ERNCIP-IMPROVER Joint Operators Workshop

Industrial Control Systems Resilience on the IT Front

Georgios Koutepas
IT Security Consultant
Unisystems S.A.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen
Security Technology Assessment Unit
ISPRA, Italy

Serving society
Stimulating innovation
Supporting legislation

www.jrc.ec.europa.eu

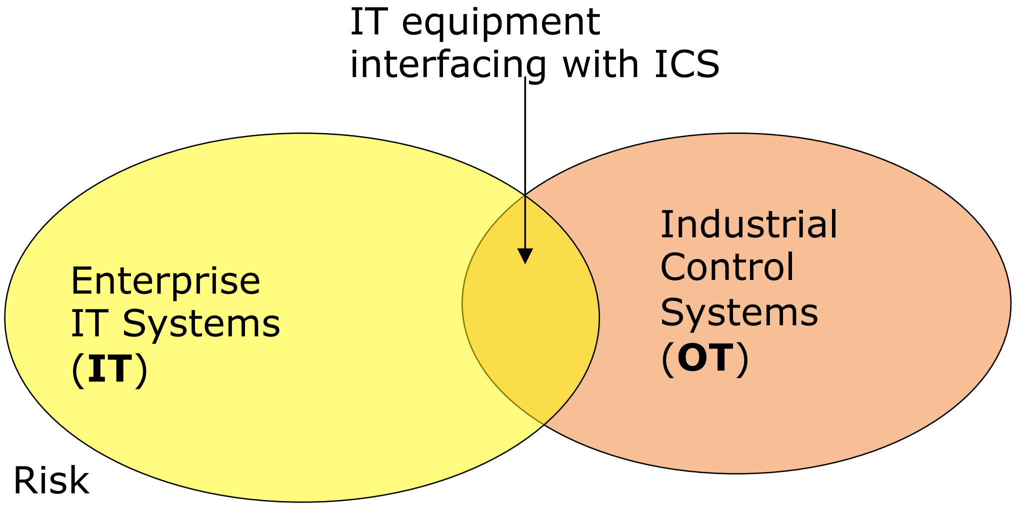
Viewing Critical Infrastructure resilience from the side of IT

Overview

- The IT and OT
- How the IT world integrates with ICS
  - Challenges and horror stories
- How the IT world affects ICS: Lessons and new opportunities
- How IT approaches resilience and business continuity
- IT solutions to ICS resilience challenges, action plans

The distinction between IT and OT

- **OT**, Operation Technology, in contrast to Information Technology (or **IT**) refers to the collection of all the (automated or non-automated) technical equipment that via the coordination of hardware and software accomplices the production goals of the organization at a technical level. In contrast, IT refers to the computing and communication equipment that supports the business side of the organization (which however may include aspects of the OT)



IT equipment
interfacing with ICS

Enterprise
IT Systems
(**IT**)

Industrial
Control
Systems
(**OT**)

Covered by
Enterprise IT Risk
Methodologies

How ICS have become more IT dependent

Technical Side and Threats (1)

- In the past: Custom-made solutions for individual industrial processes and protected by an “air-gap”
  - Considered secure by default.
- Now: Part IT systems, part proprietary specialized equipment
- IT developments and cost-cutting approaches have directed the ICS sector towards the developing and adopting systems:
  - Implemented as applications on commercially available computing platforms and methods (hardware, operating systems, application servers , client-side processing, etc.)
  - Interconnected with widely-used (instead of proprietary) protocols and in many cases sharing the same networking infrastructure as the rest of the Enterprise

How ICS have become more IT dependent

Technical Side and Threats (2)

- IT related ICS vulnerabilities
  - Many have appeared in the last 2 years
  - Expected to be the trend from now on (“Low hanging fruit”?)
- Problems that have been solved (or are seriously considered) in general computing platforms
  - They still appear in ICS systems
  - Networking of ICS plays a key role
- This is a new problem for ICS manufacturers

How ICS have become more IT dependent

Technical Side and Threats (3)

- Indirect threats to infrastructure
  - Reliance on third party networks
    - VPNs not a completely secure solution
    - Continuous threats against TLS and other encryption solutions
    - The threat of eavesdropping
    - The threat of "repetition" attacks
  - The continuous threat via the enterprise IT part of the organization
    - Phishing Emails
    - Web based threats - Malware
    - Mobile device threats (communication devices, data storage devices)
    - Advanced Persistent Threats
    - Unavailability of vital IT equipment

How ICS have become more IT dependent

Organizational Side and Threats

- Lack of readiness (even willingness) from the industry (both manufacturers and end users) to consider protection needs in the new ICS status
- Difficulty to understand ICS as computing systems and integrate them in a systematic and rigorous protection process (an Information Security Management System)
- Long turnaround times to improve security in equipment and processes due to:
  - failure to understand problems
  - the unavailability of quick solutions
  - lack of IT expertise
  - the need for undisrupted operations
  - the need to certify correct operation in new configurations

