# INTRODUCTION TO INDUSTRIAL CYBERSECURITY

## 1ST SUMMER SCHOOL: DEEP TECH TRAINING WITH IMPACT ON ENTREPRENEURSHIP AND INNOVATION

**Miguel A. Prada, Universidad de León (Spain)**

GRUPO SUPPRESS
SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN
universidad de león

REGINNA 4.0

CIClab
Critical Infrastructure Cybersecurity Lab

# CONTENTS

1. Concepts
2. Relevance of industrial cybersecurity
3. Distinctive features of industrial control systems
4. Assets, threats, vulnerabilities and impact
5. Known incidents
6. Security measures

# Concepts

# CONCEPTS

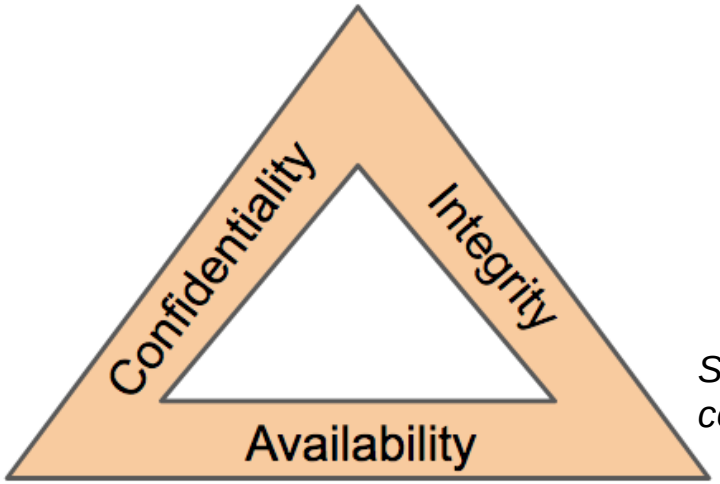
- **Industrial Process:** A process meant to obtain, transform or transport primary products
- **Automation:** Use of equipment and techniques to make an industrial process work with low human intervention
- **Control system:** It allows regulating another system to achieve the desired behavior

*Source: southernfield.com*

# CONCEPTS

- Modern control systems are **cyber-physical systems** combining control systems, computing and communications
- **Cybersecurity**: Protection of computer systems and networks against intentional attacks
- The way to deal with the cybersecurity problem is **risk** mitigation
- **Risk** = Likelihood of an undesired event X Impact


*Source: securingpeople.com*




*Source: certmike.com*

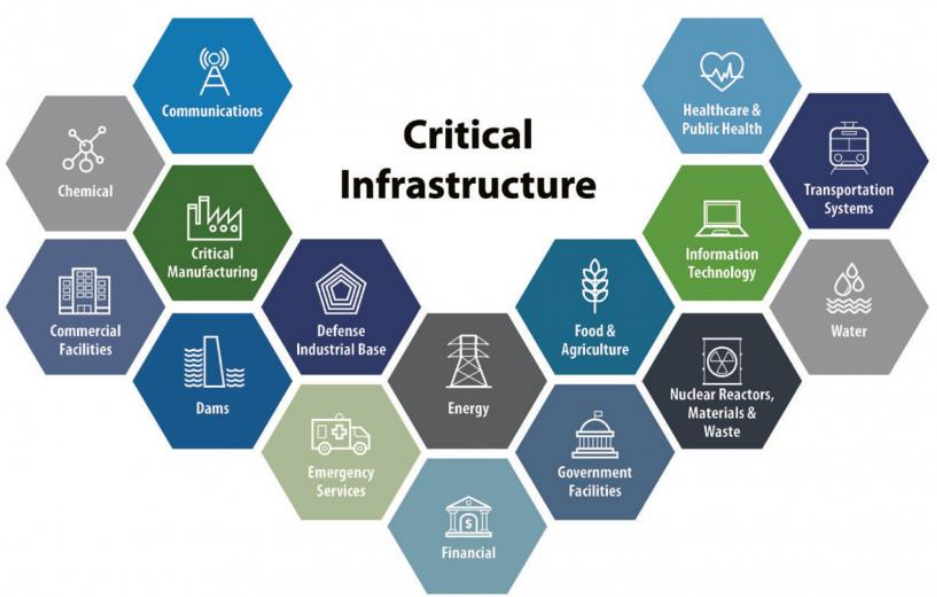
# Relevance of industrial cybersecurity

# UBIQUITY

- **Security of control systems is relevant because they are present in many areas:**
  - Industry
  - Building automation
  - Cars
  - Aircraft
  - “Smart” devices
  - **Critical infrastructures**
  - …

# CRITICAL INFRASTRUCTURES

- Control systems are essential components of critical infrastructures
- A **critical infrastructure** is a facility or system that supports services that are essential for the security and economy of a country




© US Cybersecurity & Infrastructure Security Agency (CISA)

- Laws and regulations are applicable

# A WRONG STARTING POINT

- ***Safety* or protection against accidental events has always been considered in control systems**
  - Prevention of damages in equipment, facilities and people due to natural disasters, failures or errors
  - Clear regulations and procedures

- **About *Security* or protection against intentional damages**
  - There have always been clear procedures for physical security against theft or sabotage
  - However, cybersecurity was not traditionally considered prioritary, neither by manufacturers nor by operators
  - Until recently, neither regulations nor standards

# REASONS

- **A false sense of security**
  - Untrained staff
  - It was assumed that the control system worked in complete isolation, without connection to other information systems (air gap)
  - Security by obscurity, since specific technology was used

- **However**
  - Convergence: currently, off the shelf software is massively used
  - For management and operation needs, control systems are connected to the corporate network  or the Internet
  - There is enough publicly accessible information about the technologies

~~**AIR GAP**~~

# CURRENT SITUATION

- **IT (information technologies) vs OT (*operational technologies*)**
- **Cybersecurity in industrial control systems less developed than IT cybersecurity**
- **The distinctive features of control systems make it difficult to apply the same solutions directly**

