Industrial Control System - Cybersecurity

NWWC 2022: Nov 6, 2022

HATCH

Manifesto Share

Our Client's Mandate:

To provide for the responsible delivery of **high quality, efficient** and **safe** public infrastructure and customer focused services that support community, environmental and economical **sustainability.**

We build practical **SOLUTIONS** that are **SAFE, INNOVATIVE, & sustainable.**

Hatch – Controls & Automation

78+
offices, including Hatch LTK

9,000+
employees

$50B+
in projects

Over 65
years of experience

Experience in
150+
countries

Mining, energy, and infrastructure know-how

100%
employee-owned

Focused on value-driven solutions

40+ Years Delivering Control, Automation & Electrical Solutions	500+ Staff Dedicated to Controls & Automation	An Agnostic & Independent Technology Integrator
20+ Years Delivering System Integration	300+ Controls & Automation Staff in NA	
65+ Years of Technologies & Innovation		

HATCH

Significant Cybersecurity Incidents

2014 German Steel Mill

Control system compromised after corporate network compromised. Caused multiple components in system to fail.
Massive physical damage.

2015 Ukrainian Power Grid

SCADA system compromised. 225,000 customers lost power for several hours.
Operationally constrained for larger period. Manual operation

2018 Saudi Aramco Facility

First time a safety system was attacked
Intended to manipulate safety signal and cause explosion.

2020 a US natural compressor facility

Email with a malicious link gain control of plant
2-days Loss of production

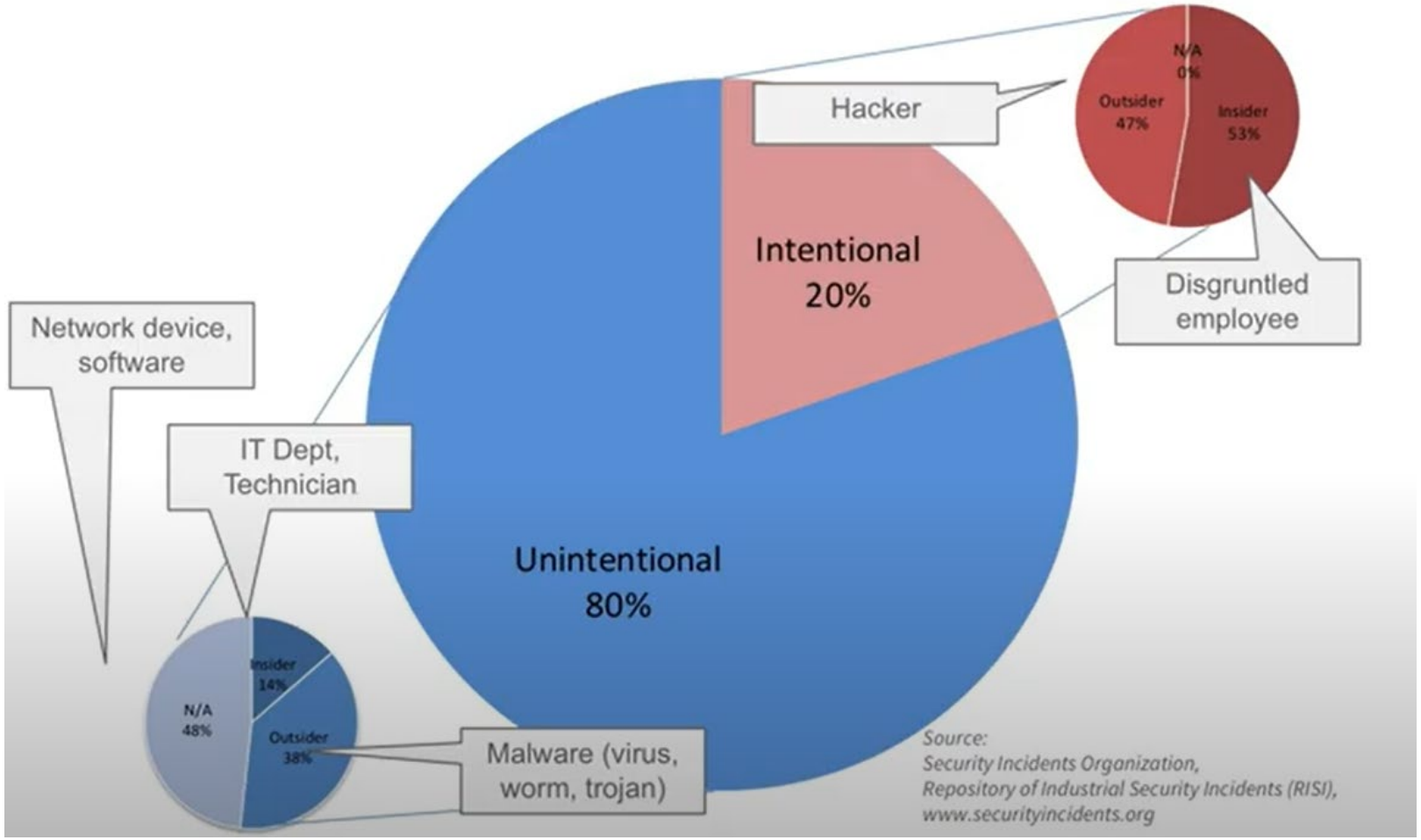
2021 Oldsmar water supply in Florida

Access to an outdated SCADA system through TeamViewer.
Elevate the chemical level to a dangerous level.

