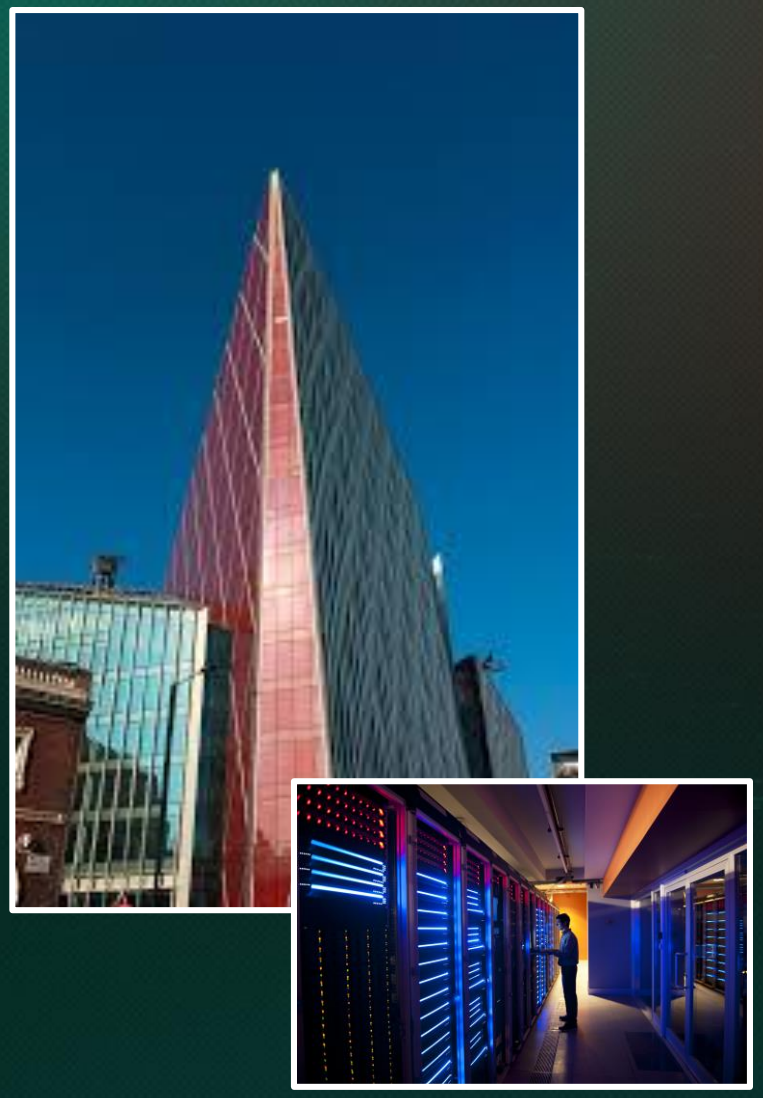
kaspersky

Designing Cyber Secured Building Management Systems (BMS)



