A Semi-Quantitative Risk Assessment Technique for Cyber Security Threats

Presented by
Owen Tavener-Smith, Director, Exida South Africa
Lizelle van der Walt, Senior Control Engineer, Sasol Technology

With contributions from
John Cusimano, Director Cyber Security, Exida LLC
Greg Chantler, Senior Safety Engineer, Exida South Africa

2012 Safety Control Systems Conference
Topics covered

• Background/Requirement, (Sasol Technology)
• Risk Management
• Threat hazard identification
• Consequence Analysis
• Frequency Analysis
• Countermeasures
• Evaluating SAL targets
• Challenges going forward
• Conclusion
• Benefits of semi-quantitative risk assessment, (Sasol Technology)
Background

Cyber threats are increasing in:
- Frequency
- Sophistication

Incidents can lead to:
- Loss of IP
- Production
- Integrity of safety systems
- Control system reliability
Process

Need
- Cyber security assessment process
- Quantify cyber security risks
- Provide platform for mitigation

Methodology
- Characterises threat types, their potential causes and define possible countermeasures
- To effectively protect against occurrence of consequences

Outcome
- Important step forward in the measurement of risk associated with cyber security hazards
PLCs Crashed by IT Security Audit

Date: 1995
Company: Undisclosed
Location: USA
Industry: Food & Bev
Incident type: Unintentional - Insider
Impact: Loss of Production >$1M

Description:
A security consultant was scanning the food companies business and process networks for vulnerabilities. Probe packets containing deliberately malformed entered the Ethernet-based process control network and caused all PLCs to hard fault. The packets contained malformed ICMP Redirects messages with a subcode of 4 or greater.
Browns Ferry Nuclear Plant Scrammed

Date: Aug. 2006
Company: Browns Ferry Nuclear
Location: Athens, AL, USA
Industry: Nuclear Power
Incident Type: Accidental Equipment Failure
Impact: Unit #3 shutdown

Description:
Operators manually scrammed Browns Ferry, Unit 3, following a loss of both the 3A and 3B reactor recirculation pumps. The root cause was the malfunction of the VFD controller due to excessive traffic on the plant Ethernet based integrated computer system (ICS) network.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)
Disgruntled Contractor Disables Pipeline Leak Detection System

Date: March 2009
Company: Pacific Energy Resources Ltd.
Location: Long Beach, CA, USA
Industry: Petroleum
Incident Type: External Hacker
Impact: Leak Detection System Disabled

Description:
A disgruntled employee, Mario Azar, accessed the system that monitors the detection of pipeline leaks for three oil derricks off the Southern California coast. He knowingly temporarily disabled the system.

The FBI announced that, on September 14, 2009, Mario Azar pleaded guilty to intentionally damaging a computer system used in interstate and foreign commerce and faced ten years in prison. His sentencing is scheduled for December 7 in the United States District Court of Los Angeles.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)
Hackers Penetrate Water System Computers

Date: October 2006
Company: Harrisburg Water System
Location: Harrisburg, PA, USA
Industry: Water & Wastewater
Incident Type: Intentional - External - Hacker
Impact: Unknown

Description:
A foreign-based hacker used the internet to infiltrate the laptop (via internet) of an employee at the Harrisburg water system. The hacker used the employee’s remote access as the entry point into the SCADA system and installed malware and spyware on a SCADA HMI computer.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)
The Impact of STUXNET, DuQu, Flame, Gauss…

- Provided proof-of-concept and a blueprint for hackers
- Stuxnet was designed to and did infiltrate the system front-end controllers, (PLC)
- Exposed corporate executives, regulators and the public to the potential dangers of cyber attacks on critical infrastructure
- Created a market for “security researchers” to identify and exploit control system vulnerabilities
Project Basecamp

• Announced at S4 Security Conference in Jan 2012
• Project Basecamp involved six researchers looking for vulnerabilities in six different embedded ICS devices (PLC’s, RTU’s, substation controllers)
• The researchers found backdoors, weak credential storage, ability to change ladder logic and firmware, buffer overflows, etc.
• Nessus plugins and Metasploit modules have been publically released enabling anyone to find and exploit these vulnerabilities
# Project Basecamp: Results