Source: Significant Cyber Incidents | Center for Strategic and International Studies (csis.org)

What is ICS Cybersecurity?

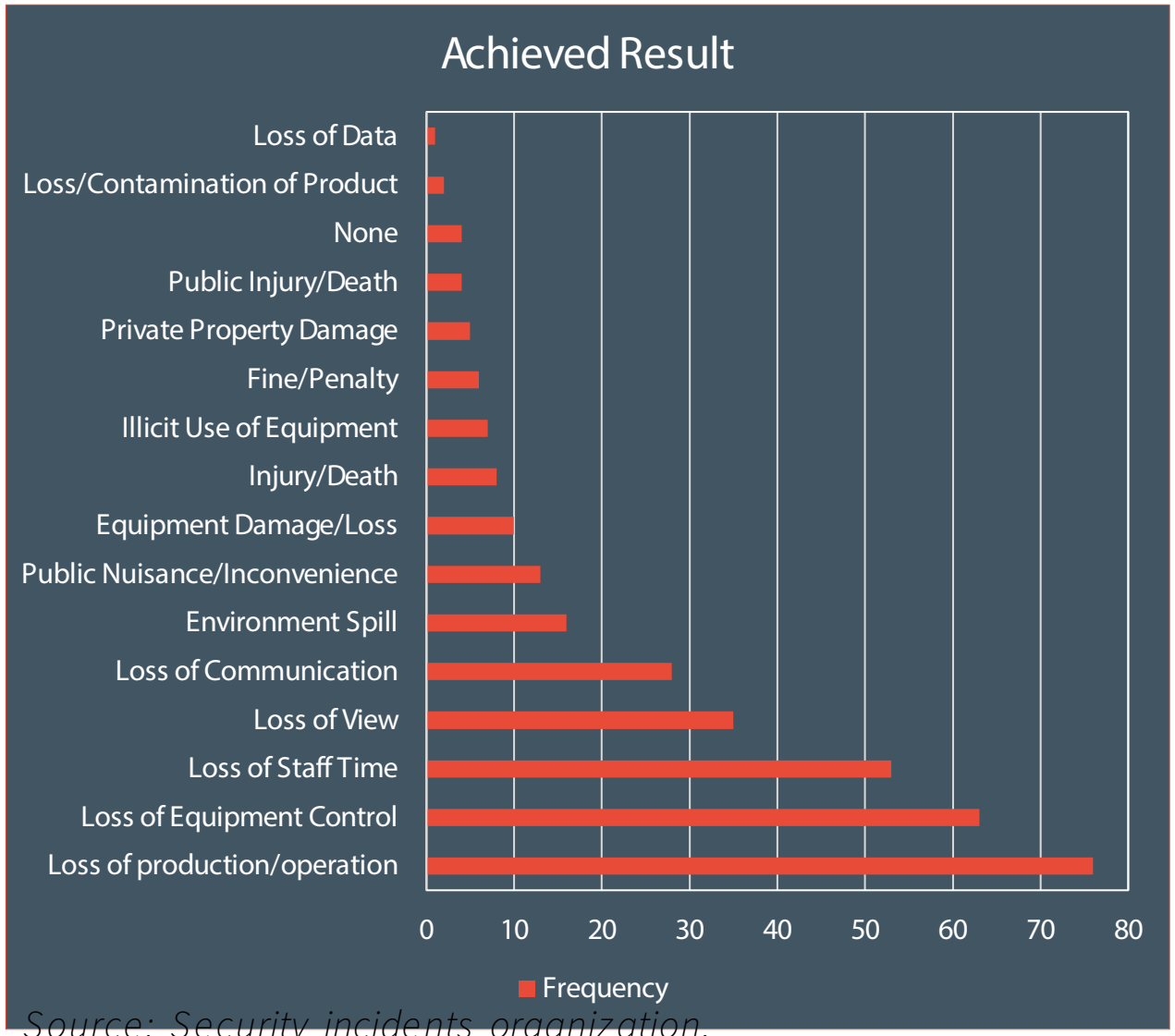
- Prevention of intentional or unintentional interference with the proper operation of industrial automation and control system



