>
<tr>
<td>8 High level shutdown LT-101B closes inlet valve SDV-101</td>
<td></td>
<td>1.5.1.1</td>
</tr>
</tbody>
</table>
8. Likelihood

A. Team makes an assessment of the likelihood that the event, and its associated consequence, will occur considering all of the safeguards that are available.
9. Risk

A. The overall risk posed by the scenario is a function of the combination of consequence and likelihood.

B. Each intersection represents a statement about tolerable risk of the Consequence and Likelihood pair.

C. If the consequence severity was a category 4 and the likelihood was a category 1, then the table shows an orange risk level 2.

D. If this is unacceptable to the plant, then recommendations must be made to lower the risk to an acceptable level.
Security PHA Review

• Identify the locations where safeguards that are inherently safe against cyber-attack should be deployed or an increased security level should be put in place

• Another PHA or HAZOP is not required, a small cybersecurity team can accomplish the task maybe with an I&C technician

• Each scenario is reviewed to determine if a pathway that is subject to exploitation via cyber-attack (i.e., “hackable”) exists
  • Review all the scenarios and their safeguards to see if they are hackable
  • Spring-based safeguards are not hackable
  • Valves physically operated by humans are not hackable yet
  • Microprocessor-based controls with routable protocols are hackable
Security PHA Review

Flowchart

Start

- Obtain PHA Report
- Identify Scenario
- Identify Scenario Cause
- Is the Cause Hackable?
  - Yes
    - Identify Scenario
    - Identify Scenario Cause
    - Identify First Safeguard
    - Is the Safeguard Hackable?
      - Yes
        - More Safeguards?
          - Yes
            - Identify Consequence
            - Consequence Significant?
              - Yes
                - Add Non-Hackable Safeguard?
                  - Yes
                    - Select Highest SL
                    - Assign SL
                  - Not Feasible
                    - Document Recommendation for SL Target
              - No
                - Document as NO CONCERN – Next Scenario
          - No
            - Document Recommendation for Non-Hackable Safeguard
            - Document as NO CONCERN PENDING RECOMMENDATION – Next Scenario
    - No
      - Document as NO CONCERN – Next Scenario

- Is the Cause Hackable?
  - Yes
    - Identify First Safeguard
    - Identify Consequence
    - Consequence Significant?
      - Yes
        - Add Non-Hackable Safeguard?
          - Yes
            - Select Highest SL
            - Assign SL
          - Not Feasible
            - Document Recommendation for SL Target
      - No
        - Document as NO CONCERN – Next Scenario
  - No
    - Document as NO CONCERN – Next Scenario

Choose Recommended SL from Appendix 3 Safety Consequence Category Table

- More Scenarios
  - No
  - Select Highest SL

Table: Safety Consequence Category Table

<table>
<thead>
<tr>
<th>S</th>
<th>Category</th>
<th>Safety</th>
<th>Environment</th>
<th>Commercial</th>
<th>TRAIL</th>
<th>SL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>No signifi cant safety consequence</td>
<td>None</td>
<td>None</td>
<td>NA</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
<td>Minor injury – first aid</td>
<td>Minor release with minimal clean up requirements</td>
<td>$50,000</td>
<td>10-02</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Lost time injury, non-impairing, hospitalization</td>
<td>Moderate release with limited cleanup and moderate costs</td>
<td>$200,000</td>
<td>10-03</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Severe injury (hospitalization, dismemberment, amputation)</td>
<td>Moderate release with limited cleanup and moderate costs</td>
<td>$5 Million</td>
<td>10-04</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Single fatality</td>
<td>Large release with extensive clean up and damage to sensitive areas</td>
<td>$50 Million</td>
<td>10-05</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Very High</td>
<td>Multiple fatalities</td>
<td>Very large release with extensive clean up and damage to sensitive areas</td>
<td>$50 Million</td>
<td>10-06</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Very-Very High</td>
<td>Multiple, offline fatalities</td>
<td>Very-Very large release with extensive clean up and remediation ongoing for many years along with permanent damage to many sensitive areas</td>
<td>$5 Billion</td>
<td>10-07</td>
<td>4</td>
</tr>
</tbody>
</table>
• If the DEVIATION in the HAZOP includes at least one non-hackable safeguard like a spring-based relief valve, then the deviation cannot be generated through a cyber-attack and is thus considered not hackable

• If you find that everything is hackable, you need to look at the CONSEQUENCES to determine if that deviation results in a significant consequence
  • If the CONSEQUENCE is acceptable, that attack vector is essentially a nuisance that is best left to traditional cyber-security
  • If the CONSEQUENCE is significant and not acceptable, then it is incumbent upon the analyst to make a recommendation to add a non-hackable safeguard or establish a Security Level (SL) based on the organizations tolerable risk criteria
  • SL is chosen from an example chart like the one on the next page...
- Risk reduction is expensive so practical measures are used
- Individual Risk of Fatality (IR)
- As Low As Reasonable Possible (ALARP)
- Target Maximum Event Likelihood (TMEL)
- Typical risk tolerance criteria will be developed using a scenario-based fatality TMEL of $1 \times 10^{-5}$ per year
- $10^{-5}$ or $1 \times 10^{-5}$ is 1 in 100,000
• Security PHA Review documented, using paper and highlighters
### Security PHA Review documentation, new document