<table>
<thead>
<tr>
<th></th>
<th>A-B</th>
<th>Schneider Electric</th>
<th>GE</th>
<th>SEL</th>
<th>Koyo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Ladder Logic</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Backdoors</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Fuzzing</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Web</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Basic Config</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Exhaustion</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Undoc Features</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
</tbody>
</table>

Source: [http://www.digitalbond.com/2012/01/19/project-basecamp-at-s4/](http://www.digitalbond.com/2012/01/19/project-basecamp-at-s4/)
IACS Specific Vulnerabilities Reported 2001 - 2011

Source: Slide 25 from the presentation “Documenting the ‘Lost Decade’ An Empirical Analysis of publicly disclosed ICS vulnerabilities since 2001” by Sean McBride
Summary of Situation

• IACS products have rapidly evolved to incorporate COTS technology (Ethernet, Windows, SQL, webservers, etc.)
• Security was not a significant requirement when most systems were developed
• The threat environment is changing – more sophisticated, tools available for novices
• IACS vendors are just beginning to learn how to integrate security into their development lifecycle
• End-users and system integrators are often not aware or trained of cyber security risks to address them
• Systems are designed and installed with insufficient security controls (e.g. layers of protection)
Control System Security Standards

• IEC61508:2010-1: If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out, (refer IEC 62443).

• International Electrotechnical Commission (IEC)
  – IEC 62443 series of standards (equivalent to ISA 99)

• International Society for Automation (ISA)
  – ISA99, Industrial Automation and Control System (IACS) Security

• National Institute for Standards and Technology (NIST)
  – SP800-82 Guide to Industrial Control Systems (ICS) Security

• North American Electric Reliability Council (NERC)
  – NERC CIP-002 through CIP-009
ISA/IEC 62443 Security Lifecycle

Assess Phase
- Scope System and ID Critical Assets
- Establish Zones & Conduits (Conceptual Design)
- Analyze Security Risk for each Zone/Conduit (see threat-risk process)
- Security Requirements Specification (Assign SL-T to each Z&C)

Implement Phase
- Detailed Design
- Verification of Design (Achieved SL)
- Construction
- Validation (FAT and SAT)

Maintain Phase
- Maintain Security (Patch & A/V Mgmt)
- Monitor Security (IDS, SIEM, etc.)
- Modification or Decommissioning
- Periodic Assessments (SVA)

Repeat until security risk ≤ tolerable risk

Adapted from ISA S99.01.01
Cyber Security Event

The intentional or unintentional interference with the proper operation of industrial automation and control systems through the use of computers, networks, operating systems, applications and other programmable configurable components of the system.

• What it is
  – Malware,
  – Unauthorised intrusion,
  – Accidental.

• What it is not
  – Random hardware failure of IOM leads to….
  – Application software, (divide by zero) failure leads to…. 
Risk Management - Why

• Every business needs to manage risk
  – Identifying risk
  – Quantifying risk
  – Decision on how much can be tolerated

• Risk Receptors, (things we want to protect)
  – People
  – Environment
  – Assets
Security Risk

Risk = Likelihood x Consequence

SecurityRisk = Threat x Vulnerability x Consequence

SecurityRisk = Threat Freq x Threat Strength x Vulnerability x Consequence

**Threat Frequency (rate):**
How often will the threat occur
Represented as a rate (e.g. X times per year)

**Threat Strength (probability):**
The probability that the threat will find and penetrate existing vulnerabilities.

**Vulnerability (probability):**
The probability that a vulnerability exists that can be exploited. Also, (1-Strength of Countermeasures).
## Example Tolerable Risk Definition

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Safety</th>
<th>Financial</th>
<th>Env.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>&gt;1 fatalities</td>
<td>&gt;R100M</td>
<td>Long term national</td>
</tr>
<tr>
<td>-</td>
<td>a</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1 fatality</td>
<td>R10-100M</td>
<td>Long term regional</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Severe injury</td>
<td>R1-10M</td>
<td>Short term regional</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td>Minor injury</td>
<td>R.1-1M</td>
<td>Short term local</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Insignificant</td>
<td>&lt;R0.1M</td>
<td>Minor to none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency of consequence occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
<tr>
<td>&lt;=10,000 &lt;=1,000 &lt;=100 &lt;=10</td>
</tr>
</tbody>
</table>