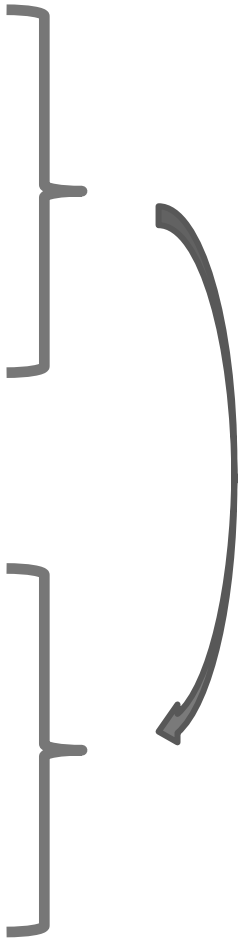
- **As a result, there is still:**
  - A lower level of maturity
  - A need for more systematic procedures
  - A need for adapted technologies
  - A need for training

# Distinctive features of industrial control systems

# DISTINCTIVE FEATURES OF CONTROL SYSTEMS

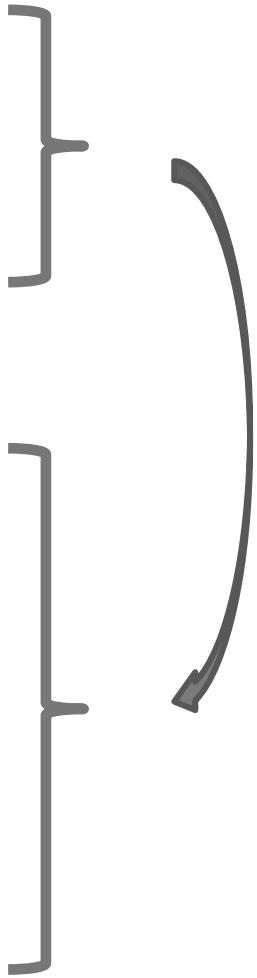
- **Great lifespan of facilities**
- **Continuous operation**
- **Availability is more important than integrity and confidentiality, unlike in other systems**
  - CIA → AIC

- **Difficult maintenance and patching**
- **Outdated technologies with limited protection or no security measures**
- **Some usual practices can't be applied because they hamper the normal operation of the system: antivirus, active scans, …**



# DISTINCTIVE FEATURES OF CONTROL SYSTEMS

- Often, low latencies and determinism or real time
- Specific software and hardware
- Specific, and potentially vast, network architectures



- Specific (and insecure) communication protocols
- Generally limited computational resources
- Difficulties to introduce changes, disable services or add additional software to the provided setup
- Log management and forensic analysis is difficult
- Certification or standardization might be compulsory

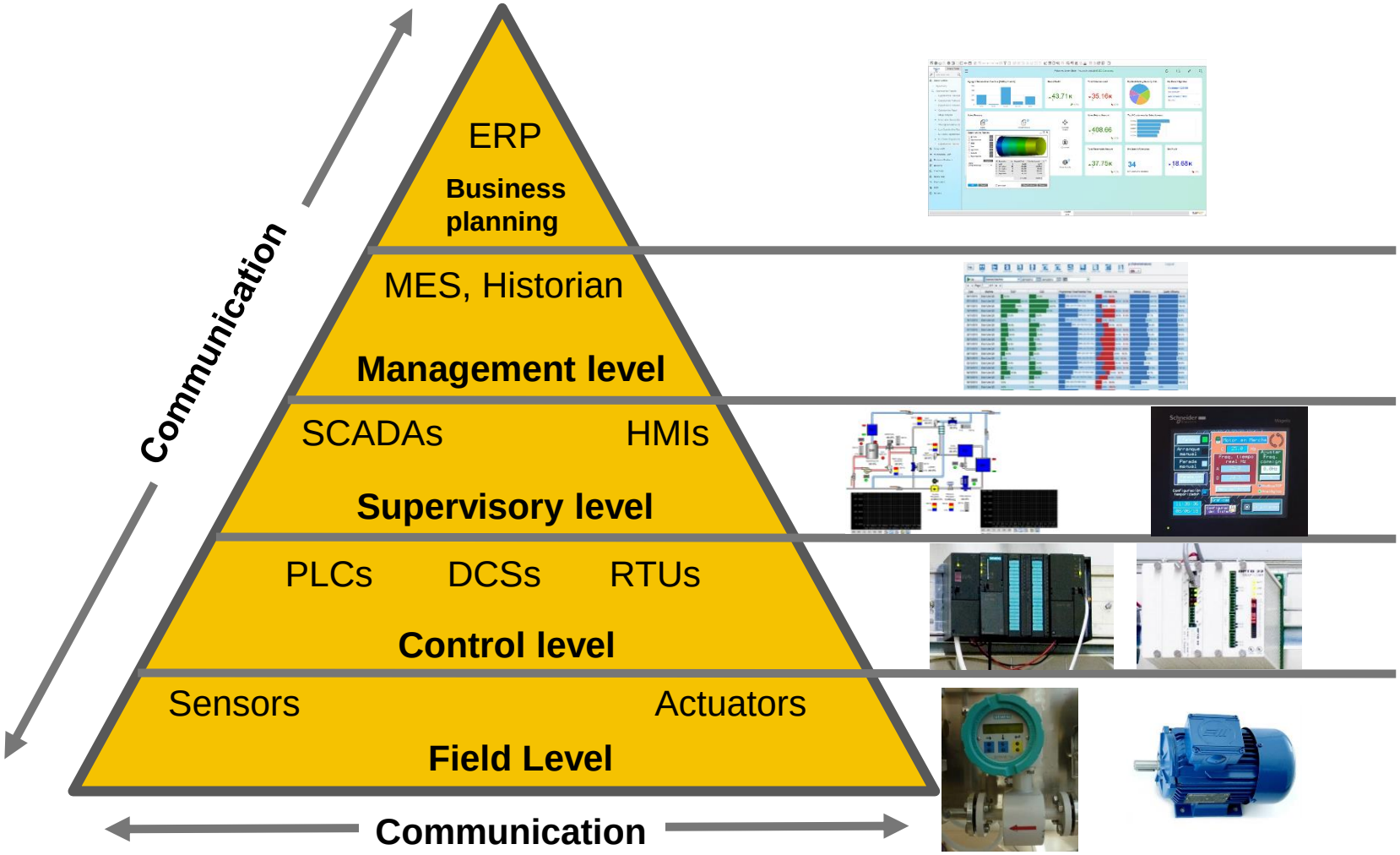
# DISTINCTIVE FEATURES OF CONTROL SYSTEMS

- **A part of the staff is not IT:**
  - Different priorities, language and training
- **Greater dependence on manufacturers/integrators of the control system**
- **More concrete impacts of cybersecurity incidents**

