Topic 5
Risk Management

Dr Diarmuid Ó Briain

13 Mar 2025

setu.ie
INSPIRING FUTURES

Version: 2.0

Licence

Learning objectives

By the end of this topic you will be able to:

- Understand the nature of Risk Management in OT environments.
- Identify the major potential risks to OT systems as cyber attacks, natural disasters, and human error.
- Assess the likelihood and impact of each risk using quantitative and qualitative methods.
- Define controls to reduce the likelihood or impact of risks.
- Implement controls to reduce the likelihood or impact of risks.
- Monitor the effectiveness of the controls to reduce the likelihood or impact of risks.

Risk Management in OT

- OT systems are increasingly connected to IT networks, which exposes them to cyber threats.
- Risk management in OT is the process of identifying, assessing, and mitigating risks to OT systems.
- The five steps of OT risk management are:
  - Risk Identification
  - Risk Assessment
  - Risk Mitigation
  - Control Implementation
  - Monitoring

Risk Management in OT

- Here are some specific risks that need to be considered in OT risk management:
  - Cyber attack
  - Natural disaster
  - Human error.

What is Risk

*Risk is a function of the likelihood of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organisation*

Risk Assessment Process

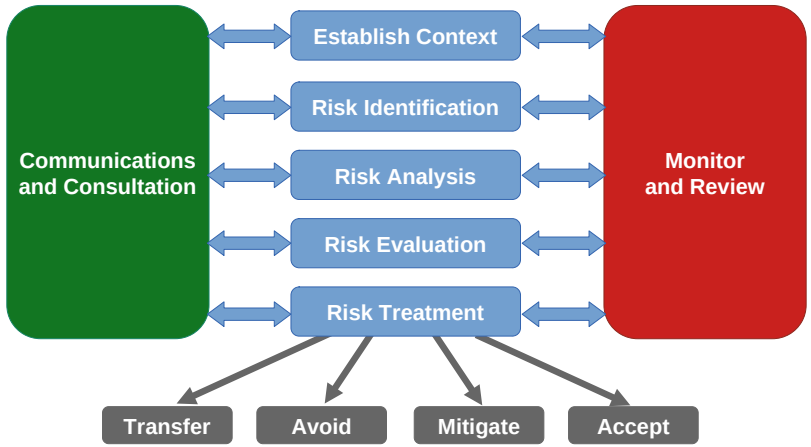
- Phase 1: Preliminary Risk Assessment
- Phase 2: Risk Analysis of Critical Areas and Processes
- Phase 3: Organisation-Wide Risk Assessment

Risk Assessment Process

Risk Assessment Process

- Asset
- Asset Valuation
- Threats
- Vulnerability
- Exposure
- Risk
- Safeguards
- Attack
- Breach

Risk Management Process



ISO 31000:2018 – Risk Management Guidelines

- Establishing the Context
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Continuous Monitoring & Review
- Communication & Consulting.

NIST SP 800-30 – Risk Management Guidelines

- System Characterisation
- Thread Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation.

Risk Log

- Identify Risks.
- Perform Qualitative/Quantitative Risk Analysis.
- Plan Risk Responses.

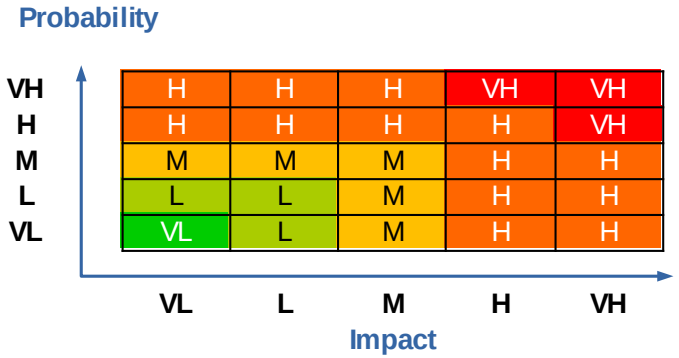
Project: <Project Title>

Summary				Description				Preventative Actions			Contingency Actions		
ID	Date Raised	Raised By	Description of Risk	Description of Impact	Probability Rating	Impact Rating	Priority Rating	Action	Resource	Date	Actions	Resource	Date

VL = Very Low | L = Low | M = Medium | H = High | VH = Very High

Risk Log

- Probability and Impact Matrix Tool



Quantitative Risk Analysis

- Quantitative risk analysis attempts to **assign monetary values** to the components of the risk assessment and to the assessment of the potential loss.
- Asset valuation
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Asset valuation

- An organisation must be able to place a dollar value on each information asset it owns, based on:
  - How much did it cost to create or acquire?
  - How much would it cost to recreate or recover?
  - How much does it cost to maintain?
  - How much is it worth to the organisation?
  - How much is it worth to the competition?

