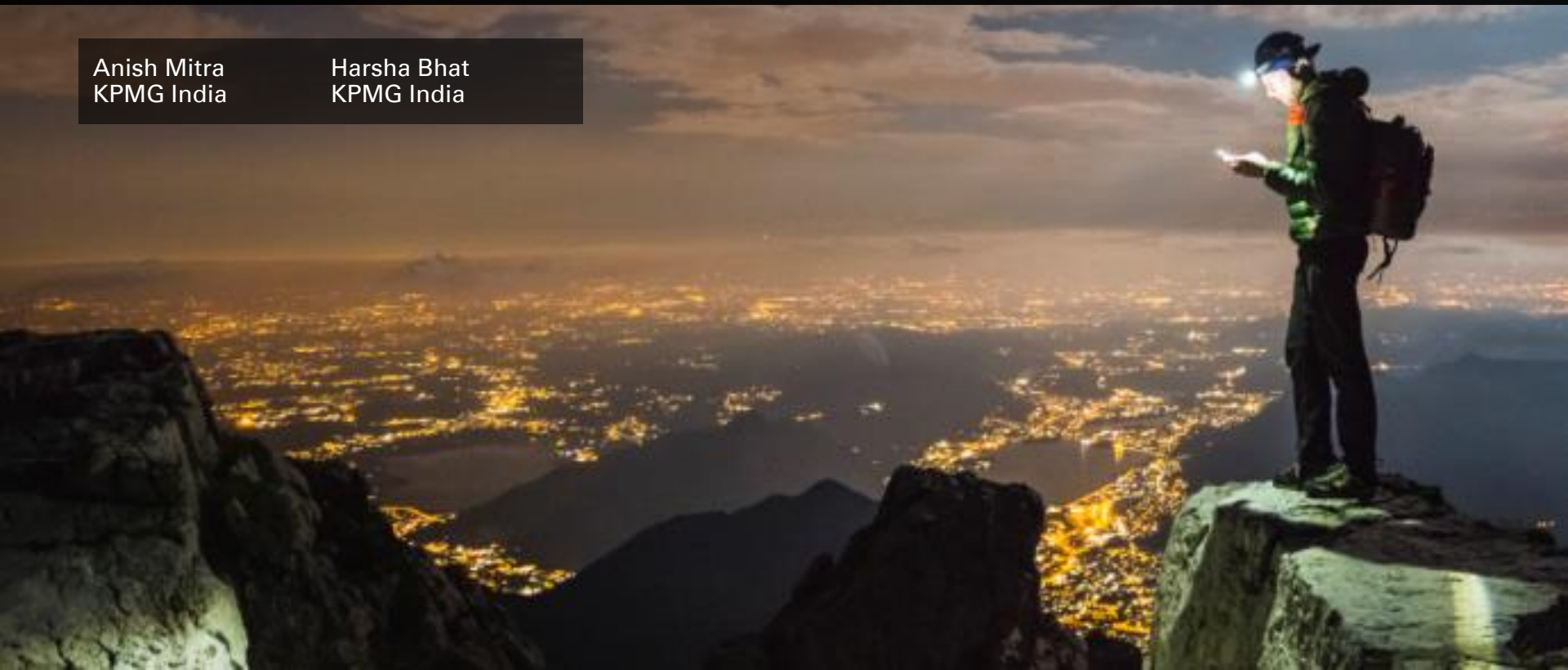
KPMG

Who turned off the lights!