# Distinctive features: Architecture & technologies

# BASIC ARCHITECTURE OF A CONTROL SYSTEM

**Automation pyramid**

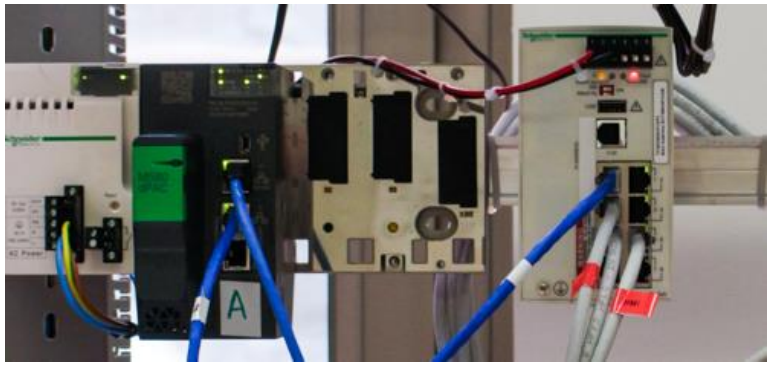


# BASIC ARCHITECTURE OF A CONTROL SYSTEM

- **Field level:**
  - Instrumentation, i.e., devices that interface with the physical world
  - Sensors measure values
  - Actuators act in the physical system

# BASIC ARCHITECTURE OF A CONTROL SYSTEM

- **Control level**
  - We have **control devices**:
    - The most general and common case is the **Programmable Logic controller (PLC)**
    - Other technologies, such as Distributed control systems (DCSs), Industrial computers, Remote terminal units (RTU), …



  - And the **engineering workstations**:
    - Computers used to program/manage the control devices

# CONTROL DEVICES: SECURITY FEATURES

- **Generally limited**
  - Password-protected program
  - Physical protection of program overwriting
  - Disabling, by default, the vulnerable services
    - Web and/or FTP services are often provided for monitoring, configuration or maintenance (and disregarded)

- **In the best case scenario (cutting-edge devices)**
  - Access control lists
  - Firewalls and ability to create VPN tunnels

# BASIC ARCHITECTURE OF A CONTROL SYSTEM

- **Supervisory level:**
  - Systems in charge of monitoring the production units and intervening on them
  - Decision taking, manual setpoints, data acquisition and processing, alarm management, etc.
  - **HMI** (Human Machine Interfaces)
  - **SCADA** (*Supervisory Control And Data Acquisition*) systems

# HMI AND SECURITY

- **Monitoring and control touch panels, to enable a quick visualization of the system variables, alarms and setpoints**
- **Losing its operation means losing visibility of the process**
- **Usually found in areas with strong physical security**
- **HMI operators usually don’t authenticate**
  - During an emergency, it might block access
- **Some specific functions have access control**

# SCADA AND SECURITY

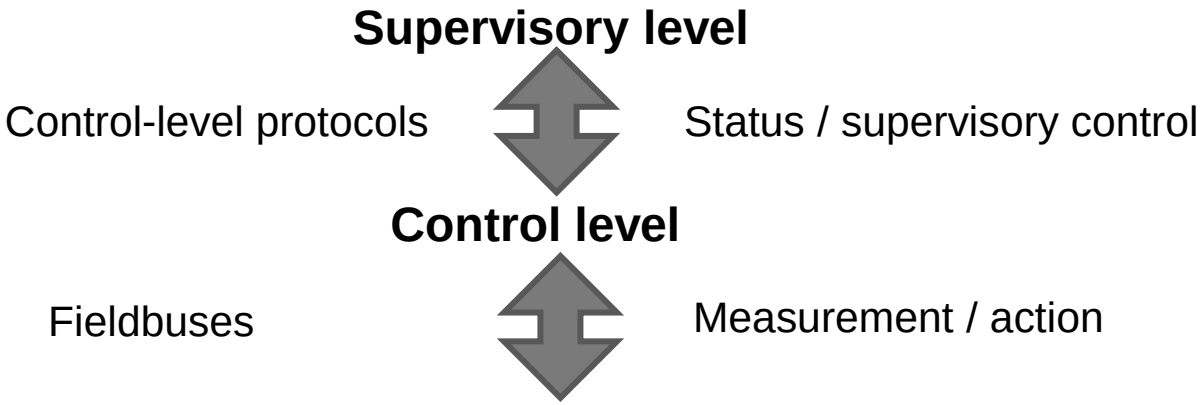
- **Software for real-time monitoring of industrial processes with a user interface. Remote control of systems is also available**
- **It is also known as *Building/Energy/… management system***
- **Redundancy at different levels might be needed**
- **The SCADA server must be hardened**
- **External access might be needed**
  - From the Internet or the business intranet
  - This connections must be protected to avoid they are used as an input vector to a cyberattack

*Source: EFY Bureau*

# Distinctive features: Industrial communications

# COMMUNICATION WITH THE CONTROL DEVICE

- **Communication during the control system operation**




- **Communication during device programming, configuration and maintenance**
  - Between the engineering workstation and the control device
  - Proprietary protocols or proprietary extensions of standard protocols
  - Before, serial protocols. Now, with Ethernet and TCP/IP

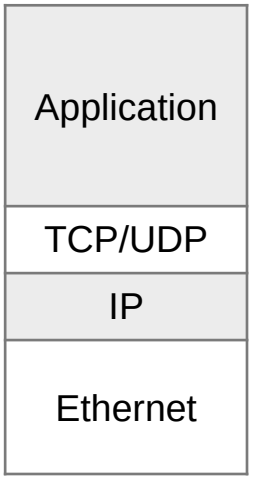
# FIELDBUSES

- **Designed to provide efficiency**
- **Serial communication, short messages, low computational resources**
- **Fundamental differences with other IT networks**
- **Often master-slave**
- **Only implement layers 1, 2 and 7**

| Application |
| --- |
| |
| Data link |
| Physical |

# CONTROL-LEVEL PROTOCOLS

- **Not only protocols to communicate between control and field levels, also higher in the pyramid**
  - Among control devices,  or between control and supervision
  - Different requirements




- **Generally over TCP/IP and, therefore, routable**
  - Of special interest then to cybersecurity
  - Non-periodical and larger messages, usually
  - Less strict time requirements
  - Strategies and changes to achieve real-time