Exposure factor (EF)

- **Loss Potential** or the percentage of loss an organisation would realise if a risk was realised.
- **Single Loss Expectancy (SLE)**
  - The monetary value expected from the occurrence of a risk on an asset.
  - SLE = AV x EF
- **Annualised Rate of Occurrence (ARO)**
  - An estimate based on the data of how often a threat would be successful in exploiting a vulnerability.
- **Annualised Loss Expectancy (ALE)**
  - A calculation of the single loss expectancy multiplied the annual rate of occurrence, or how much an organisation could estimate to lose from an asset based on the risks, threats, and vulnerabilities. It is:
  - ALE = SLE x ARO
- **Annual Cost of Safeguard (ACS)**
  - This is the cost of the researched safeguard.
- **Cost Benefit Analysis (CBA)**
  - CBA determines whether or not a control alternative is worth its associated cost. CBAs may be calculated before a control or safeguard is implemented, to determine if the control is worth implementing, or calculated after controls have been implemented and have been functioning for a time:
  - CBA = (ALE(prior) – ALE(post)) – ACS

Performing a quantitative risk analysis

- Create an inventory of assets and assign a value [**Asset Value (AV)**].
- Conduct a risk assessment and vulnerability study to determine the risk factors for each asset. For each threat calculate the **Exposure Factor (EF)** and **Single Loss Expectancy (SLE)**.
- Perform threat analysis to determine the likelihood of the threat occurring in a single year – **Annualised Rate of Occurrence (ARO)**.
- Determine the **Annualised Loss Expectancy (ALE)** for each risk factor.
- Research **countermeasures** for each threat and calculate the change to the ARO and ALE if they were deployed.
- Perform a **Cost/Benefit Analysis (CBA)** of the countermeasures and choose the most appropriate response to each threat.

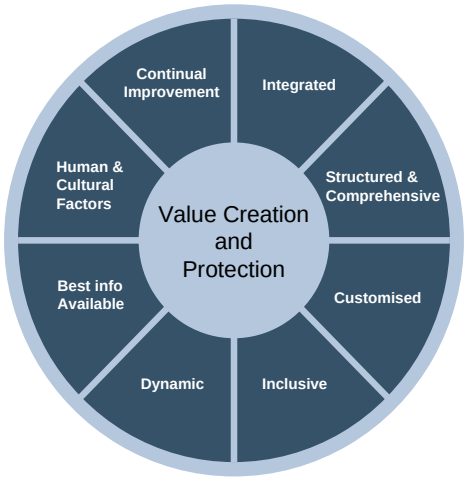
Qualitative Risk Analysis

- Relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10.
- Techniques used to assess the risk and produce a Risk Registrar.
  - Brainstorming
  - Delphi Technique
  - Storyboarding
  - Focus Groups
  - Surveys
  - Questionnaires
  - Check Lists
  - Interviews.

Delphi Technique

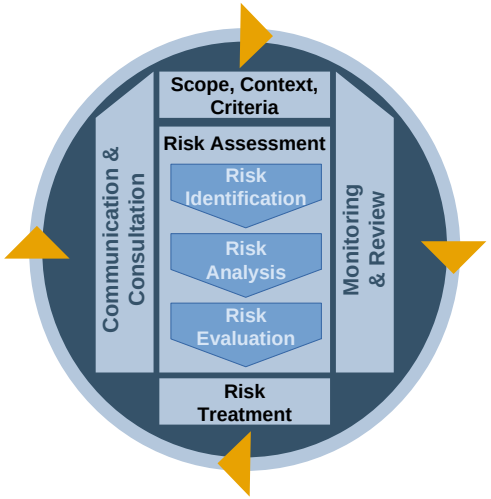
- Systematic, interactive forecasting method which relies on a **panel of experts**.
  - The experts answer questionnaires in two or more rounds.
  - After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgements
  - Experts are encouraged to revise their earlier answers in light of the replies of other members of their panel.
  - During this process the range of the answers will decrease and the group will converge towards the "correct" answer.
  - Process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results.