- Less than 1 event in 1 year to 1 event in 10 years
- Between 1 in 10 and 1 in 100 years
Risk Assessment

Any well designed risk assessment methodology should include the following elements:

- Determining the assets that need to be protected (people, processes, equipment, information, etc.)
- Determining the consequence of a compromise for each of the assets (loss of production, health/safety impact, environmental impact, etc.)
- Determining the threats to those assets (theft, tampering, misuse, accidental misconfiguration, etc.)
- Determining the countermeasures that could be effective in prevention or mitigation of the consequence
- Calculating the residual risk
IACS Threat-based Risk Assessment Process

• Characterize the product or system
  • Model the system (zones & conduits)
  • Identify trust boundaries
  • Identify entry points and data flows
  • Document assumptions and external dependencies

• Identify Critical Assets and Consequences
  • Identify critical assets
  • Evaluate consequence of compromise

• Identify threats
  • Enumerate threats
  • Classify and evaluate threats

• Analyze threats
  • Identify vulnerabilities
  • Identify countermeasures
  • Assess the risk of each threat
Risk Assessment Inputs

• Scope definition and integration requirements with networks outside the scope
• IACS proposed architecture
• List of assets and asset functionality
• Important dataflows
• Existing cyber security countermeasures
Scope and Network Interfaces

**Business Zone**
- DUPONTNET Domain Controller
- DNS Server
- Manufacturing Message Bus Adaptors: SAP, EConnect
- PE Clients
- Corporate Patch Management Server

**Operations Management Zone**
- PCN Firewall
- Ethernet Switch
- IP 21 Server PM&C
- Manufacturing Application Server
- Process Explorer Clients
- Web 21 Server (optional)

**Process Control Zone**
- DCS AD Domain Controllers
- DCS Application Server
- DCS consoles
- Field Bus Gateway
- Process Explorer Clients

**Safety System Zone**
- Field Devices
- SIS
- Field Devices

**WAN**
- DUPONTNET Resource Domain Controllers

**LAN**
- Manufacturing Application Server
- Web 21 Server (optional)
- Process Explorer Clients

**OMN**
- Dupontnet Domain Controller
- Manufacturing Application Server
- Process Explorer Clients

**PCN**
- DUPONTNET Resource Domain Controllers
- Manufacturing Application Server
- DCS Application Server
- DCS consoles
- Field Bus Gateway
- Process Explorer Clients
Scope and Network Interfaces

**Business Zone**
- DUPONTNET Domain Controller
- DNS Server
- Manufacturing Message Bus Adaptors: SAP, EConnect
- Web.21 Server (optional)
- Corporate Patch Management Server

**Operations Management Zone**
- PCN Firewall
- Ethernet Switch
- IP.21 Server PM&C
- Manufacturing Application Server
- Process Explorer Clients
- PE Clients

**Process Control Zone**
- DCS AD Domain Controllers
- DCS Application Server
- DCS consoles
- Process Explorer Clients
- Field Bus Gateway

**Safety System Zone**
- Field Devices
- SIS

**Zones**
- Conduits
- LAN
- WAN
- PCN
- FBN

**Scope**
Identification of Cyber Security Hazards

• Threat hazard: the characterisation of a threat type which could lead to a credible loss of or compromised functionality of an IACS asset.

• Examples:
  – Denial of service resulting in loss of functionality of domain controller,
  – Tampering with resultant incorrect controller configuration and loss of intended functionality
  – Information disclosure of …leading to loss of competitive advantage

• Systematically create a list of all threat hazards for each asset within all zones within the scope.
Threat Hazard Risk Evaluation

1. Process begin
2. For each Threat Hazard
3. Define the worst credible consequence for the threat hazard
4. Define threats for each entry point
5. Assign the threat frequency for each threat per entry point
6. Identify IPLs for each threat and assign their effectiveness (PFD)
7. Calculate consequence frequency for each threat
8. Add the consequence frequencies for all threats associated with the threat hazard
9. Select the associated SAL from the Risk Matrix
10. Next threat hazard
11. End of process
Consequence Analysis