# INDUSTRIAL PROTOCOLS

- **Several technologies competing for the market, but they are open standards**
- **Protocol families with alternatives for fieldbus and level-control protocol**
- **Applying Ethernet also in lower levels for increased interoperability is becoming a trend**

- **All of them <u>lack any security measure</u>**
  - They don’t implement encryption, authentication or integrity checks

# INDUSTRIAL PROTOCOL EXAMPLE: MODBUS TCP

- Modbus RTU frames  encapsulated over TCP/IP
- TCP used in the transport layer
- The server (slave) listens to port 502
- Point to point communication (unicast)
- Simple and widely supported
- Function codes and parameters/responses

# INDUSTRIAL PROTOCOLOS – SECURITY FEATURES

- **No authentication and *checksums* at the application level:**
  - Not possible to verify that the message comes from a trusted device
  - Integrity can't be checked
  - Possible simple *man-in-the-middle* (MitM) or *replay* attacks

- **No encryption:**
  - Information about addresses, function codes and values can be extracted directly from a traffic capture

# CONFIGURATION PROTOCOLS

- **For programming and parameterization of control devices, manufacturer software generally uses**
  - Proprietary protocols or proprietary extensions of open protocols
- **Extremely critical actions**
  - Replacing the control program or modifying the execution status: start/stop
- **The deficiencies of open protocols are inherited**
- **Furthermore, ignorance about the structure and content of the messages is an additional problem**
  - Only recently there are firewalls with support to filter these protocols

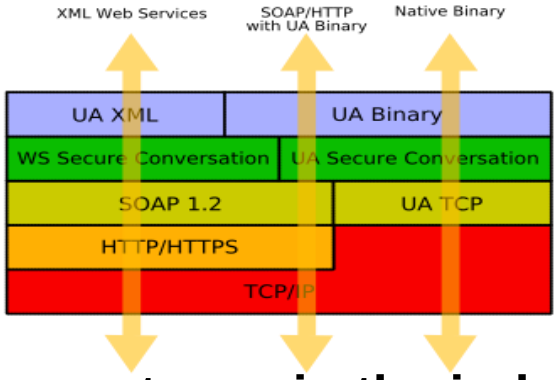
# OPC STANDARD

- **In complex systems, communication between SCADA and devices would required many different APIs**
- **Standardization need**


- **<u>OPC: Communication standard</u>**
  - Client-server architecture
  - The OPC client uses a standard interface
  - The OPC server translates from the OPC standard to the specific PLC drivers
  - Manufacturers provide OPC servers for their PLCs
  - Classic OPC, initially based on obsolete Microsoft technology → OPC UA, new platform-independent specification

# OPC UA

- **General features**
  - Binary or XML format (SOAP web services)
  - Device and process model: types, semantic information, links
- **Security features:**
  - Encryption with public key infrastructure
  - Token-based or certificate-based authentication
  - WS Secure Conversation,TLS.




- **The “modern standard” → quick acceptance in the industrial area**
- **It can be used in more scopes than classic OPC**

# TREND: INDUSTRIAL DIGITALIZATION

- **Industry 4.0, Connected Industry, Industrial Internet of things, … → IT/OT Convergence**
- **Approach centered on cyber-physical systems**
- **The digitalization process is replanning the way an industrial control system works:**
  - Greater connectivity
  - Closer integration with IT services
  - Application of new enabling technologies such as digital twins, augmented reality, mobile interfaces, additive manufacturing, collaborative robotics, web and cloud services
  - Data analysis to improve the process and product
  - Closer integration with providers and customers

# TREND: INDUSTRIAL DIGITALIZATION

- **Since functions, exposed as services, must be available for different resources**
  - Generic technologies such as HTTPS, OPC UA, MQTT or CoAP are increasingly used
  - Especially when communicating with edge and cloud

- **Protocol updates to include security measures**
  - Modbus/TCP *security* or CIP *security*:
    - Too late for general acceptance

# Distinctive features: Other application fields

# BUILDING AUTOMATION

- **Similar protocols to the industrial field**
- **Generally available over several physical layers**
- **Programming is usually simpler → Creating groups, linking blocks, etc.**
- **Situation *slightly better* with respect to security**

*Source: Dave Miller, aquilacommercial.com*

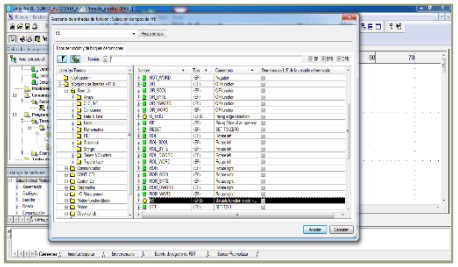
# ELECTRICITY SUPPLY MANAGEMENT

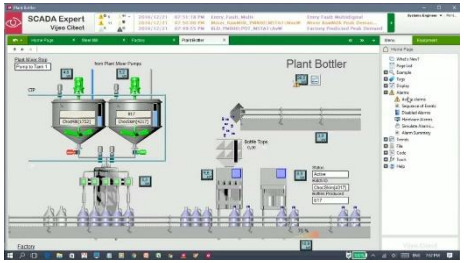
- **Vast and complex system:**
  Generation ⇔ transport ⇔ distribution ⇔ consumption and measurement
- **Electricity transport and distribution**
  - Control, protection and measurement in their substations
    - Some control devices have to react fast to avoid supply interruption
    - Other devices control the management of substations and transforming centers as devised in network planning
  - Elements for supervision in remote control centers
  - Communication technologies inside substation and with the control centers: IEC 60870-5 101 & 104, DNP3 and IEC 61850
- **Great attack surface, from generation to consumption → Physical security is difficult**
- **Smart meters are physically accessible → Privacy and fraud**