ISO 31000 - Risk Management Principles



ISO 31000 - Risk Management Framework

ISO 31000 - Risk Management Process



Risk Management Plan (RMP)

- Document that describes the risks associated with a product, service, or project, and the actions that will be taken to mitigate those risks
- Commonly used in a variety of industries, including healthcare, OT industries and organisations as well as IT
- An RMP typically includes sections such as:
  - Risk Identification
  - Risk Assessment/Analysis
  - Risk Mitigation/Treatment
  - Risk monitoring
  - Risk review.
- RMPs are living documents that should be updated regularly as new information becomes available and as the product, service, or project changes.

Simplified RMP – Risk Identification

- **Safety hazards**
  - Machinery accidents
  - Ergonomic injuries
  - Exposure to hazardous materials
- **Quality hazards**
  - Defects in products
  - Product recalls
- **Production hazards**
  - Equipment failures
  - Material shortages
  - Supply chain disruptions

Simplified RMP – Risk Identification

- In addition to the general risks, consider specific risks that are associated with assembly lines. These risks include
  - **Repetitive motion injuries**: Assembly line workers often perform the same repetitive tasks over and over again, which can lead to repetitive motion injuries.
  - **Ergonomic hazards**: Assembly line workers may have to work in awkward or uncomfortable positions, which can lead to ergonomic hazards.
  - **Exposure to hazardous materials**: Assembly line workers may be exposed to hazardous materials, such as chemicals, fumes, and dust.

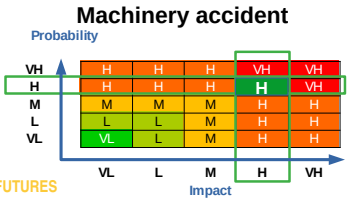
Risk Identification

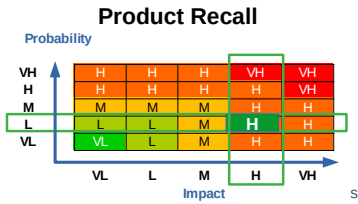
- Group exercise
  - Discuss specific risks associated with a Hydro-electrical Power Station

10

Simplified RMP – Risk Assessment

- The likelihood and impact of each risk should be assessed
- For example
  - the risk of a machinery accident may be considered to be high probability and high impact
  - the risk of a product recall may be considered to be low probability and high impact.





Risk Assessment

- Individually
  - Assess the risk of a worker in the power station falling into the tailrace of the power station.

2

- Group
  - Discuss the individual findings and come to an agreed assessment.

3

Simplified RMP – Risk Mitigation

- For each risk, a risk mitigation strategy should be developed
- Risk mitigation strategies can include:
  - Avoiding the risk
  - Reducing the probability of the risk
  - Reducing the impact of the risk
  - Transferring the risk to a third party.

Risk Mitigation

- Individually
  - Consider mitigation strategies to the risk.
- Group
  - Discuss the individual strategies and come to an agreed strategy.

Simplified RMP – Risk Monitoring

- The risks should be monitored regularly to ensure that the risk response strategies are effective
- This is important because risks can change over time, and new risks may emerge.

Simplified RMP – Risk Review

- The RMP needs to move with changes in the operation of the organisation
- To ensure this happens it is essential that the RMP is evaluated for its effectiveness of risk management controls and identifying areas for continual improvement.

OT RMP

- **Step 1: Asset Identification**
  - What is at risk?
- **Step 2: Risk Identification**
  - What are the threats?
- **Step 3: Risk Assessment**
  - How do the risks expose the OT?
- **Step 4: Risk Mitigation**
  - Access controls, Segmentation, Data Encryption, IDS, IPS, SIEM
- **Step 5: Monitor and Review the RMP**
  - Is the RMP still effective?

Learning objectives

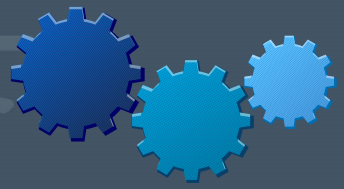
You should now be able to:

- Understand the nature of Risk Management in OT environments ✓
- Identify the major potential risks to OT systems as cyber attacks, natural disasters, and human error ✓
- Assess the likelihood and impact of each risk using quantitative and qualitative methods ✓
- Define controls to reduce the likelihood or impact of risks ✓
- Implement controls to reduce the likelihood or impact of risks ✓
- Monitor the effectiveness of the controls to reduce the likelihood or impact of risks ✓

Exercise #5

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Scenario



Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

engcore
advancing technology