The State of Industrial Control System Security Implementation

Anish Mitra
KPMG India

Harsha Bhat
KPMG India



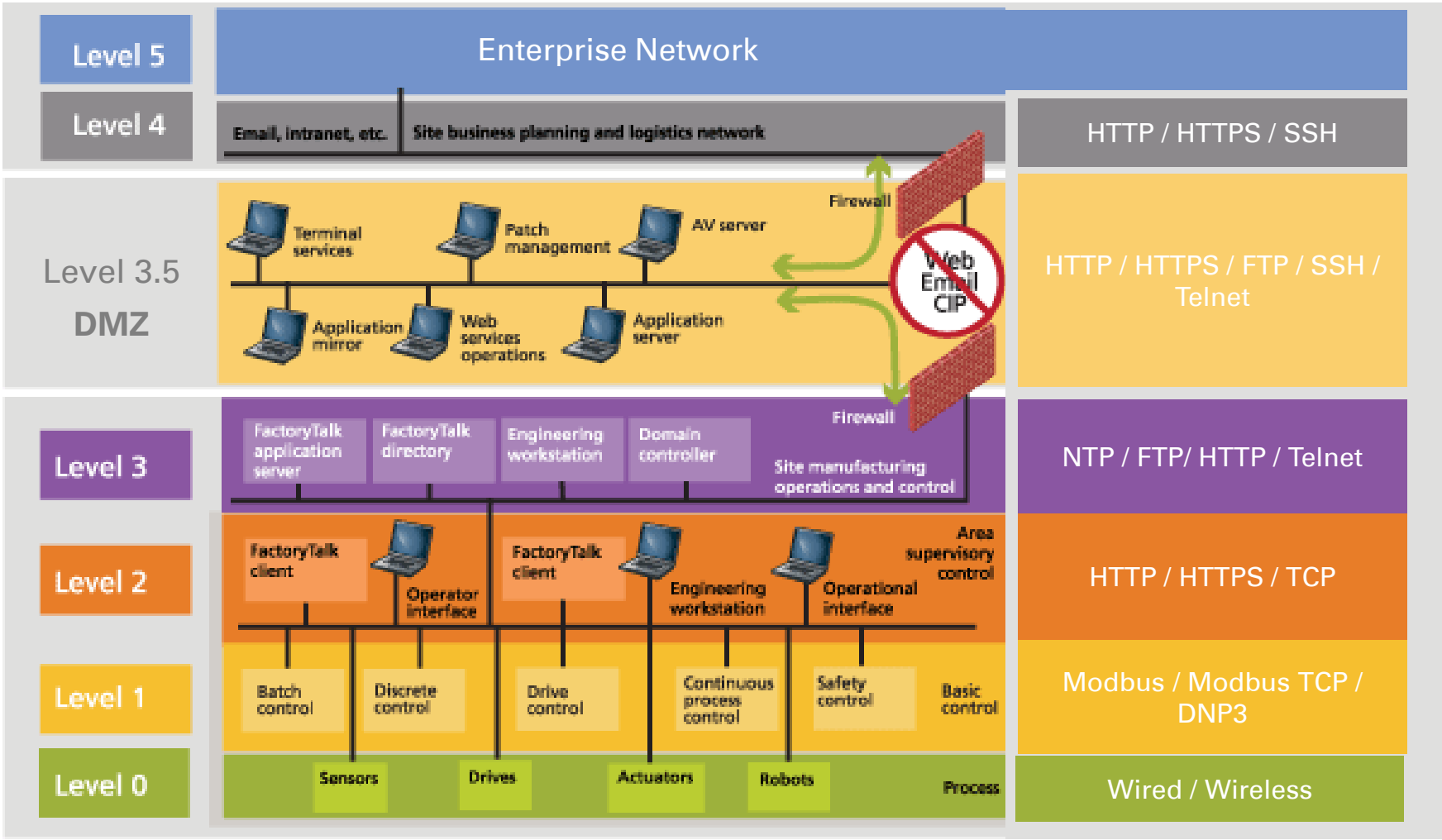
Introduction | Industrial Control Systems

What are Industrial Control Systems?

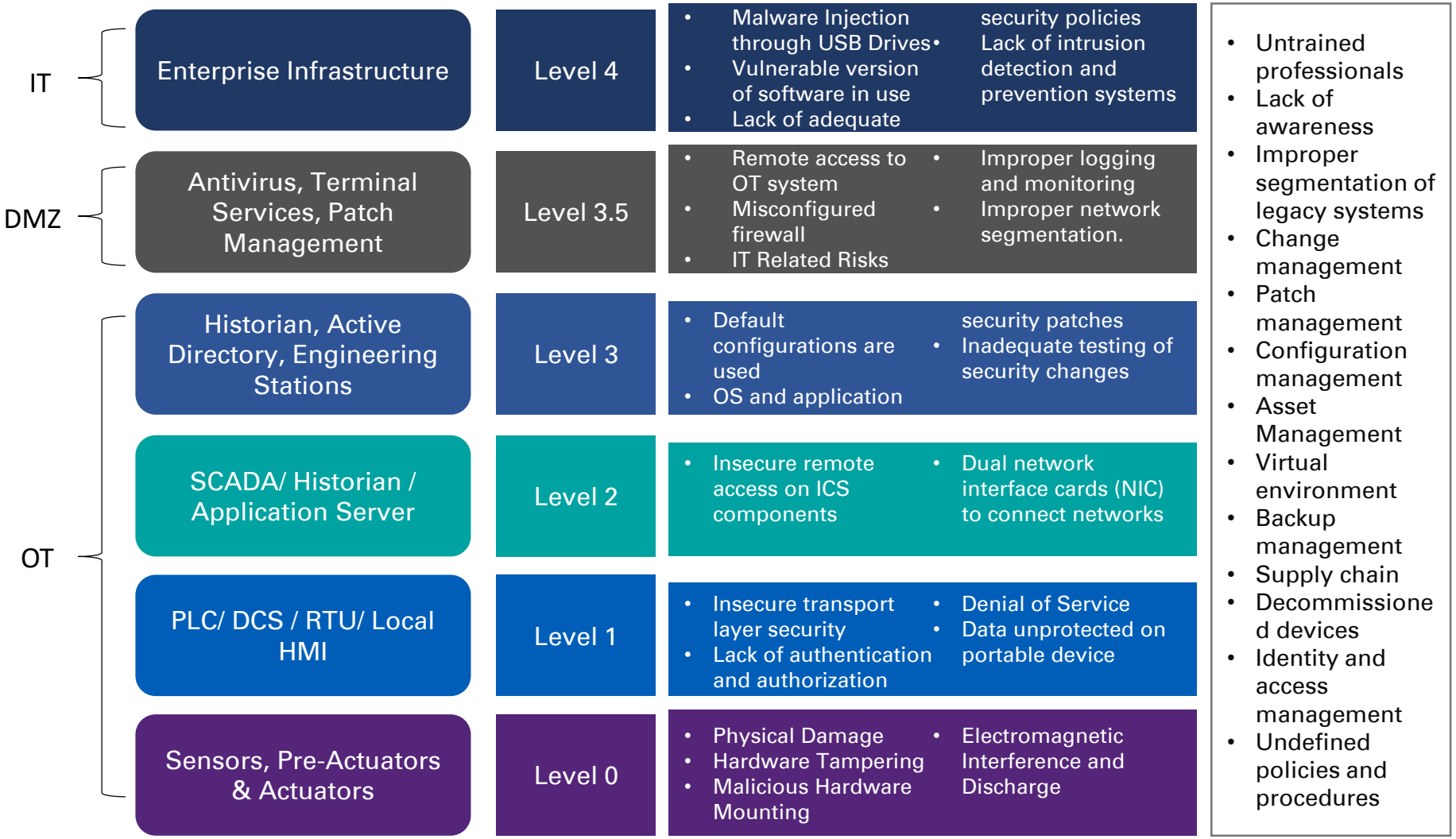
> **Industrial control system (ICS)** is a term used to describe an umbrella of control systems and automation instrumentation that include logic controllers, networks, servers and application software