HATCH

Difference between IT Security and ICS Security

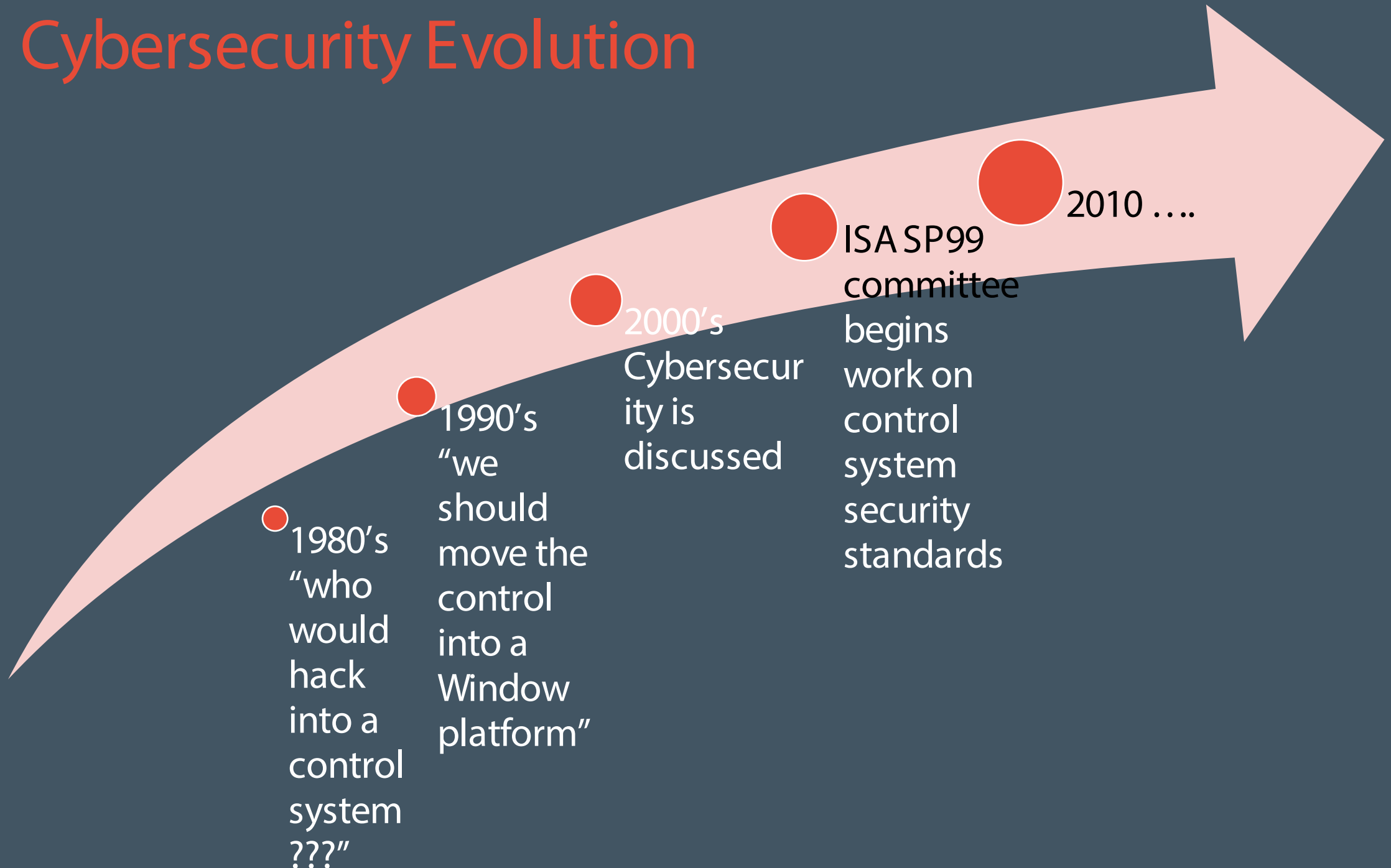
- Although the same technologies may be used in ICS and IT, the purpose and use is significantly different.
- ICS cyber security must address additional consideration of health, safety, environmental protection and product integrity.
- Other differences include higher expectation of availability, integrity, performance, change management and equipment life cycle.