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1 Failure of FIC-202, Quench After Bed #1, such that the valve goes to the</td>
<td></td>
<td></td>
<td>Operator intervention based on high outlet temperature alarms TAH-204, TAH-205, TAH-206, TAH-207</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>closed position and the quench flow is stopped</td>
<td>DCS</td>
<td>Yes</td>
<td></td>
<td>DCS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operator intervention based on low quench flow alarm – FAH-201</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Instrumented Function UZC-207 Stopping Inlet Flow Upon Detection of High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature</td>
<td>DCS</td>
<td>Yes</td>
<td></td>
<td>DCS</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deviation</td>
<td>Consequence</td>
<td>S</td>
<td>L</td>
<td>RR</td>
<td>LOPA Required</td>
<td>Cause</td>
<td>Cause Hackable</td>
<td>Safeguards</td>
<td>Safeguard Hackable</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---</td>
<td>---</td>
<td>----</td>
<td>--------------</td>
<td>-------</td>
<td>---------------</td>
<td>------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1.5 High Level</td>
<td>1.5.1 Potential overfill of the High Pressure Separator M-101 with liquid flow to the Gas Export Pipeline. Potential for Off-Spec product.</td>
<td>0 ▼</td>
<td>2 ▼</td>
<td>0 ▼</td>
<td>1.5.1.1 Failure of control loop LIC-101 such that liquid outlet valve is too much closed.</td>
<td>Yes △</td>
<td>8 High level shutdown LT-101B closes inlet valve SDV-101</td>
<td>Yes △</td>
<td>Yes △</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5.1.2 Failure of shutdown valve SDV-102A to the closed position.</td>
<td>Yes △</td>
<td>9 Operator response to high level alarm LT-101A - not independent from control loop failure</td>
<td>Yes △</td>
<td>Yes △</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5.1.3 Slug greater than 90 bbl from production header.</td>
<td>No ▼</td>
<td>9 Operator response to high level alarm LT-101A - not independent from control loop failure</td>
<td>No ▼</td>
<td>No ▼</td>
</tr>
<tr>
<td>1.6 Low Level</td>
<td>1.6.1 Potential for gas blowby into the Low Pressure Separator V-102. Potential for overpressure of Low Pressure Separator. Potential for loss of mechanical integrity. Potential for rupture of vessel or piping.</td>
<td></td>
<td></td>
<td></td>
<td>1.6.1.1 Failure of control loop LIC-101A such that valve is too much open</td>
<td>10 Relief valve PSV-102, which is sized for gas blow-by</td>
<td>No ▼</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11 Low level shutdown LT-101B closes low pressure separator inlet SDV-102A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Tank Reactor Runaway Reaction
  • Continuously Stirred Tank Reactor (CSTR) producing a highly reactive chemical compound
  • Reactor is charged with a fixed quantity of Reactant A
  • After reactant A has been completed charged, the agitator (i.e., mixer) is started, and cooling water is introduced into the cooling water jacket
  • After cooling and agitation are established, Reactant B is added to the reactor at a slow and controlled rate
  • After a set period of time, all of Reactant A is consumed by the addition of Reactant B, and the reactor vessel is left containing the reaction product, Product C
  • The product is drained from the tank reactor and sent downstream for further processing
• Tank Reactor Runaway Reaction
  • Simplified P&ID of the batch chemical reaction process
• Tank Reactor Runaway Reaction
  • Cooling water failure causes reactor to increase
  • Increased temperature increases reaction rates and runaway
  • Once the runaway reaction starts it can no longer be stopped by re-establishing the flow of cooling water
  • Causes a significant pressure increase as Product C decomposes into gaseous by-products
  • Pressure in the reactor vessel will quickly rise in excess of the maximum allowable working pressure of the vessel causing it to rupture
  • Vessel rupture is also expected to result in a fire and vapor cloud explosion in addition to the physical explosion of the pressure vessel
• Tank Reactor Runaway Reaction
• HAZOP

<table>
<thead>
<tr>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>S</th>
<th>L</th>
<th>RR</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 High Pressure</td>
<td>8.1.1 Failure of Cooling Water Pump P-403, which results in loss of cooling water flow to Cooling Jacket E-402 of Reactor R-401</td>
<td>8.1.1.1 Once the flow of cooling water is stopped, the heat of reaction begins to build up in the reactor, resulting in temperatures. A runaway reaction will then start resulting in thermal decomposition of Product C into gaseous byproducts and a rapid increase in pressure in the reactor beyond the Maximum Allowable Working Pressure (MAWP). Loss of containment of process material with physical explosion. Potential fire and potential vapor cloud explosion. Potential single fatality is expected to operator or maintenance in area of reactor.</td>
<td>H</td>
<td>M</td>
<td>3</td>
<td>Safety Instrumented Function UZC-402 Dumping the reactor contents into the quench vessel which stops the reaction.</td>
</tr>
</tbody>
</table>
• **Tank Reactor Runaway Reaction**
  • SPR begins with an analysis of the initiating event
  • Failure of a cooling water pump such that flow of cooling water stops flowing to the reactor cooling jacket
  • Unlikely cyber-attack could cause the pump to fail, a cyber-attack could cause the pump to stop if any start/stop functionality is included in the control system or the safety instrumented system, which is quite likely in a batch process
  • Initiating event is determined to be hackable.