- Sensors and actuators: allow interaction with the physical world (pressure sensor, valves, motors, ...)
- Local HMI: Human-Machine Interface, permits the supervision and control of a subprocess
- PLC: Programmable Logic Controller : manages the sensors and actuators
- Supervision screen: remote supervision of the industrial process
- Data historian: Records all the data from the production and Scada networks and allows exporting to the corporate IS (to the ERP for instance)

Purdue Model | Blueprint of Standard OT Network



ICS Threat Landscape



When worlds collide | The IT-OT Security Convergence

1. **Confidentiality is the top priority.** In order of importance, priorities are: confidentiality, integrity and availability
2. Use of hardware, software and communication systems used to input, store, process and output data
3. The goal is to achieve effective business operations through enterprise solutions, using modern Ethernet and Wireless Protocols

IT

OT

1. **Control and Availability is the top priority in OT.** In The new order: control, availability, integrity, and confidentiality
2. Use of hardware and software elements to perform real-time monitoring, automation, device control and generate events
3. The goal is to achieve automation of machines, processes and systems through point-to-point network in isolated environments

Convergence of IT and OT domains have given rise to shared Cyber Security concerns

Open-ended access to all devices emerging out of the IT network which allow remote control of OT devices

Wide range of OT protocols which use cleartext communication that allows eavesdropping

Advanced threat vectors acting on the OT network causing not only data loss but potentially could harm the human life as well

IIoT / SMART Factories | Changing Attack Vectors

Drivers for IIOT / Smart Factory and Security

Smart Maintenance Systems

- Autonomous maintenance systems would add more attack vectors to the picture

Self-driving vehicles

- The attack vectors on wireless communication would add-on due to autonomous vehicles on the shop floors