Source: Security incidents organization, www.securityincidents.org

HATCH

Cybersecurity Evolution



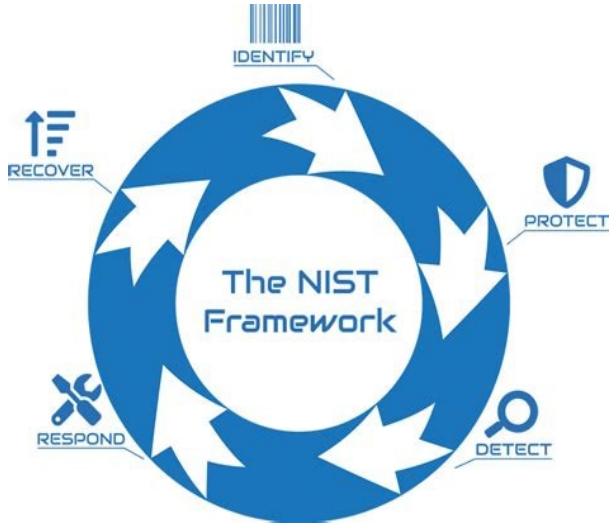
Due Diligence

American Water Works Association

Dedicated to the World's Most Important Resource®

Cybersecurity & Guidance

ISO 27001



ISA/IEC 62443

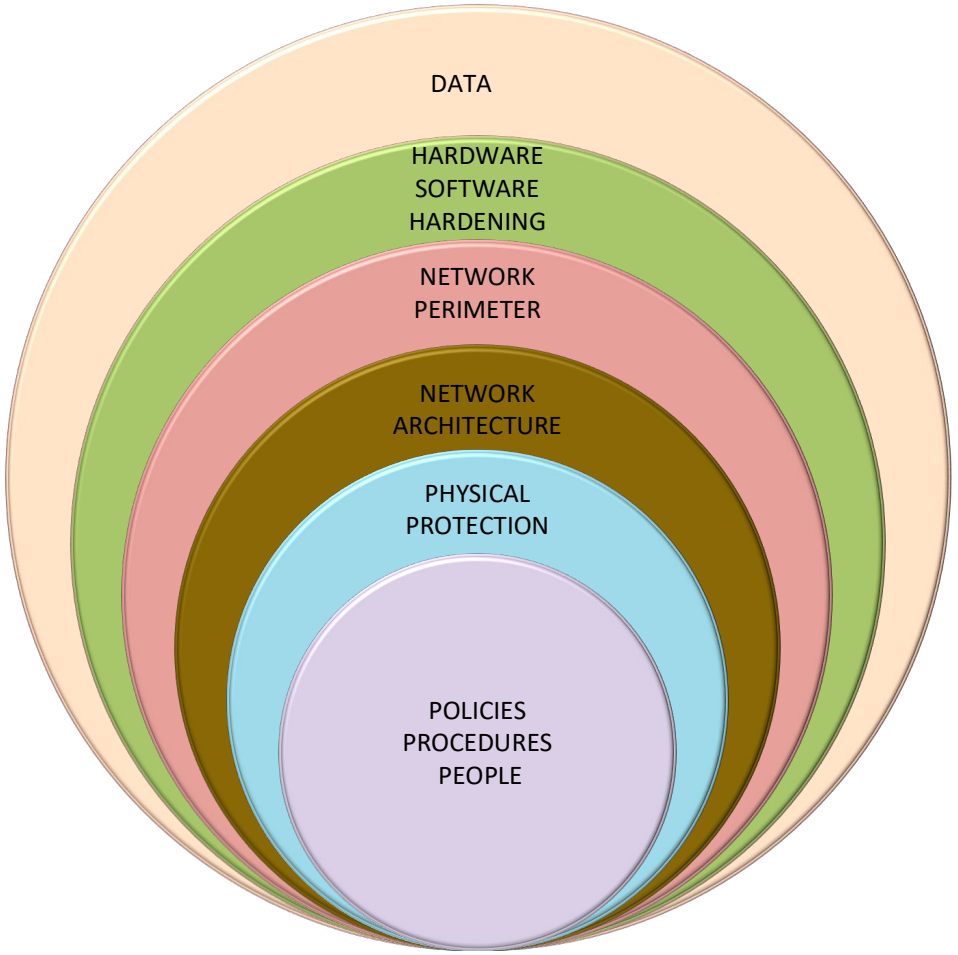
NIST SP 800-82,

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

HATCH

Defense-in-Depth

- Cybersecurity isn't easy. There is no magic solution or product or service to magically solve all the cybersecurity problems
- Increases security by increasing the adversary's effort needed in an attack
- Concerted effort to build out resilient infrastructure
- Deploy integrated strategies that drive resiliency and bolster defenses
- Multiple levels of protection must be deployed within each layer
- Any layer of protection might fail



HATCH

Cyber Security in Action

The Cyber Security Lifecycle from design to implementation and operation

Design

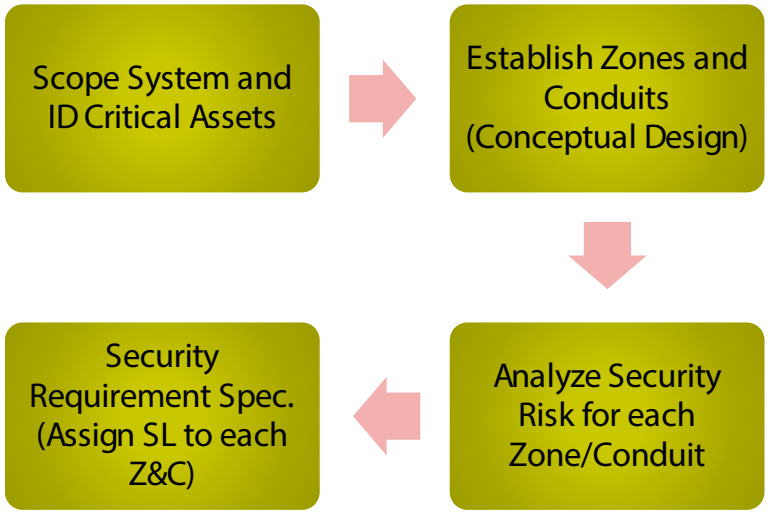
Implementation

Operation & Maintenance

Design Phase

Input

- Standard, policies, procedure
- Asset inventory
- Risk criteria/matrix
- Process grouping of asset
- System architecture
- WAN/LAN logical physical topology
- Data flow
- Remote access requirements



Outcome

- Cybersecurity and nontechnical control requirements
- System architecture with zones and conduit, target security level and data flow
- Risk assessment report

Security Risk Assessments

- High-Level Risk Assessment
  - Grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access, or responsible organization.
  - Multi-disciplinary risk assessment
  - Identify highest areas of risk
- Detailed Cyber Risk assessment
  - Quantify cybersecurity risk for critical zones
  - Consider System Vulnerabilities
  - Model the threat vectors looking at likelihood and consequence
  - Account for existing or planned countermeasures

HATCH

Why risk cybersecurity assessments are critical?