# Assets, threats, vulnerabilities and impact

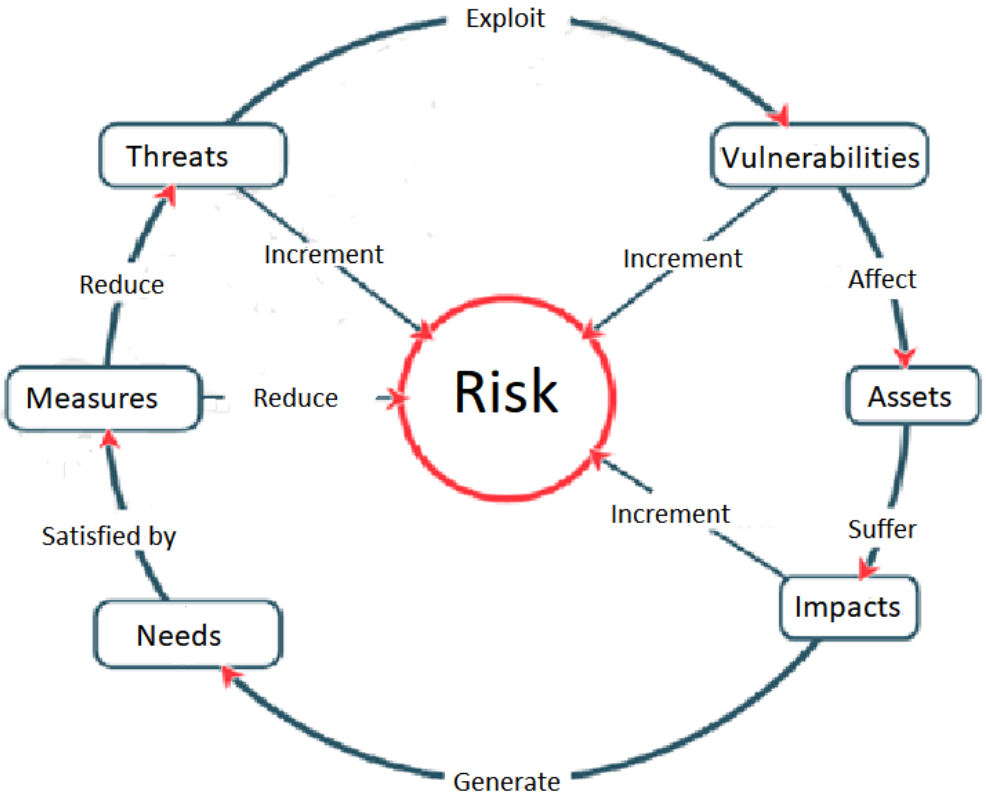
# ASSETS

- **Targets that might suffer a threat**
  - Engineering workstations, PLCs, RTUs, etc.
    - Project files
    - Program Logic
    - Firmware
  - HMIs, SCADAs and historians
  - Network devices and security elements (filtering elements, authentication and authorization, …)




# THREATS




*Source: Incibe*

- Every **threat** has:
  - An agent (who)
  - A vector (how it starts)
  - A target
- And requires:
  - Skills
  - Intention
  - Opportunity
- Types of threats:
  Internal or external
  Targeted or untargeted

# VECTORS AND INITIAL TARGETS

- **Typical vectors of directed attacks:**
  - Social engineering
    - *Spear Phishing*
    - Removable devices
  - *Watering Hole*
  - SQL injection / XSS in web
  - External staff / VPN access stolen

- **The initial aims are:**
  - SCADA servers and historians
  - Remote accesses, network devices, etc.

# SPECIFIC THREATS

- **Control elements can be subject to the following threats:**
  - Firmware alteration
  - Execution mode alteration (e.g., stop)
  - Interception or alteration of the control program to observe or modify (temporally o permanently) its activity
  - Interception or alteration of communications
- **And supervisory elements to threats in:**
  - The integrity of communications with other elements
  - The integrity/authenticity of process data

# SPECIFIC THREATS

- **Advanced persistent threat (APT)**
  - Directed attack by very capable specialists
  - It might be oriented to interrupt the system operation
  - Sophisticated attack with multiple stages
  - Initial gathering of relevant information
  - Sophisticated vectors
  - Remains hidden but operating for a long time
  - Uses diverse malware

# VULNERABILITIES

- **The system might be vulnerable at the level of:**
  - Host
    - Configuration
    - Software
    - Hardware
  - Network
  - Policies and procedures

- **Every level of the pyramid might face different vulnerabilities**

# HOST VULNERABILITIES

- **No physical protection of devices and interfaces**
  - Disassembly of de device, analysis of technical documentation, *bus snooping, memory dumping*
- **Unrestricted removable devices**
  - Malware infection through USB
- **No integrity protection for firmware**
- **Insecure coding in firmware, OS or application**
  - No input validations
  - Buffer, heap or array overflows
  - SQL injection, XSS y CSRF in web services
- **Outdated devices**
- **Default configurations and unnecessary services**

# NETWORK VULNERABILITIES

- **Unclear and undocumented logic architecture**
  - Although the physical one is usually clear
- **Inadequate or inexistent segmentation**
- **Incorrect configuration of filtering devices**
- **Insecure protocols**
  - *All industrial protocols but OPC UA*
  - Less problematic in other automation areas
  - Susceptible to DoS, information interception and *man-in-the-middle*
  - In proprietary configuration protocols, we add:
    - Ignorance of structure and content of the messages → it is difficult to detect a misuse

# VULNERABILITIES OF POLICIES AND PROCEDURES

- **With regard to staff and third parties**
  - Deficiencies in policies for account and password management
  - Lack of staff awareness and training: might fall prey too social engineering
  - Inadequate use of mobile devices
- **With regard to assets**
  - Deficiencies in configuration control and change management
  - Lack of formal documentation
  - No auditing or responsibilities
- **With regard to incidents**
  - Lack of appropriate plans for incident and recovery management

# IMPACT

- **Loss of view**
- **Loss of communication**
- **<u>Loss of control</u>**

- **Which, in turn, might cause more concrete impacts:**
  - Damage to people, equipment, environment
  - Impact to national security
  - Loss of production, quality, confidential information
  - Reputational damage
  - Violation of legal requirements, etc.