Robotic Fixtures

- The robotic fixtures would be maintained and controlled through mobile apps

Smart Supply Network

- Connected inventory tracking and supply chain

Mobile Workforce

Attack Gains

Intellectual Property

Service Disruption

Physical Harm

Monetary Gains

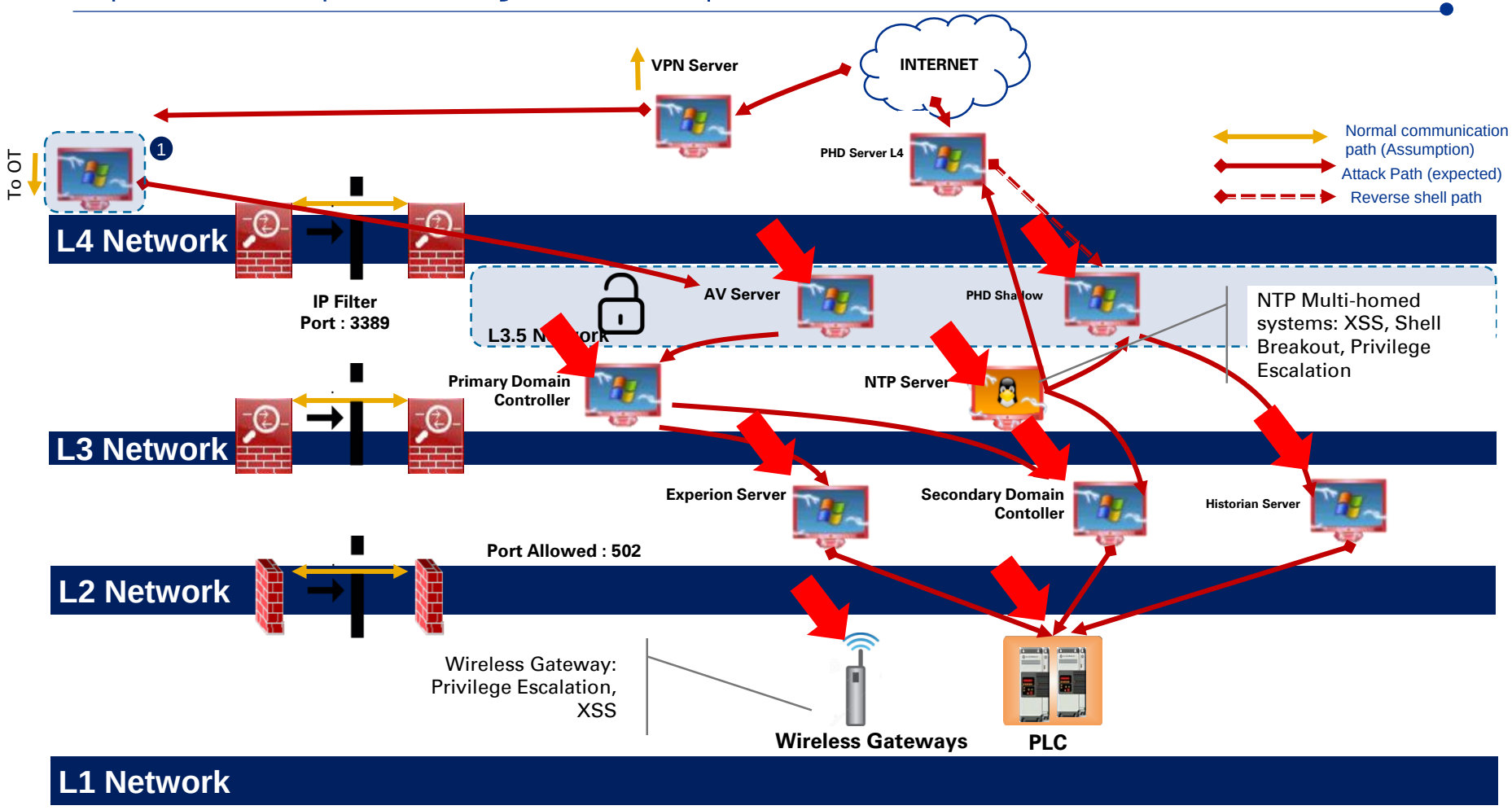
Why is it difficult?

- Different vendors and service providers
- Lack of vendor support for security updates
- Proprietary software and protocols
- Lack of support for network security controls
- Lack of interoperability
- Lack of support for security unified monitoring and operations

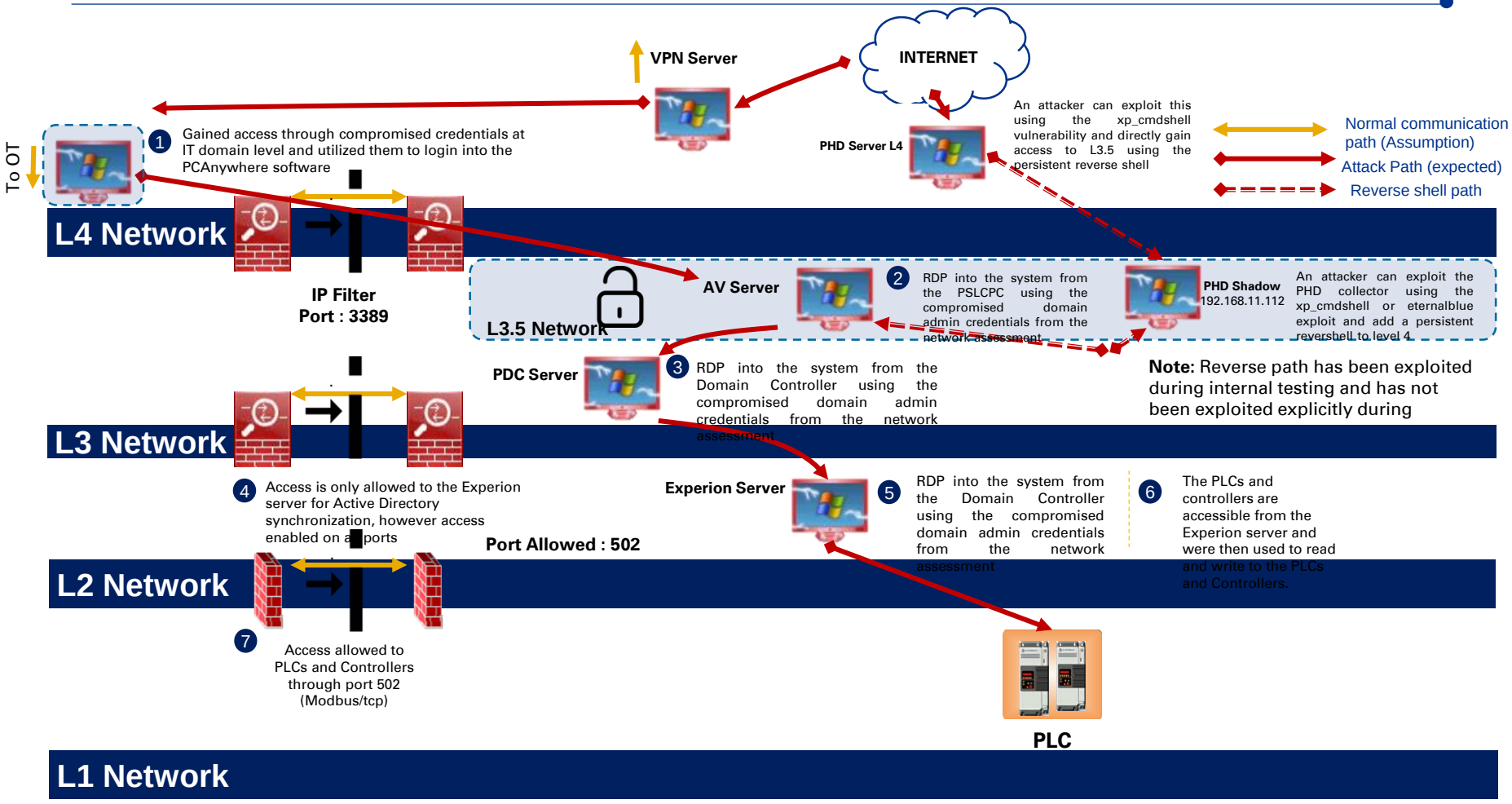
New Attack Vectors ?