- Difficulty in deciding on level of investment and how to prioritize response
- Identification of threats, vulnerabilities and consequence
- Understanding the SCADA system
- Assessing the Impact of Controls and the Residual Risk

HATCH

Network Architecture

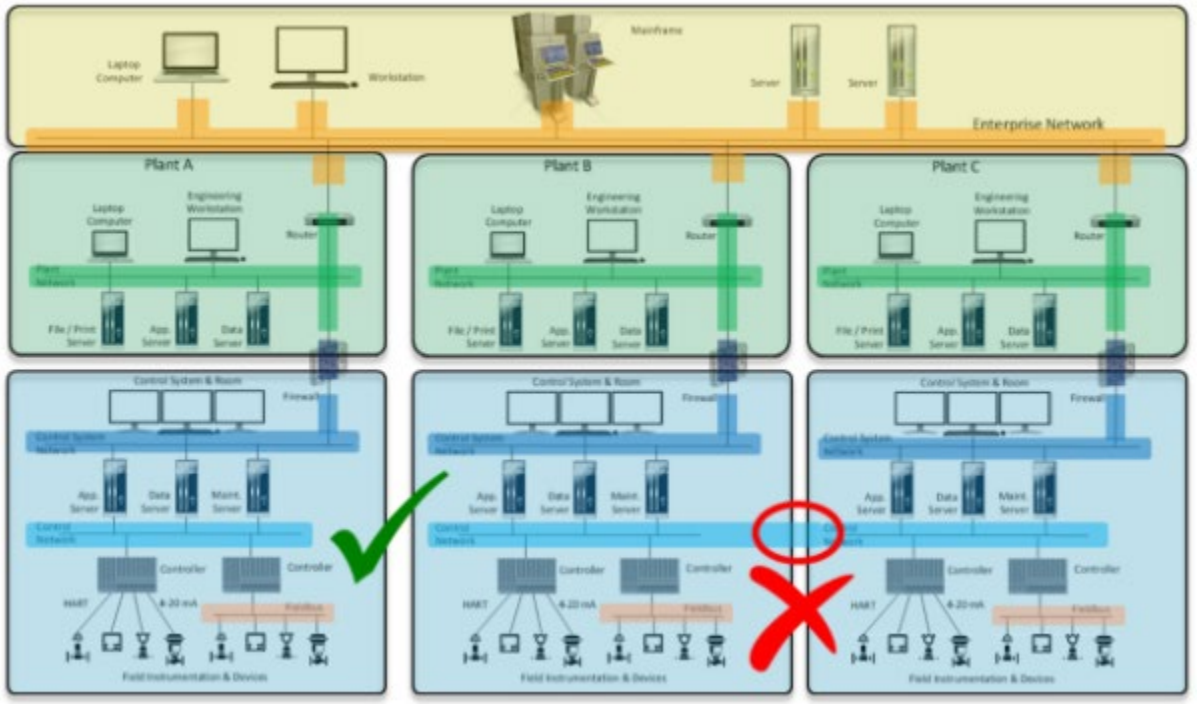
A zone can have sub-zones.

A conduit cannot have sub-conduits.

A zone can have more than one conduit. Cyber assets (HOSTs) within a zone use one or more conduits to communicate.

A conduit cannot traverse more than one zone.