# RISK ASSESSMENT

- **Prioritize risks reduction measures**
  - A difficult art
  - We need to estimate the impact and the probability
  - Knowledge about the industrial control systems, their function and weaknesses
  - Knowledge about the global trends
  - Think from the perspective of an attacker
  - Different models or frameworks

# Known incidents

# AURORA PROJECT

- Experiment in Idaho National Laboratory, 2007
- Viability assessment of cyberattacks on control systems
- Classified information until 2014
- A diesel generator
- Operation with protection relays
- Desynchronization of the generator con the power network
- They made it explode

## Aurora Project Review

- A vulnerability was discovered and an Interagency Tiger Team was formed
- Initial concerns and modeling results were confirmed by a physical test March 4 2007
- Test resulted in a total loss of generating capability with extensive damage in about 3 minutes
- A strong example of interagency cooperation and public-private partnership

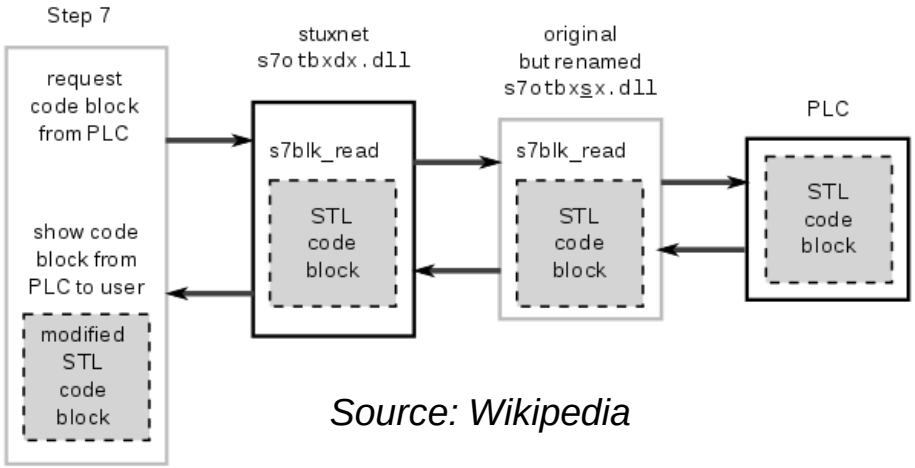
Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

3

# STUXNET

- **2010. First *malware* oriented to attack control systems**
- **Target**
  - PLCs with a certain configuration (Siemens S7)
  - That controlled the frequency of AC motors such as the ones used in uranium centrifuges
  - Modify the operation of the PLCs in an imperceptible way




*Source: Wikipedia*

GRUPO SUPPRESS
SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN
universidad de león

REGINNA 4.0

# STUXNET

- **Worm and rootkit properties:**
  - Main means of infection were USB drives
  - Exploited 4 zero-day vulnerabilities
  - Able to infect from Windows 2000 to 7/Server 2008R2
- **Using valid digital certificates**
- **Complex communication with C&C**
  - P2P network
- **Behavior depends on the host**
  - If it is not its target→ rootkit that loads malware in startup and deploys different propagation tactics
  - If it is the target → payload

# STUXNET

- **Payload:**
  - It copies in the SCADA database to modify monitoring screens
  - Replaces communication DLL with the PLC and copies itself to the project files
  - Looks for systems controlling AC motors with a very high frequency
  - When it finds that configuration, it changes back and forth the frequency to render them useless
  - It interferes in the process while deceiving the system operators

# STUXNET

- **Lessons learnt**
  - Advanced persistent threat
    - Estimated effort over 6 person-years and probably investment in a replica of the environment
    - Extremely high resources, ability and motivation
  - Cyberattack as a weapon
    - 60% of de devices in Iran
  - Vulnerabilities exploited
    - Of the device, both in the OS and the specific software (WinCC / STEP 7)
    - Of the procedures: insufficient control of removable devices
    - Of the network: communications with auxiliary services

# STUXNET

- **Lessons learnt**
  - Protection measures
    - It’s difficult to defend against such a sophisticated attack
    - Reinforce network and  perimeter security
    - Use whitelisting
    - Monitor security events