ICS and the IT threats: Horror story 1

The Ukrainian Incident

- End of 2015, beginning of 2016: Attacks on the electricity grid in Ukraine
  - BlackEnergy malware was used – Active since 2011, v.3 is the latest – Sandworm group
- IT issues spilling into production
  - Started with malicious email messages
  - Infection of workstations, stayed hidden, moved towards the production network. Also gathered information.
  - Remote control of systems (workstations) that controlled electrical relays
  - Attack was followed by destruction of files (KillDisk) and the systems themselves
  - Blackouts lasted for 3 hours, relays had to be restored manually, on-site
  - Accompanied by Denial of Service attack against the customer calling center
- The aftermath, worldwide concern:
  - March 23, 2016, full report by the Electricity Sector Information Sharing and Analysis Center (ISAC) of the North American Reliability Corporation (NERC)
  - April 12, 2016: FBI Warning Power Companies of Cyber Threats to the US Grid

ICS and the IT threats: Horror story 2

Some recent IT based threats against ICS

- Feb. 15, 2016: Cisco Industrial Switch **DoS**
- Jan. 15, 2016: EKI-132x platform devices (gateways between Ethernet and serial connections to ICS), **SSH default password**. Still:
  - September 2015 - a number of "**Zero-Day**" (previously unknown) vulnerabilities
  - November 2015 - **pre-configured SSH and HTTP servers with hard-coded passwords**
  - December 2015 - new Zero-Day Vulnerabilities: **Buffer Overflows**, **Shellshock and Heartbleed** in code issued to solve previous issues
- Dec. 17, 2015: Juniper VPN Firewalls had serious **backdoor**
- Dec. 2015: Honeywell Gas detectors could be **remotely controlled** (via web interface flaws)
- Dec. 15, 2015: Schneider PLCs found to contain serious buffer overflow problem resulting in **device crash** or **remote code execution**.

How IT systems affect ICS operations
The positive

- We can build resilience for IT systems (an important part of the infrastructure) and the IT portion of ICS
- Use IT resilience methods to approach the problem of protecting Industrial components
- Build upon IT industry best practices

The IT approach to resilience
Main terminology - Explanations

NIST 800-34 – Contingency Planning Guide

- Business Continuity Plan
- Critical Infrastructure Protection Plan
- Disaster Recovery Plan

CERT® Resilience Management Model (CERT®-RMM)

- The concept of Resilience is part of Operational Risk Management
  - “To more effectively manage and mitigate operational risk requires that an organization focus its attention on operational resilience”
- Resilience Requirements must be defined for each asset
- “Capability” levels to indicate how well a process is performed during stress

The IT approach to resilience
Opportunity 1: Organizational level

- Resilience is one of the goals of organizational Security Governance
  - One of the aims of the Information Security Risk Management Process
  - Interconnected with the process of assessing Risk in the IT systems of the organization
    - Definition of Asset – based on specific system, group of systems, or enterprise processes
    - Identification of the connection of Threats with Vulnerabilities and Controls (protection measures)
  - By knowing where we stand in a Risk Management setting we understand the Resilience maturity of the organization
    - Controls introduced to counter Risk and increase resilience

The IT approach to resilience
Opportunity 2: Technical level

- Expertise in ways to secure systems and infrastructure
  - Including from insider threats and internal problems (e.g. programming errors)
- Make use of IT systems past challenges to help identify problem areas in ICS
  - Manufacturers should seriously consider component security
  - Users should (learn to) demand levels of security that are acceptable in the IT industry
- Perform IT asset management (even for ICS components)
  - Including software, network connectivity (protocols, server types etc.)
  - Quickly identify systems affected by new threats and vulnerabilities
- Build compensatory Enterprise IT security measures when the ICS components themselves cannot be protected
  - Network Filtering, network segregation, Remote device protection
  - “Virtual patching”
  - Security Awareness Training

The IT approach
Building for Resilience

- Have a good understanding of IT infrastructure, critical assets, their nature (systems, software, components, interdependencies), and their value for the business processes.
- Have a good indication of threats that can be relevant to the infrastructure and thanks to the Risk Management process how they relate to existing vulnerabilities.
- Establish reaction plans
- Calculate acceptable downtime, time to resume operations, time to recovery
- Introduce Security Controls to help achieve
  - An Acceptable level of Risk
  - Acceptable Downtime goals
- Introduce redundancy where required (network, systems, locations, people, operations)

Challenges beyond IT
The ICS distinct characteristics

- There is always a distinct OT component
- IT not the "Silver bullet"
- We still need specialized resilience plans for the core industrial processes
  - These should not only address the issue of attacks (or IT mishaps) but also problems directly affecting Industrial processes (e.g. physical disasters, terrorism, etc.)

Summary

- IT is an integral part of the Industrial Control infrastructure
  - IT and OT keep getting integrated
- This introduces new threats
  - In the IT part of ICS
  - In the enterprise support infrastructure
- The IT approach to the problem of Resilience is to work using Risk Management
  - This can help to:
    1. Identify critical assets, part of the business processes and a various levels of abstraction
    2. Know the threats
    3. Relate them to vulnerabilities, thus making them relevant
    4. Calculate the Risk they represent to the organization
    5. Introduce controls that help manage the level of risk
  - All these are introduced via established methodologies and standards

THANK YOU

ANY QUESTIONS?