A conduit can be used for two or more zones to communicate with each other

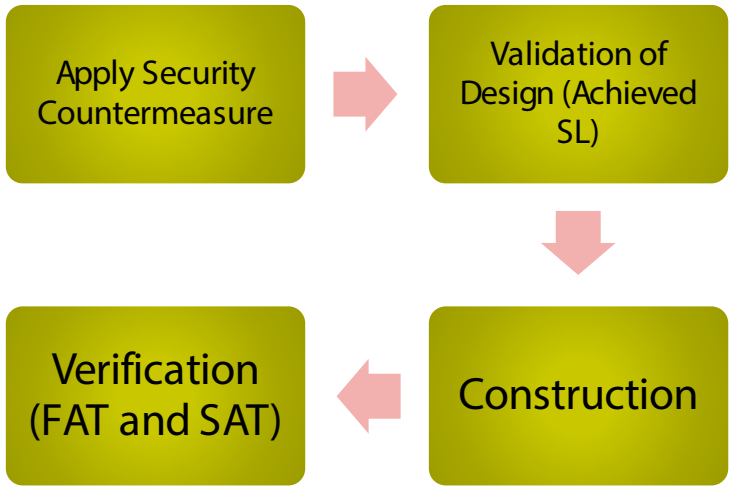


HATCH

Implementation Phase

Input

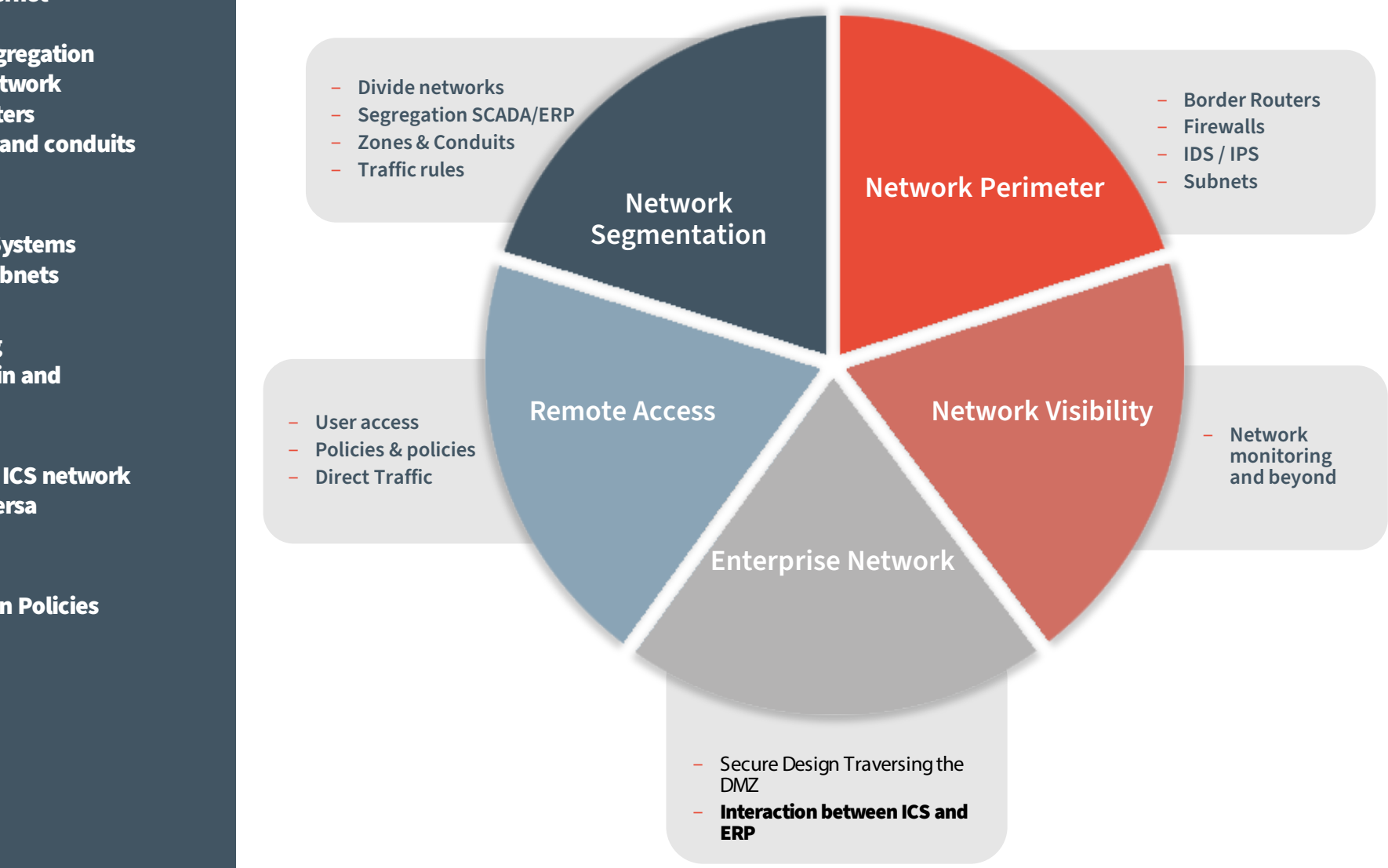
- Cybersecurity and nontechnical control requirements
- System architecture with zones and conduit, target security level and data flow
- Risk assessment report



Outcome

- Design specification
- System network architecture
- Data flow
- Design specification and procedures
- Training material
- PenTest report
- Backups
- Asset inventory

- **Network Segmentation / Segregation**
  - Divide networks into separate ethernet segments
  - Implement physical and logical segregation between SCADA and Enterprise Network
  - Define zones and conduits perimeters
  - Define traffic rules between zones and conduits
- **Network Perimeter**
  - Border Routers and Firewalls
  - Intrusion Detection & Prevention Systems
  - De-Militarized Zones/ Screened Subnets
- **Network Visibility**
  - A step beyond network monitoring
  - Deep insights into everything within and moving through the network.
- **Enterprise Network**
  - Identify ERP network interact with ICS network
  - ERP users' tasks on ICS and vice versa
  - Duration of required access
- **Remote Access**
  - Use User Access and Authentication Policies and Procedure
  - Control the Application
  - No Direct Traffic
  - Only One Path In or Out