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Location</th>
<th>Hackable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of Cooling Water Pump P-403, which results in loss of cooling water flow to Cooling Jacket E-402 of Reactor R-401</td>
<td>DCS</td>
<td>Yes</td>
</tr>
</tbody>
</table>
• Tank Reactor Runaway Reaction
  • There is only one safeguard which is a Safety Instrumented Function (SIF)
  • The SIF is determined to be hackable because it resides in a SIS that is based on a programmable logic controller
  • If the control system were taken over by an attacker, the output of the SIF could be frozen in an energized state, preventing the dump valve from opening

<table>
<thead>
<tr>
<th>Safeguard</th>
<th>Location</th>
<th>Hackable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Instrumented Function UZC-402 Dumping the reactor contents into the quench vessel which stops the reaction.</td>
<td>SIS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

ALL SAFEGUARDS HACKABLE? | YES
• Tank Reactor Runaway Reaction
  • Next step is assign SL based on Consequence Category
  • Potential for a single fatality as the result of the fire and explosion that could accompany the loss of containment

<table>
<thead>
<tr>
<th>S</th>
<th>Category</th>
<th>Safety</th>
<th>Environment</th>
<th>Commercial</th>
<th>TMEL</th>
<th>SL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>No significant safety consequence</td>
<td>None</td>
<td>None</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
<td>Minor injury - first aid</td>
<td>Small release with minimal clean up requirements</td>
<td>$50,000</td>
<td>1E-02</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Lost time injury not requiring extended hospitalization</td>
<td>Moderate release limited to onsite damage with moderate clean-up effort</td>
<td>$500,000</td>
<td>1E-03</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Severe injury (extended hospitalization, dismemberment)</td>
<td>Large release with limited offsite impact requires significant onsite clean up</td>
<td>$5 Million</td>
<td>1E-04</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Single fatality</td>
<td>Large release offsite on extensive clean up and damage to sensitive areas</td>
<td>$50 Million</td>
<td>1E-05</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Very High</td>
<td>Multiple fatalities</td>
<td>Very large release off site with extensive clean up and permanent damage to several sensitive areas</td>
<td>$500 Million</td>
<td>1E-06</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Very-Very High</td>
<td>Multiple Offsite Fatalities</td>
<td>Very-Very large release offsite with extensive clean up and remediation ongoing for many years along with permanent damage to many sensitive areas</td>
<td>$5 Billion</td>
<td>1E-07</td>
<td>4</td>
</tr>
</tbody>
</table>
• Tank Reactor Runaway Reaction
  • Sometimes in situations like this, the team may recommend the use of a non-hackable safeguards so that the scenario consequence does not unduly increase the required SL
  • Upon review of the common non-hackable safeguards, it is determined that no self-contained mechanical device will prevent the scenario under consideration
• Tank Reactor Runaway Reaction
  • Analog “mimic” of the SIF UZC-403 will employ the second thermocouple of a dual element thermocouple set in the existing thermowell
  • Wired to an analog temperature transmitter that will convert the temperature measurement to a 4-20 mA signal
  • 4-20 Ma signal will be analyzed by an analog current monitor relay that will open a contact in the 24 VDC signal to the solenoid valve for UZV-403, de-energizing the solenoid, venting the valve’s actuator, and causing the valve to go to the open position
  • Entire analog “mimic” is inherently safe against cyber-attack, and any cyber-attack that is waged on the digital complement (UZC-207) will be not interfere in the safety functionality of the analog “mimic” function
• Tank Reactor Runaway Reaction
  • Analog “Mimic” of the digital SIF
• Non-hackable Safeguards
  • Analog “Mimic” of a Digital SIF
• Non-hackable Safeguards
  • Pressure Relief Valve, Rupture Disc
  • Buckling Pin, Check Valve
• Non-hackable Safeguards
  • Mechanical Overspeed, Current Relay

CENTRIFUGAL FORCE OVERCOMES THE SPRING AND ROD SLIDES OUT TO TRIP THE SWITCH
• Non-hackable Safeguards
  • Excess Flow Check Valve
In this session...

- Described the problem and made the case for doing it differently
- We described a Security PHA Review
- We explained how a HAZOP works
- We showed how to perform a SPR on a HAZOP
- We provided a real world scenario
- We threw in a few non-hackable systems for consideration
• Final Thoughts
  • We know we can connect everything
    • But should we
    • Does every device need to be remotely controllable or programmable