• Consideration of what could happen, (worst credible). Assume countermeasures have failed.
• Categorise the consequence into the most appropriate severity class for all relevant risk receptors.
• How to address consequences which could lead to loss of containment incidents with potential for safety, environmental as well as financial impact?
Safety/Environmental Consequences

- IACS control failures can lead to loss of containment consequences
- LOC consequences referred from prior SIL Determination analysis
- If the cyber security risk assessment indicates a consequence frequency < 0.1* “normal failure frequency” of controller then the risk is covered?
Frequency Analysis

• Risk: a function of consequence severity and frequency of occurrence.
• The threat or threat agent is the initiating event
• Vulnerabilities are weaknesses which threats can exploit
• Countermeasures are attributes of the IACS which can prevent the threat realising the consequence
• A weak system with little or no countermeasures will be vulnerable to threats
Threat Propagation Path

Countermeasures

Consequence occurrence

Threat

WHAT PART OF THE COMPUTER SEEMS TO BE CAUSING THE SECURITY PROBLEM?

THE NUT AT THE KEYBOARD!
Threat Propagation Path Contd.

Threat: Unauthorised Worker

Consequence: database deleted

<table>
<thead>
<tr>
<th>Threat</th>
<th>IPL PFD</th>
<th>IPL PFD</th>
<th>IPL PFD</th>
<th>Frequency of consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.003 per year</td>
</tr>
<tr>
<td>Medium</td>
<td>3 per year</td>
<td></td>
<td></td>
<td>~ once per 330 years</td>
</tr>
</tbody>
</table>

Are the countermeasures independent?
Threat Types

• Intentional threat types using the “STRIDE” model
  – Spoofing
  – Tampering,
  – Repudiation
  – Information disclosure
  – Denial of service
  – Elevation of privileges

• Unintentional threats include accidental misconfiguration when authorised worker performs routine maintenance
Threat Characterisation

• Threat Agents
  – Authorised worker, (non-malicious)
  – Unauthorised worker, (mischievous)
  – Outsider, (malicious)
  – Malware, (virus, worm, trojan horse)

• Entry points
  – Via conduit
  – Computer keyboard
  – Portable media
Scope, Trust Boundary & Entry Points

Entry Point: Conduit

Entry Points: Keyboard, Flash disc

Zone Trust Boundary
## Threat Characterisation

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Threat</th>
<th>Opportunity Frequency (per year)</th>
<th>Characterisation</th>
<th>Threat Frequency (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access via conduit from another zone, <em>(note: the threat is outside the zone)</em></td>
<td>Authorized Worker (non-malicious)</td>
<td>10</td>
<td>Makes configuration error on computer in another zone</td>
<td>0.1</td>
</tr>
<tr>
<td></td>
<td>Authorized Worker (non-malicious)</td>
<td>10</td>
<td>Task opportunity requires portable media and probability of infected media</td>
<td>0.1</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous)</td>
<td>30</td>
<td>Needs the skills in order to make a configuration modification</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous)</td>
<td>30</td>
<td>Probability of media infected could be high</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Outsider, (malicious)</td>
<td>0.3</td>
<td>No modification in frequency</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>30</td>
<td>There is a firewall and DMZ on the IACS trust boundary</td>
<td>3</td>
</tr>
<tr>
<td>Physical access via keyboard within zone</td>
<td>Authorized Worker (non-malicious)</td>
<td>10</td>
<td>Makes configuration error on computer in the zone</td>
<td>0.1</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous)</td>
<td>30</td>
<td>Needs the skills in order to make a configuration modification</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Outsider, (malicious)</td>
<td>0.3</td>
<td>This is considering physical intrusion.</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>30</td>
<td>Malware is not a valid threat via this entry point.</td>
<td>0</td>
</tr>
<tr>
<td>Usage of portable media within zone: -USB -CD/DVD -Cell phone</td>
<td>Authorized Worker (non-malicious)</td>
<td>10</td>
<td>Task opportunity requires portable media and probability of infected media</td>
<td>0.1</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous)</td>
<td>30</td>
<td>Probability of media infected could be high</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Outsider, (malicious)</td>
<td>0.3</td>
<td>This is considering physical intrusion. Probability of media infected would be high.</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>30</td>
<td>Not applicable since by itself malware cannot enter.</td>
<td>0</td>
</tr>
</tbody>
</table>
Countermeasures