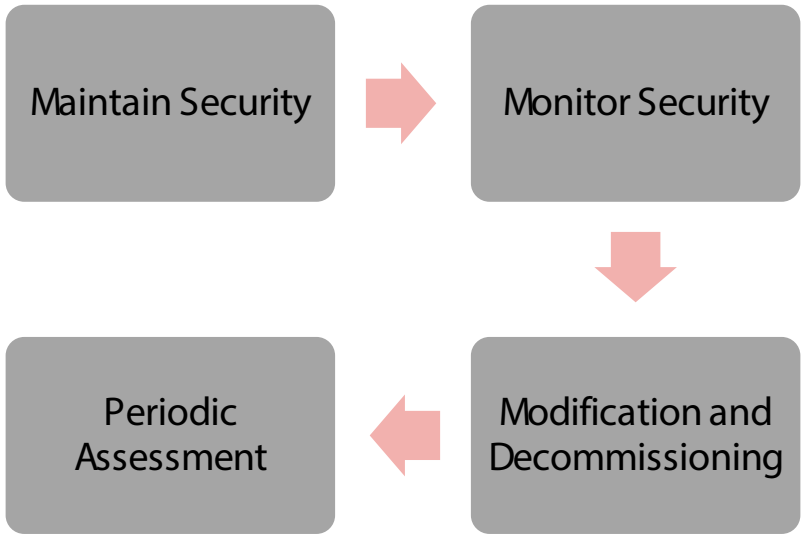


HATCH

Operation & Maintenance Phase

Input

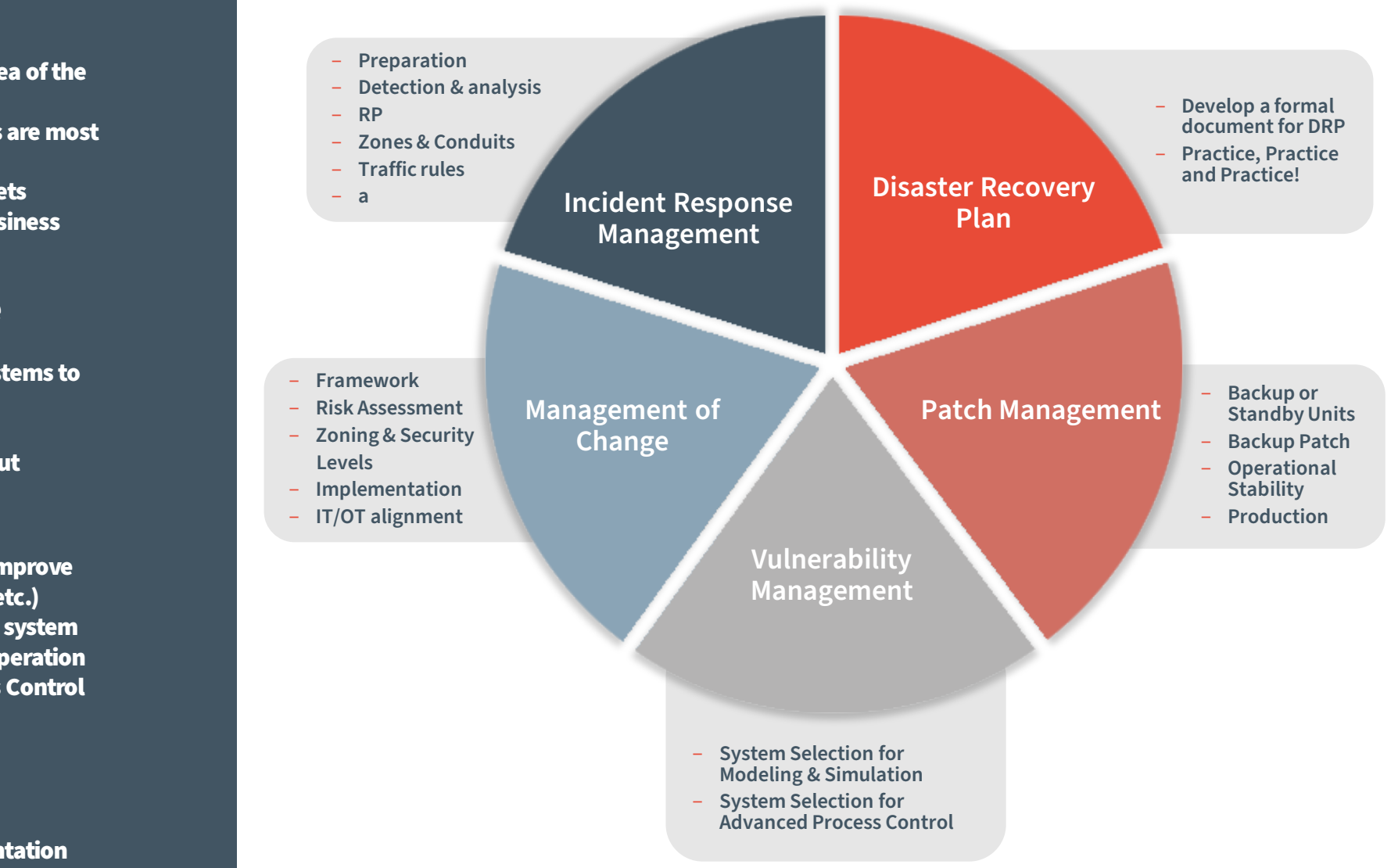
- Assignment of new office and/or reginal managers.
- Improving regional bench capacity for emergency situations.
- Identify and address technical difficulties and challenges in early stages.
- Support from BUs for maintaining specific niche skill sets