- 802.15 Wireless HART Protocol
- Cloud Services connected to ICS infrastructure
- External services in the cloud environment
- Supplementary IT Services which may be vulnerable

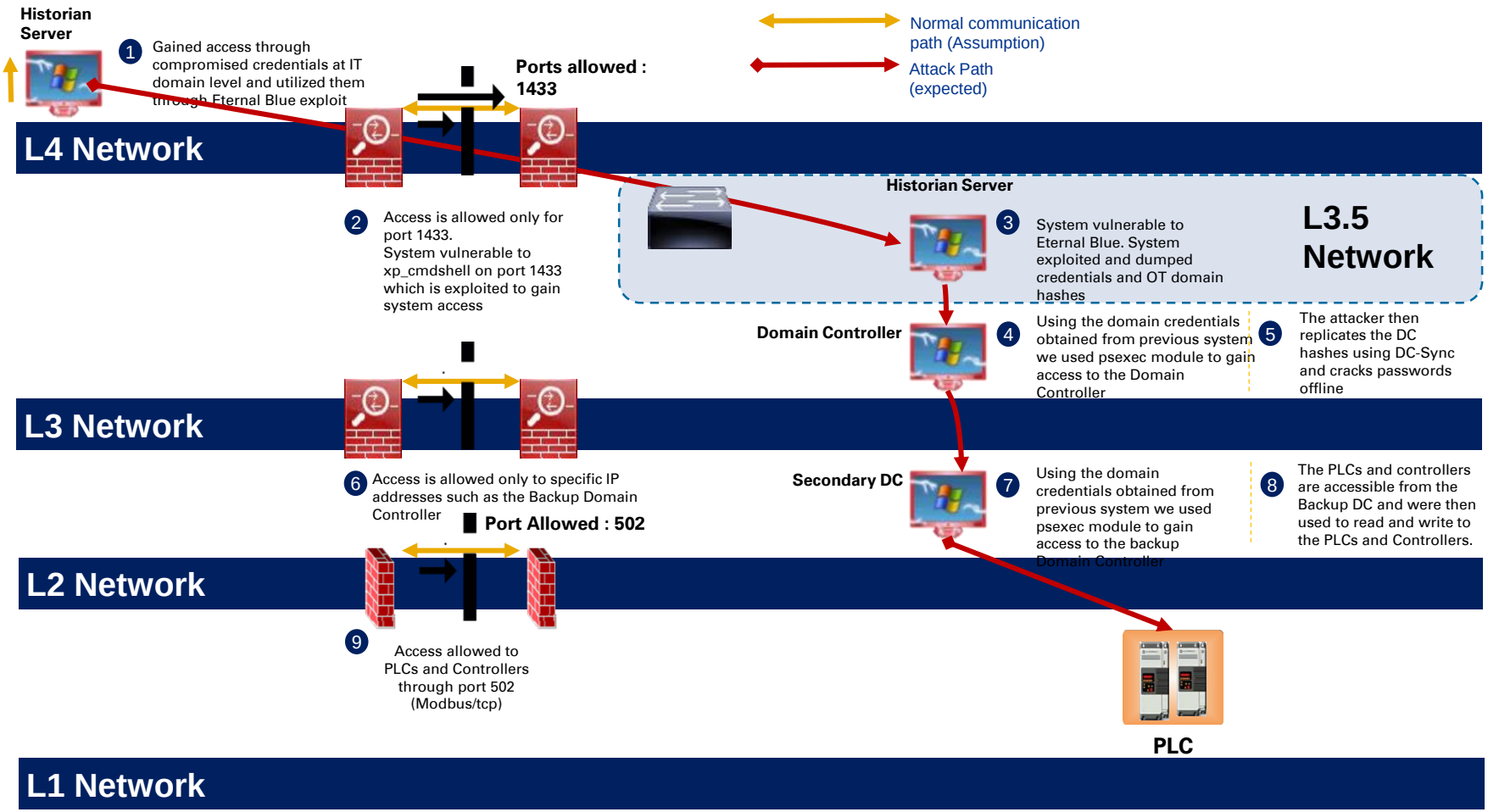
Open the pod bay doors | Brief explanation of the attack vectors