• Techniques involving procedures and equipment specifically used to protect against cyber security hazards,

• Countermeasure effectiveness measured by probability of not protecting against a hazard, (probability of failure on demand – PFD).
Countermeasure Examples

• Physical access control
• Logical access control
• Portable media management
• Malicious code protection
• Organisational and operational controls
• Communications filtering
## Countermeasure Effectiveness

Measured by the probability of the countermeasure failing:

<table>
<thead>
<tr>
<th>Cyber Security Countermeasures</th>
<th>SAL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Physical access control</strong>&lt;br&gt;Measures to prevent unauthorized physical access to critical IACS assets.</td>
<td>Facility physical security only (e.g. perimeter fence, main gate, etc.)</td>
</tr>
<tr>
<td><strong>Logical access control</strong>&lt;br&gt;Measures to identify and authenticate users to prevent unauthorised logical access to entry points.</td>
<td>No authorisation</td>
</tr>
<tr>
<td><strong>Portable media management</strong>&lt;br&gt;Measures to control the connection of portable media (e.g. USB memory devices, external hard-drives, CD/DVDs, foreign laptops etc.)</td>
<td>No controls</td>
</tr>
<tr>
<td><strong>Malicious code prevention together with patch management</strong>&lt;br&gt;Measures to detect and prevent the execution of malicious or unauthorized code</td>
<td>No controls</td>
</tr>
<tr>
<td></td>
<td>Measures to manage and install security patches to mitigate known vulnerabilities</td>
</tr>
<tr>
<td><strong>Communication filtering</strong>&lt;br&gt;Measures to restrict communications in and out of an entry point</td>
<td>None</td>
</tr>
<tr>
<td><strong>Organizational and operational controls</strong>&lt;br&gt;Policies, procedures and practices to guide and encourage personnel to be vigilant about security together with competence assessment.</td>
<td>Basic policies exist</td>
</tr>
<tr>
<td><strong>Communications integrity and confidentiality</strong>&lt;br&gt;Measures to protect the integrity and confidentiality of data entering and exiting an entry point</td>
<td>None</td>
</tr>
</tbody>
</table>
Consequence Frequency

The consequence frequency is the frequency of the consequence with a given severity relating to a specific asset within the zone under evaluation.

It is the sum of all possible threats paths that could lead to the same consequence.

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Threat</th>
<th>Threat Frequency (per year)</th>
<th>Probability that cause can produce consequence</th>
<th>Segmented Architecture</th>
<th>Physical Access Control</th>
<th>Logical Access Control</th>
<th>Anti-Virus+</th>
<th>Consequence Frequency (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access via conduit from another zone, (note: the threat is outside the zone)</td>
<td>Authorized Worker (non-malicious) access via keyboard</td>
<td>0.1</td>
<td>0.3</td>
<td>1</td>
<td>1</td>
<td>0.1</td>
<td>1</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td>Authorized Worker (non-malicious) connection of portable media</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.001</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous) access via keyboard</td>
<td>3</td>
<td>0.3</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>1</td>
<td>0.009</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Worker, (mischievous) connection of portable media</td>
<td>24</td>
<td>1</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.024</td>
</tr>
<tr>
<td></td>
<td>Outsider, (malicious)</td>
<td>0.3</td>
<td>1</td>
<td>0.1</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0.0003</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>3</td>
<td>0.8</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.024</td>
</tr>
</tbody>
</table>
# Target SAL Evaluation

**Project Description:** Reference Architecture  
**Risk Assessment Date:** 29/08/2012

| Asset Name: Manufacturing Application Server | Zone: Operations Management |

**Threat Type:** Tampering or accidental loss of functionality  
(how the threat type can lead to loss/impaired functionality and incident outcome)

Intentional/accidental modification of configuration setting or disabling settings could cause changes to advanced control applications leading to reduced or loss of process optimisation and lower production yield.