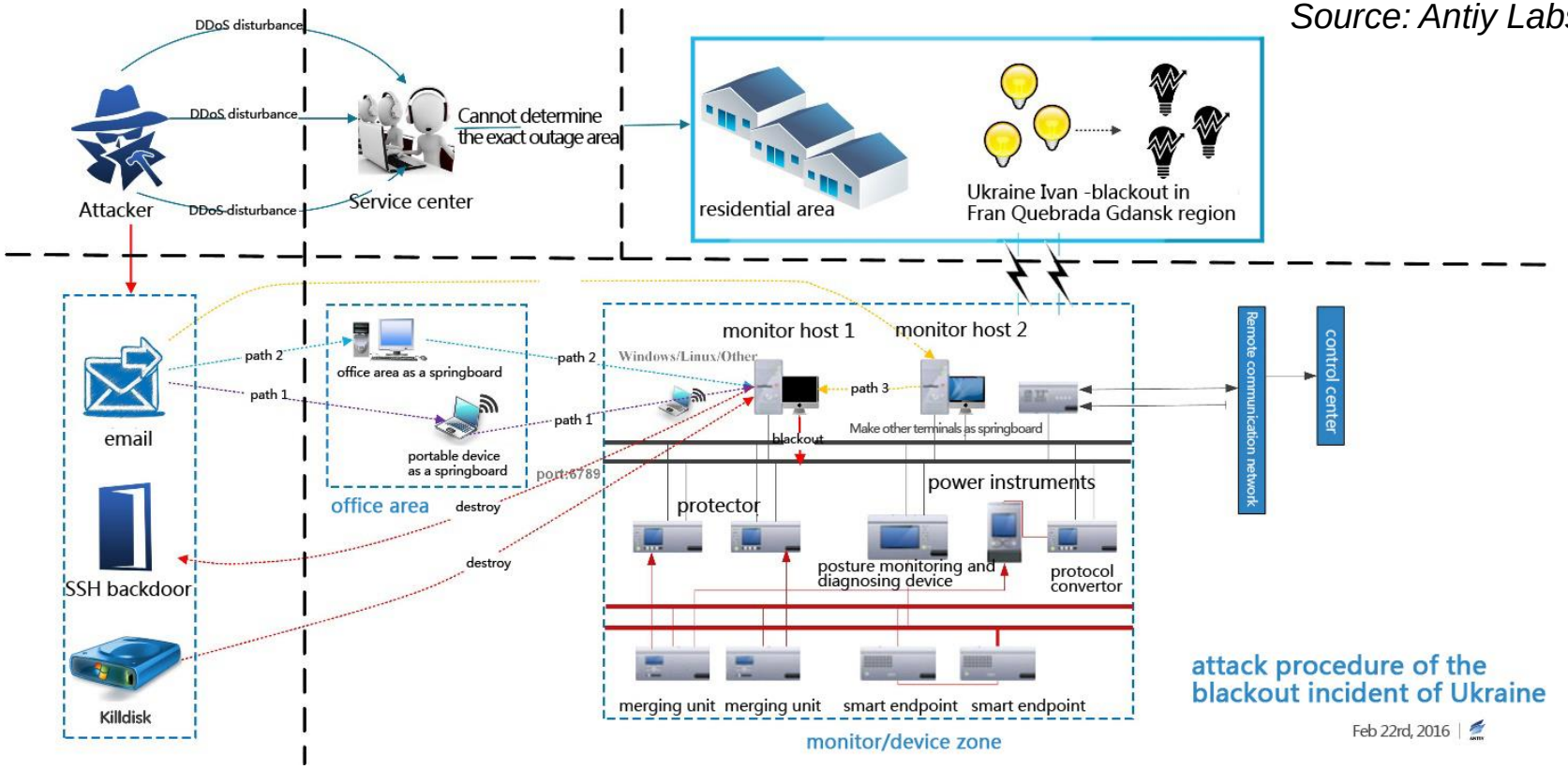
# UKRAINIAN ELECTRICITY NETWORK

- **2015, affected 225,000 people for 6 hours**
- ***Spear phishing* with Excel files to obtain credentials and gather information**
- **Used  BlackEnergy (3) malware**
- **But service interruption was caused by the direct interaction of the attackers**
- **Connection through compromised VPNs and remote desktops to send commands from SCADAs**
- **Coordinated attacks to gateways and routers firmware, disk wiping with KillDisk, manipulation of UPSs**
- **DoS to the phone customer service**

# UKRAINIAN ELECTRICITY NETWORK

- **Advanced persistent threat**
- **Joint and coordinated exploitation of several vulnerabilities**

*Source: Antiy Labs*



# CRASHOVERRIDE/INDUSTROYER

- **Incident in an Ukrainian substation in 2016**
- **<u>Spear Phishing.</u> In this case, a malware was used to open the relays**
- **The malware shows the level of evolution in the attacks:**
  - Platform to attack electricity distribution systems, but not restricted to a single manufacturer
- **It exploits several protocols**
  - OPC DA, IEC 101 y 104 e IEC 61850
  - To gather information but also to send commands

- **Spear phishing once again → More training/awareness**
- **Vulnerabilities of protocols and devices**
- **First reusable malware platform → Qualitative leap**

# Security measures in control systems

# DEFENSE IN DEPTH

- **Several layers of security measures to improve protection:**
  - Data security
  - Host security
    - Patching management
    - Intrusion prevention
    - Anti virus protection
    - Host firewall
    - Server hardening
  - Internal network security
  - Perimeter security
  - Physical security
  - Policies and procedures

# APPROACH

- **How to decide systematically the measures we apply:**
  - Standards - **IEC 62443**
  - Security models- NIST Cybersecurity Framework

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# POLICIES AND PROCEDURES

- **Apart from corporative security policies, specific policies for control systems should be added**
  - Change management: they should be managed as a small project
  - Cybersecurity assessment in acceptance tests
  - Human resources and acceptable use of resources
  - Supply chain management
    - Security of acquisition, development and maintenance
    - Standard compliance and contractual demands
  - Incident response:
    - Regulation compliance
  - Recovery plans and continuation of activity
    - Define degraded operation modes

# CREDENTIALS AND PRIVILEGES

- **Privileges**
  - Least privilege principle
  - “Deny all” policy
  - Unambiguous identification principle
  - Role-based privilege management
- **Good practices of authentication and authorization**
  - Multi-factor authentication, biometric authentication, challenge/response, tokens, etc.
- **Good management of accounts and passwords**
- **Monitor user activity**

# SECURITY OF DEVICES

- **Physical security**
  - Cover, ports
  - Prevent boot from removable devices
- **Service separation when necessary**
  - Virtualization, sandboxing
  - Especially if a vulnerable service must be exposed
- **Hardening**
  - Block unnecessary ports and services
  - Secure boot, partitioning
  - Enable authentication, privileges, …
  - Change default users/passwords
  - Host-based firewall

# SECURITY OF ENGINEERING AND MONITORING STATIONS/SERVERS

- **They should be dedicated computers**
- **In controlled rooms, without access to the Internet**
- **Hardened as determined by the manufacturer, blocking unused services**
  - Well documented
  - Administrator must check logs frequently
- **We should keep**
  - confidentiality and integrity of configuration and communications with the control device,
  - authenticity and integrity of software, logs and authentication methods
  - availability of event logging

# SECURITY OF CONTROL DEVICES

- **Trusted firmware**
- **Authentication in the management interface**
- **Secure secret storage**
- **Ensure integrity and confidentiality**
  - Of configuration and control strategy
- **Ensure authenticity**
  - Of control strategy, commands and execution mode
- **Ensure integrity**
  - Of logs and alarms
- **Control the access to physical interfaces**

# UPDATES AND PATCHES

- **Patch management:**
  - It is unacceptable to patch a system in operation
  - It would be desirable to patch a system replica, but it is usually too expensive
  - Patch during planned system stops
    - A few ones per year and staff is busy

- **Secure sources**
  - Verify integrity and authenticity
  - Intermediate update server in DMZ
  - End of support management

# ANTIVIRUS VS WHITE LISTS

- **Antivirus**
  - High computational load → they might not be supported
  - Too disruptive → loss of availability
  - Blocks only known threats
  - Needs frequent update (that might be impossible)

- **White lists**
  - For files and applications
  - Useful because control systems are highly static
  - Only accepts changes that were verified for the system
  - Doesn't need so frequent updates

# SCANNING TOOLS

- **It is important to know the latest vulnerabilities**
- **But the use of automatic tools might not be possible in production environments**
  - Enumeration /discovery
  - Vulnerability scanners
- **Active tools might have a disruptive behavior that might harm availability**
  - Don’t use in operation

# PERIMETER SECURITY

- **Remote access is a necessary evil**
- **Minimize attack vectors: only one way in**
  - Use Virtual Private Networks
  - Users should only have access to the specific systems and applications they need
  - Prevent direct access to critical systems
  - Avoid storing credentials in the remote computer
  - Log everything
- **Firewall to filter allowed traffic and Intrusion prevention system (IPS) for malware detection**

# NETWORK SECURITY: SEGMENTATION

- **Segmentation**
  - At the data link or network layer
  - Separating in small networks that are easier to handle makes it easier to decide and configure the additional security controls

- **“Zones and conduits” model**
  - The idea is to group similar/related devices and the communications among them
  - Functional groups based on: network connectivity, processes or control loops, level of the pyramid, users and roles, criticality, etc.
  - For each one, a required security level might be set → And so, systematically decided which countermeasures are needed