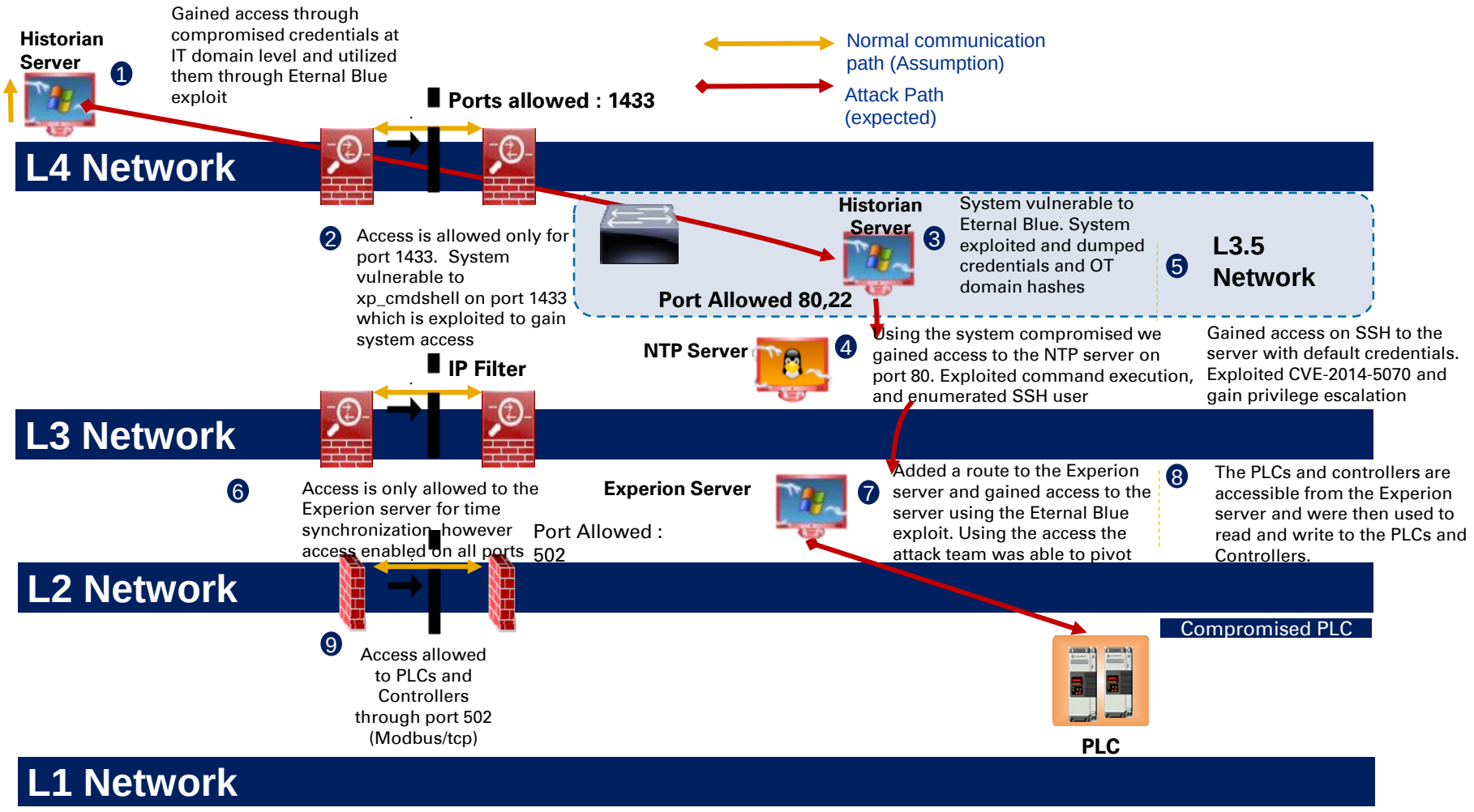
Reaching the heart of the system | Attack Path - 1



Reaching the heart of the system | Attack Path - 2



Reaching the heart of the system | Attack Path - 3



Destruction Ensues | Demonstration of what can happen

DEMO

Arms and Ammo

PLC Testing

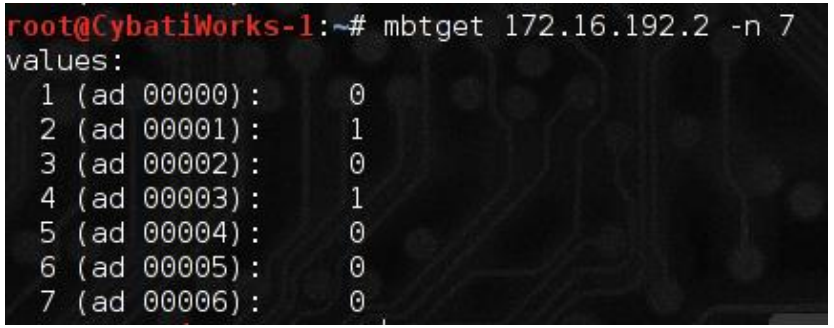
- **mbtget** - Simple perl script for make some modbus transaction from the command line
- **ControlThings** - Platform consisting of all tools required to test the OT / IoT environment
- **pymodbus**: Python library for Modbus protocol implementation using twisted for its asynchronous communications core
- **pyModbusTCP**: A simple Modbus/TCP client library for Python.
- **EXPLIoT**: Framework for IoT Hacking