## Threat Frequency:

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Threat Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Worker (non-malicious) access via keyboard</td>
<td>0.1</td>
</tr>
<tr>
<td>Authorized Worker (non-malicious) connection of portable media</td>
<td>0.1</td>
</tr>
<tr>
<td>Unauthorized Worker, (mischievous) access via keyboard</td>
<td>0.1</td>
</tr>
<tr>
<td>Unauthorized Worker, (mischievous) connection of portable media</td>
<td>3</td>
</tr>
<tr>
<td>Outsider, (malicious)</td>
<td>20</td>
</tr>
<tr>
<td>Malware</td>
<td>0.3</td>
</tr>
</tbody>
</table>

## Consequence:

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Personnel Safety</th>
<th>Community Safety</th>
<th>Financial</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>1 - 10 Million</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

## Entry Point

<table>
<thead>
<tr>
<th>Access via conduit from another zone, (note: the threat is outside the zone)</th>
</tr>
</thead>
</table>

**Probability that threat can produce consequence**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0.3</td>
</tr>
</tbody>
</table>

## Segmentated Architecture

<table>
<thead>
<tr>
<th>Segment</th>
<th>Physical Access Control</th>
<th>Logical Access Control</th>
<th>Anti Virus/Malware</th>
<th>Intermediate Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM #1 [PF]</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Authorized Worker (non-malicious) access via keyboard</td>
<td>0.1</td>
<td>0.3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Authorized Worker (non-malicious) connection of portable media</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0.001</td>
</tr>
<tr>
<td>Unauthorized Worker, (mischievous) access via keyboard</td>
<td>0.1</td>
<td>0.1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Unauthorized Worker, (mischievous) connection of portable media</td>
<td>0.1</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
</tr>
<tr>
<td>Outsider, (malicious)</td>
<td>0.3</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td>0.1</td>
<td>1</td>
<td>1</td>
<td>0.1</td>
</tr>
</tbody>
</table>

## IPL #5, (Personnel occupancy)

<table>
<thead>
<tr>
<th>IPL #5 (Personnel occupancy)</th>
<th>IPL #6 (Community occupancy)</th>
<th>IPL #6 Condition modifier</th>
<th>IPL #7 Condition modifier</th>
<th>Total Consequence Frequency/Years</th>
<th>Target SAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**PFD:** 1
## Example Tolerable Risk Definition

### Consequence

<table>
<thead>
<tr>
<th>Safety</th>
<th>Financial</th>
<th>Env.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;1 fatalities</td>
<td>&gt;R100M</td>
<td>Long term national</td>
</tr>
<tr>
<td>1 fatality</td>
<td>R10-100M</td>
<td>Long term regional</td>
</tr>
<tr>
<td>Severe injury</td>
<td>R1-10M</td>
<td>Short term regional</td>
</tr>
<tr>
<td>Minor injury</td>
<td>R.1-1M</td>
<td>Short term local</td>
</tr>
<tr>
<td>Insignificant</td>
<td>&lt;R0.1M</td>
<td>Minor to none</td>
</tr>
</tbody>
</table>

### Frequency of consequence occurrence

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=10,000 - 100,000</td>
<td>&lt;=1 - 10</td>
</tr>
<tr>
<td>&lt;=1,000 - 10,000</td>
<td>&lt;=10 - 100</td>
</tr>
<tr>
<td>&lt;=100 - 1,000</td>
<td>&lt;=10 - 100</td>
</tr>
<tr>
<td>&lt;=10 - 100</td>
<td>&lt;=1 - 10</td>
</tr>
<tr>
<td>&lt;=1 - 10</td>
<td>Less than 1 event in 1 year to 1 event in 10 years</td>
</tr>
<tr>
<td>Between 1 in 10 and 1 in 100 years</td>
<td></td>
</tr>
</tbody>
</table>
Challenges Going forward

• The usual:
  – Consistency of applying rules
  – Quality of output relies on quality of input

• How to project the future cyber security landscape
  – Periodic reassessment

• Further investigation and solutions to reliance on procedures & personnel
Conclusion

• Cyber security risks need to be managed
• This methodology provides a systematic approach:
  – Identification of the threat hazards
  – Risk evaluation of threat hazards
Risk Assessment Benefits

- Reveals threat hazards with unacceptably high risk profile
- Identifies where additional countermeasures need to be applied to address threat hazards effectively
- Provides a quantified risk profile that can be presented to business
- Systematic approach that is scalable, repeatable and technology independent
- Based on international best practices e.g. IEC 62443
Thank-you

Any questions?