ICS and Critical Infrastructure - Cybersecurity

Alvaro Soneiro - DM/OICT (Digital Blue Helmets)

Agenda

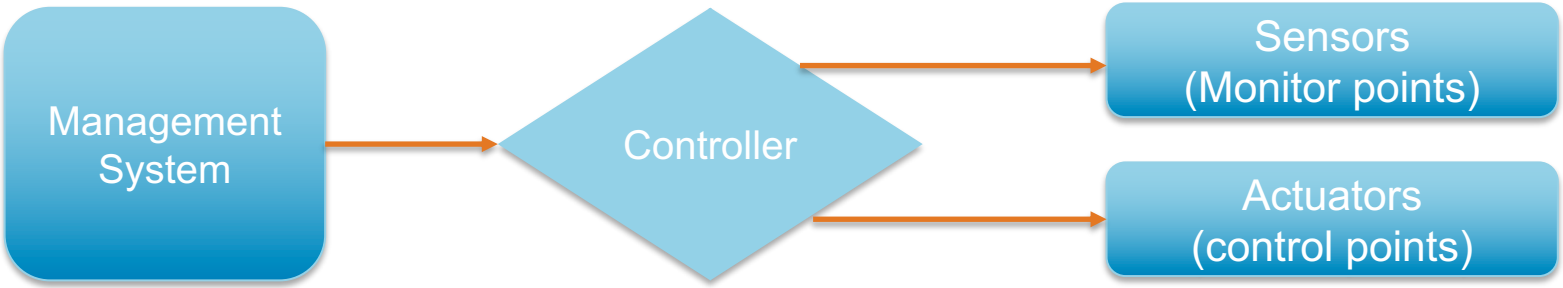
- Introduction to ICS
- Operational considerations
- Internet footprint
- Examples
- Security Council Resolution
- Q&A

INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems (ICS)

- Combination of process(es) that work together to achieve an industrial objective
  - Manufacturing, Chemical, etc
- General term describing control systems found in industrial sectors and critical infrastructure.
- Critical Infrastructure: term used to describe assets that are essential for the functioning of a society and economy
  - Electricity, water supply, public health, etc

Main components



ICS Operation

- Isolated systems
- Proprietary hardware and software
- Physically secured areas
- No connection to IT networks or systems

Evolution of ICS

- Critical infrastructure relies upon IT systems for their daily operations.
- Network interconnectivity
- Targeted attacks

Therefore, ICS cybersecurity is a risk that needs to be managed.

Operational differences

- Long life span
- Unsupported systems
- Control physical processes
- Availability requirements
- Response time requirements
- No test environments

ICS Internet Footprint

Shodan

- Google like search engine for devices in internet
- Includes classical IT infrastructure (servers, databases) as well as any internet capable device
  - IoT (webcams, baby monitors)
  - Remote sensors
  - HMI and maintenance portals


SHODAN ICS Radar
Protocols
About
REYKJAVIK
AMSTERDAM
SAN PHOENIX


SIEMENS
SIMATIC HMI Miniweb on HMI_Panel
Miniweb Start Page
Welcome on HMI_Panel
Device Status of HMI_Panel
The runtime is running
General Device Information
Device Type TP1500 Comfort
Image version V14.00.00.00_29.01
Bootloader version 1.20
Bootloader release date 6.12.2013
Device Name HMI_Panel
SSLEAY_VERSION OpenSSL 1.0.1p 9 Jul 2015

Attack Scenarios

HORUS

- Electrical grid
- European country
- Interdependencies - balance
- Solar inverters
- 2 sides of the story
  - Study from security company
  - Statement from manufacturer