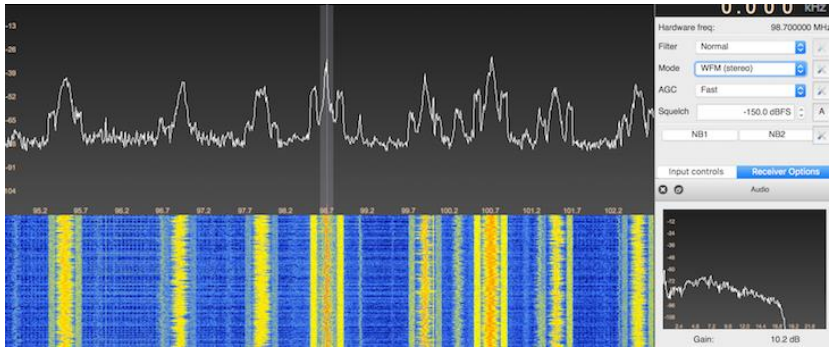
Wireless HART Testing

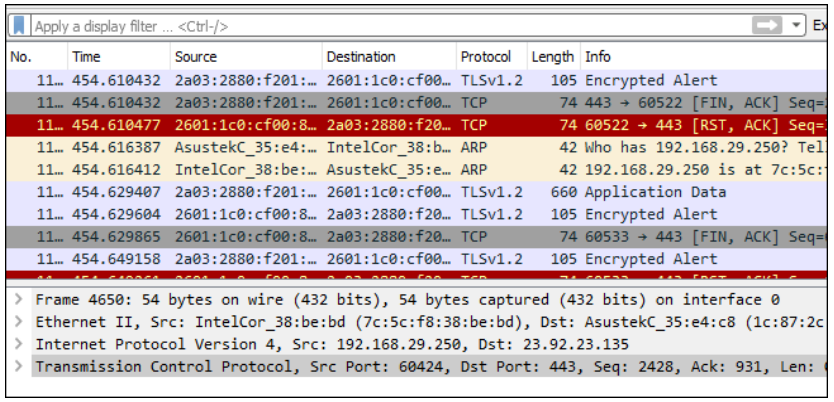
- **HackRF w/ GNURadio and gqrx:** Wireless HART communication interface
- **WirelessHART-Parser:** Analysis of the WirelessHART communications in the air
- **Wireshark**: You know why