Output

- Policies
- Procedures
- Guidelines

- **Incident Response Management**
  - Preparation
  - Detection and analysis
  - Containment eradication and recovery
  - Post incident activity
- **Disaster Recovery Plan**
  - Establish an owner
  - Identify representatives from each area of the business
  - Specify which process, data and tools are most critical
  - Maintain an inventory of physical assets
  - Determine where and how critical business information will be backed up
  - Create a communication plan
- **Patch Management Decision Tree**
  - Define KPIs for OMS
  - Determining required operational systems to achieve defined KPIs
  - Find Critical Assets
  - Inform main technology vendors about operational KPIs
- **Vulnerability Management**
  - Identify major process systems that improve plant KPIs (e.g., throughput, quality, etc.)
  - Business benefit analysis for selected system for process modeling (digital twin), Operation Training Station or Advanced Process Control
- **Management of Change**
  - Evaluate risks which may arise
  - Impact analysis
  - Approval for the changes
  - Test case for the successful implementation
  - Configuration management



HATCH

Oxford County Project

Hatch is providing SCADA Standardization and Project Management: 2021-2026

Client Profile:

- Oxford County is a regional municipality in the Canadian province of Ontario. Highway 401 runs east–west through the centre of the county, creating an urban industrial corridor. The local economy is otherwise dominated by agriculture, especially the dairy industry.

Project Objective:

- Enhancing cybersecurity and network performance
- Improvement in SCADA asset management
- Enablement of efficient control system migration by developing SCADA standard and preliminary design
- Project management of first five years of the future state projects

Total Project Budget & Schedule:

- CADxxM over 12 months

Hatch Scope:

Activities

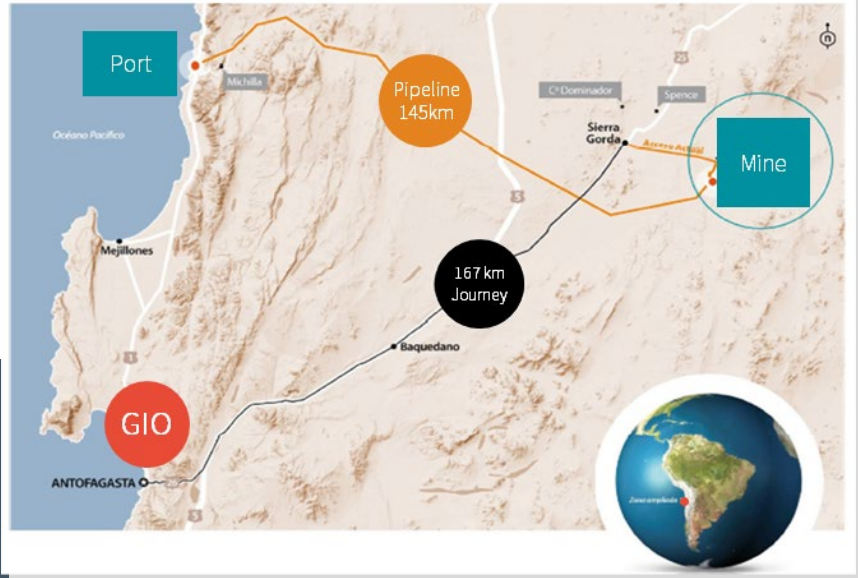
- Create a Cybersecurity Framework
- Create an Asset Registry Plan
- Develop PCN, HMI and PLC standards
- Support the Cybersecurity Implementation
- Control Panel Preliminary
- Project management of the first five years of future state projects

Technology

- Field instrumentation and cabling
- IT & Telecommunications:
- CCTV, fire detection & radio trunking
- Tele-remote control: e.g., rock-breaker
- Historian, LIMS, Process Control, APC & OTS
- Condition monitoring & asset management
- Dashboards & automated reporting.
- Abstraction layer and data integration.

AMSA Centinela IROC Project

Hatch is the EPCM & Systems Integrator for one of the largest IROC projects globally



Client Profile:

- Open-pit mining of sulfide & oxide deposits.
- Antofagasta Region of northern Chile.
- Copper and molybdenum concentrate (milling and flotation).
- Copper cathodes (SX-EW).
- 11th largest copper producer globally

Project Objective:

Drive value-chain optimization by:

- Remotely co-locating 100 people (operators, planners, engineers & management).
- Increasing volume & quality of data.
- Implementing & upgrading technology.

Total Project Budget & Schedule:

- US$63M over 21 months

Hatch Scope:

Activities

- Current state surveys
- HMI and visualization redesign
- Business cases
- Detailed engineering design
- Integrated architecture
- Definition of procurement packages
- Solution identification and evaluation
- Implementation management
- Training and commissioning plans

Technology

- Field instrumentation and cabling
- IT & Telecommunications:
- CCTV, fire detection & radio trunking
- Tele-remote control: e.g., rock-breaker
- Historian, LIMS, Process Control, APC & OTS
- Condition monitoring & asset management
- Dashboards & automated reporting.
- Abstraction layer and data integration.

Who needs Cybersecurity protection

WE ARE ALL TARGETED

LARGER FACITIES : The largest industrial sites tend to know they are targets of sophisticated / nation-state attacks.

SMALL & MEDIUM FACITIES: Smaller sites tend to believe they are not important enough to be targets of such attacks.

THE OPPOSITE IS TRUE: Because the largest sites tend to be the best defended, smaller sites are more attractive targets.

This is especially true in water and natural gas utilities, where the consequences of compromise include serious threats to public safety

Thank you

For more information,
please visit www.hatch.com

HATCH