Staged attack

- Under controlled conditions
- https://www.youtube.com/watch?v=fJyWngDco3g

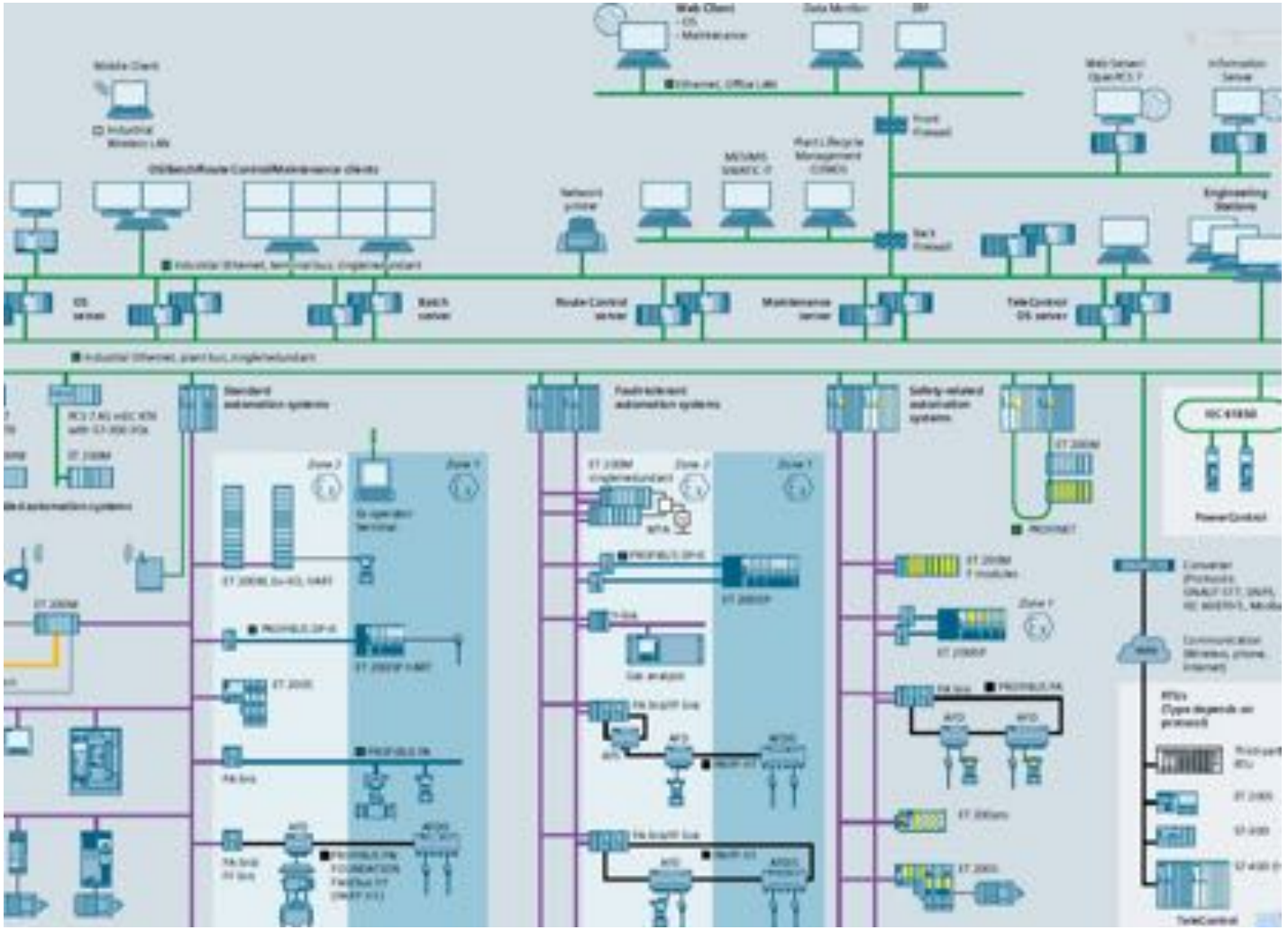
SECURITY COUNCIL RESOLUTION

Security council resolution (2341), Feb 2017

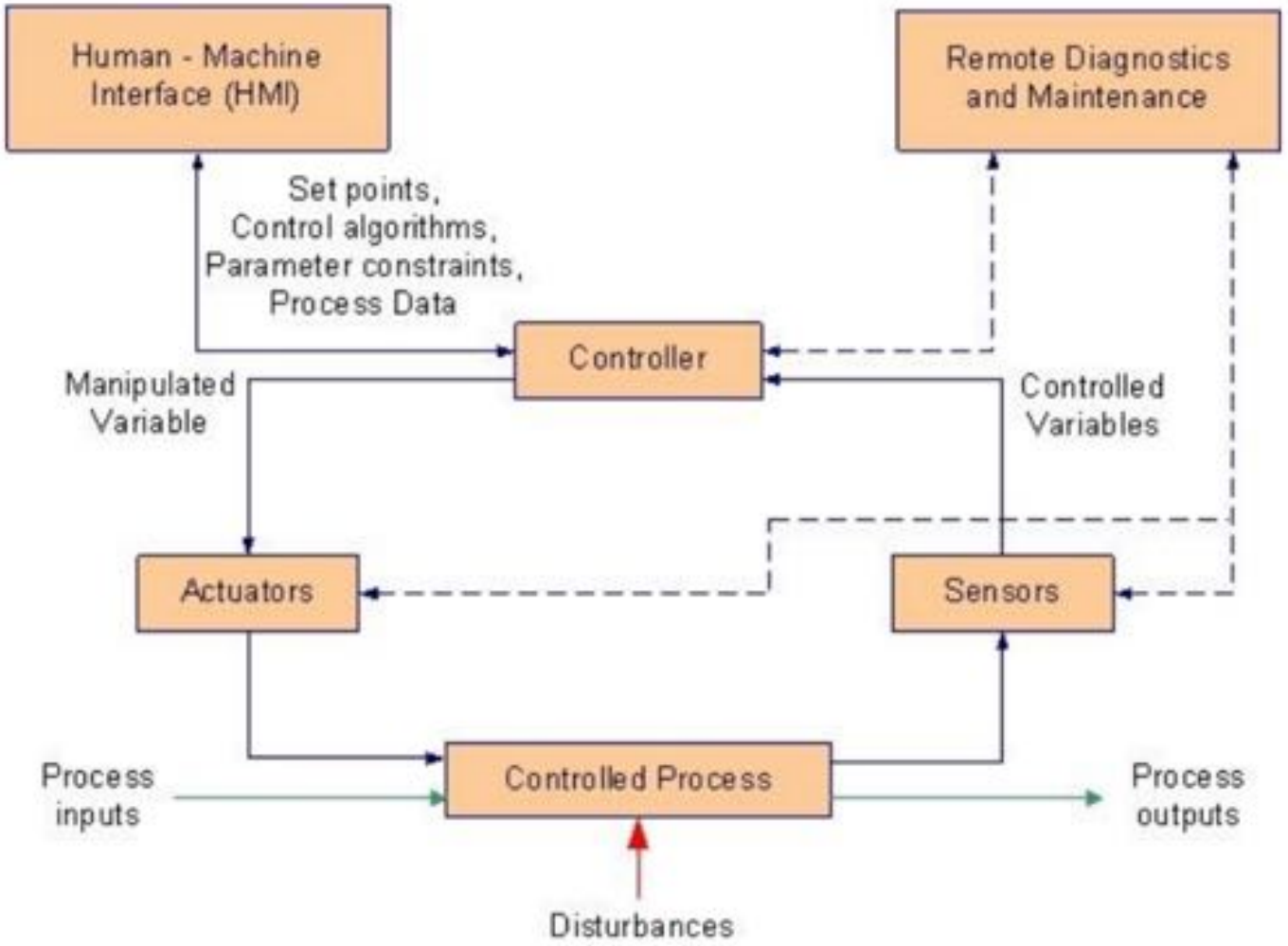
- Call upon Member States to address the danger of terrorist attacks against critical infrastructure.
- Coordinated efforts to raise awareness and exchange information and good practices.
- Each state determines what constitutes its critical infrastructure
- Importance of ensuring reliability and resilience

QUESTIONS?

ICS



ICS



*From NIST Special Publication 800-82