OT Environment Testing

- Metasploit, nmap, JTR, aircrack-ng, Nessus, BurpSuite, Ettercap, sqlmap,



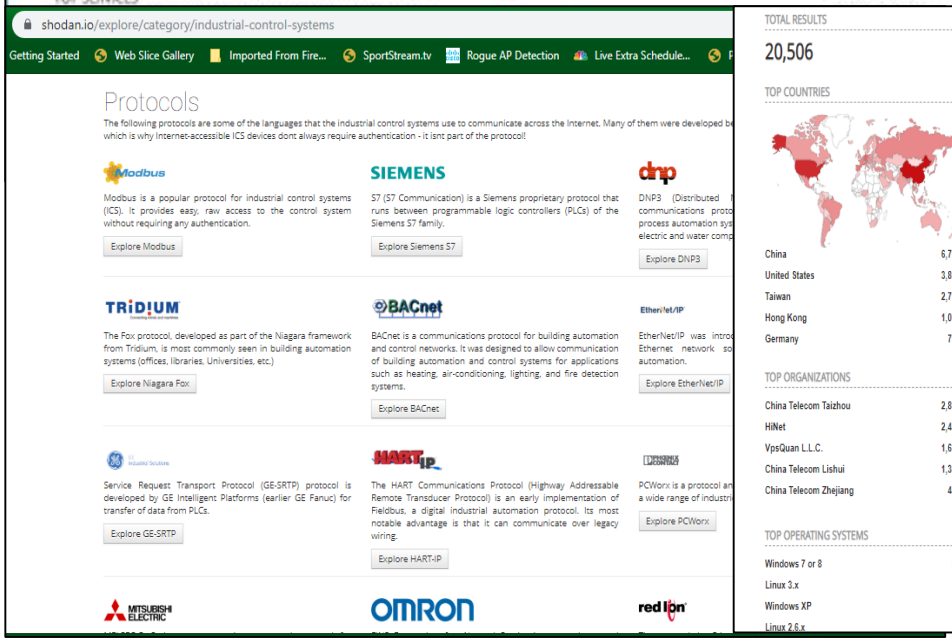




The World is your Playground | Critical Infrastructure on the Internet

Devices exposed on the internet and operate on Insecure Modbus TCP protocols

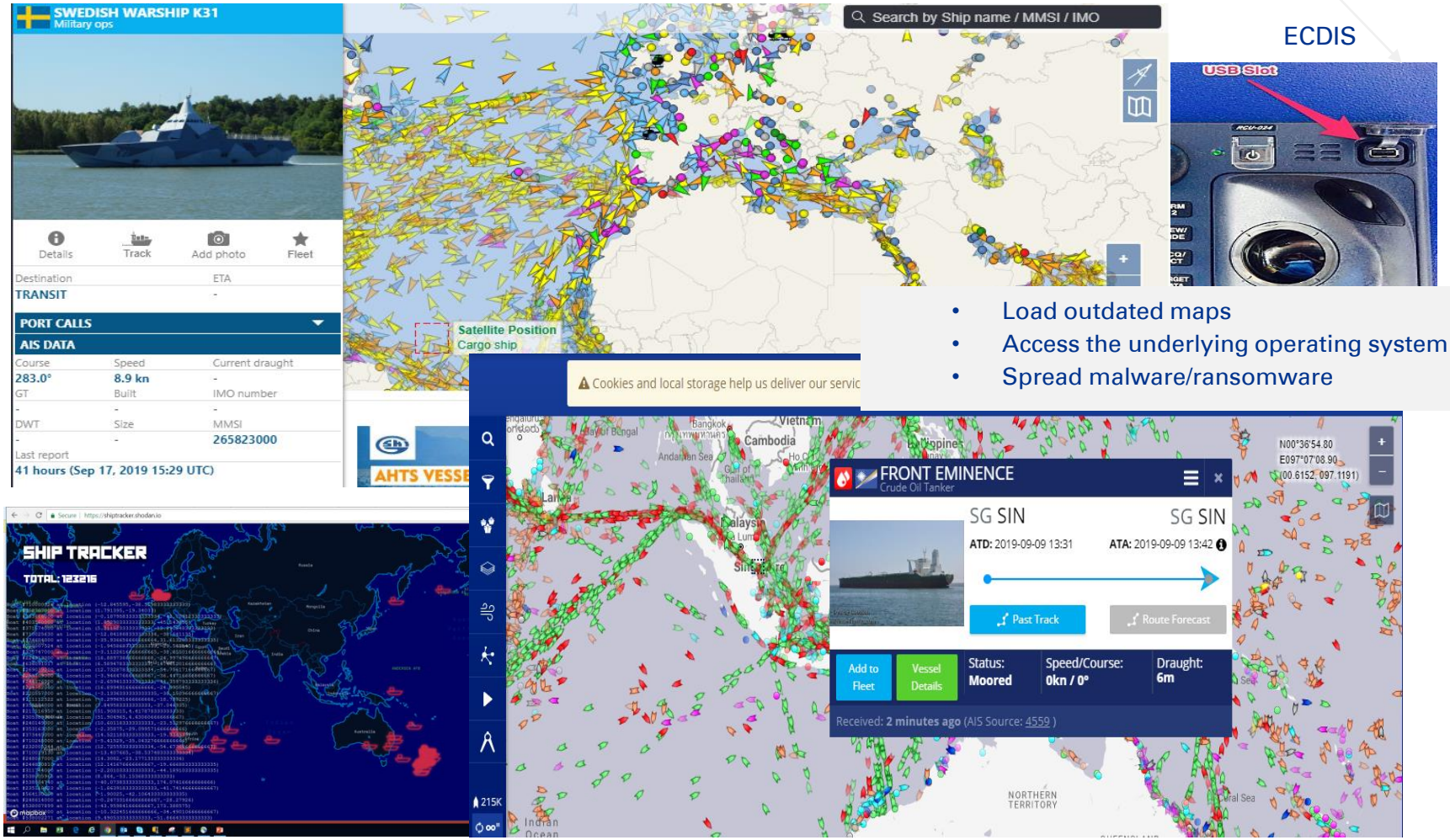
Devices on the internet on SIEMENS protocols



Explore by protocol / type

Maritime Security | AIS / ECDIS Information

Is this information you would want pirates or enemies to see?



- Load outdated maps
- Access the underlying operating system
- Spread malware/ransomware

Maritime Security | It is happening...

A "pre-warning", about what will happen in the future of shipping, with pirates using hacking to gain control and entry to vessels in order to carry out kidnap and ransom

Source: HIS Fairplay

Had to bring IT experts on board

The 10-hour attack was carried out by "pirates" who gained full control of the vessel's navigation system intending to steer it to an area where they could board and take over. The crew attempted to regain control of the navigation system but had to bring IT experts on board, who eventually managed to get them running again after hours of work

Suddenly the captain could not manoeuvre

In February 2017 hackers reportedly took control of the navigation systems of a German-owned 8,250 teu container vessel en route from Cyprus to Djibouti for 10 hours.

KPMG

Questions?

KPMG

Thank you