# SEGMENTATION TECHNOLOGIES

- **Data diodes**
  - Communication in one direction is physically impossible
- **VLANs**
- **Firewalls / Intrusion prevention systems (IPSs)**
  - IPS is problematic in control zones, as it might damage availability
    - Preferable between industrial and business networks or in semi-trusted DMZs
  - Guarantee that undefined or malware and exploit-related traffic does not cross zone limits
- **Firewalls / IPSs with application-level filtering**
  - Less frequently available than expected

# INTRUSION DETECTION SYSTEMS

- **Based on signatures or based on anomaly detection**
- **Useful in control systems because they don't block traffic**
- **Nevertheless, the analysis should rather be done transparently, without an effect of the network latency**
- **For that reason, we will use:**
  - Tap
  - Port mirroring

# SEGMENTATION TECHNOLOGIES

- **Routers/Firewalls**
  - Hirschmann Eagle
  - Cisco 800 Series Industrial
  - Siemens Scalance M/S
  - …

- **Integrated communication processor**
  - Siemens CP 1x43-x para S7 1500

- **Firewalls/IPS with application-level filtering**
  - Stormshield SNi40
  - Tofino Xenon SA
  - …

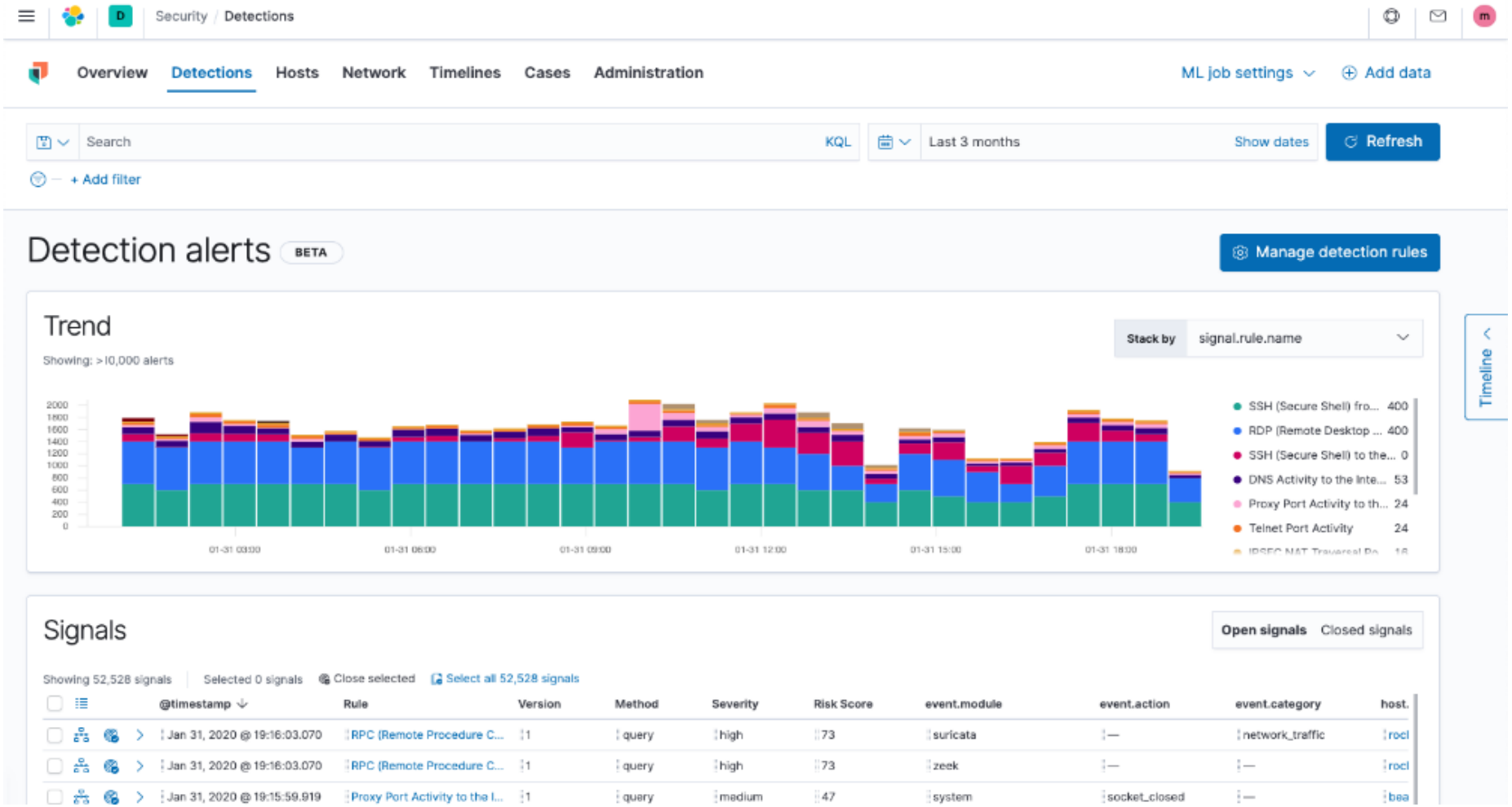

# EVENT LOGGING

- Logs of OS, applications, devices,…
  - ***In industrial devices it might be severely limited***
- Details and statistics of traffic: links, protocols, …
- Alarms generated by firewalls, routers, anti-malware tools, IDSs and IPSs, etc.
- User activity
- Configuration changes
- Additional context information
  - About the industrial process, generally obtained from historians

# SECURITY MONITORING

- **Monitoring of security events is key**
  - For incident response, forensic analysis, auditing and documentation
  - Available information exceed the storage and analysis capacity
- **We need to decide what and where to monitor**
- **Security information and event management (SIEM) systems or event correlators**
  - To enable detection, filtering and deep analysis of events
  - Queries, alerts and reports
  - Visual analysis

# SECURITY MONITORING



# FORENSIC ANALYSIS

- **Difficulties**
  - Diversity of platforms
  - Often obsolete systems
  - Impossibility or difficulty to use common tools
  - Lack of documentation of proprietary solutions
  - Insufficient knowledge: dependence on the manufacturer / integrator
- **Recommendations**
  - Exploit the static nature of the system to obtain metrics or hashes
  - Isolated environment for PLC testing
  - Analysis through serial ports or closer to hardware