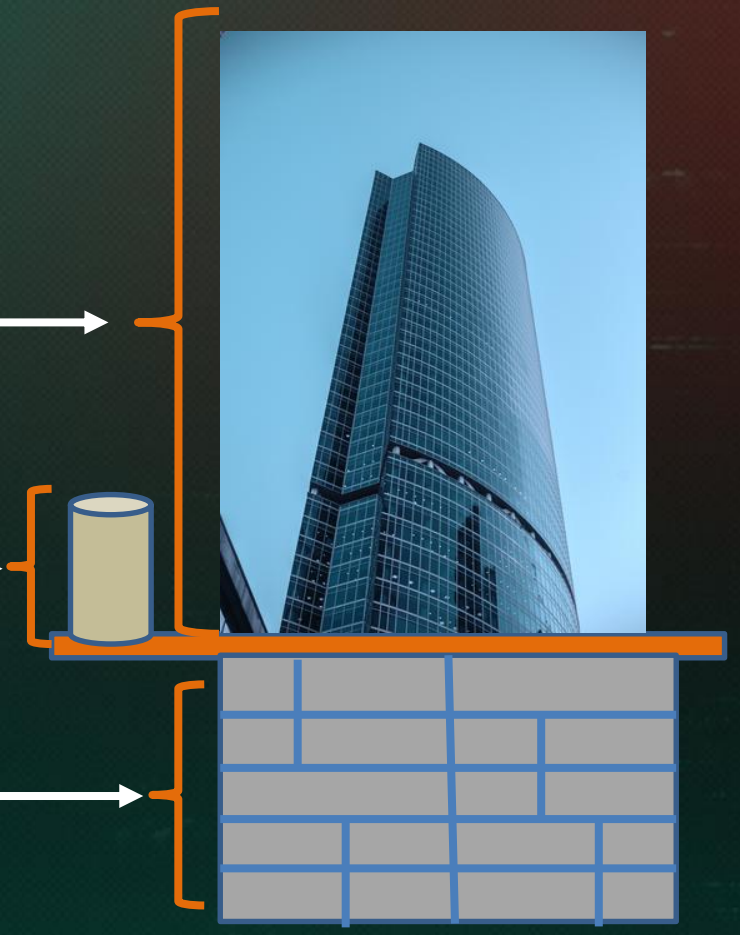
Author and Presenter:

Daniel Ehrenreich

SCCE – SCADA Security, Israel

BMS shall be separately secured

- **Above ground workspace**
  - Elevator, Smoke & fire, fire doors, access control, etc.
  - Security Cameras, HVAC, LV power, sensors, etc.
- **External installations**
  - MV feeders, Security CCTV, gates, sensors, etc.
  - Generator fuel, Emergency generator, lights, etc.
- **Underground utility facilities**
  - Cooling equip., Water & Sewage, Operator room, etc.
  - MV Generators, UPS, Computer Room AC (CRAC), etc.
  - Smoke & Fire alarms, Security CCTV, Fire doors, etc.



BMS incidents, attack vectors and impacts

- **Energy control related attacks**
  - Alter the power meter values
  - Modifying the light control
  - Resetting HVAC temp. & timing
- **Operation related attacks**
  - Power /HVAC outage in the building
  - Manipulating sewage control
  - Changing the biometric AC setting
- **IT related attacks**
  - Stealing data for a larger attack
- **Security & safety related attacks**
  - Activate smoke/fire alarms
  - CCTV turns blind or send fake pictures
  - Door and gate sensor's manipulation
  - Turning Off office and corridor lights
  - Turning fire doors to locked /opened
- **Service Damage**
  - CRAC system halt the DC operation
  - Office evacuation due to fake alarms
  - Phone, elevators not working

The BMS attack – who might do that?

- **Internally Generated Cyber Attacks**
  - Targeting underground utility equipment
    - Direct access to an embedded PLC or an IIoT device
  - Mistaken action by an authorized person
    - Good intention-poor / wrong execution (!)
- **Externally Generated Cyber attack**
  - Defined intention to attack a specific building
    - State initiated APT type action
  - Negligently designed architecture – poor zooning
    - Control Sections of the BMS exposed to internet (!)
    - Gradual compromising of safety barriers

Conducted by:
- Determined attacker
- Disgruntled employee
- Any person by intention
- Unintentional action

Conducted by:
- Determined attacker
- Disgruntled employee
- Hostile country Action
- Crime action

The BMS attack – how it can be done?

- **Supply Chain related attacks**
  - BMS Equipment and software originated
    - The malware is inserted in new or repaired PLCs/computers
    - Embedded PLCs in a machine supplied with malware
    - Purchase of a malvertized IT component
  - Service team originated
    - Service PC infected by negligent use (at home)
    - Intentionally infected computer
    - Download of an infected software version
  - Backdoors left connected “easy problem solving”
    - Good intention to deliver fast response (!)
    - Poor zoning among BMS sections (lateral move)

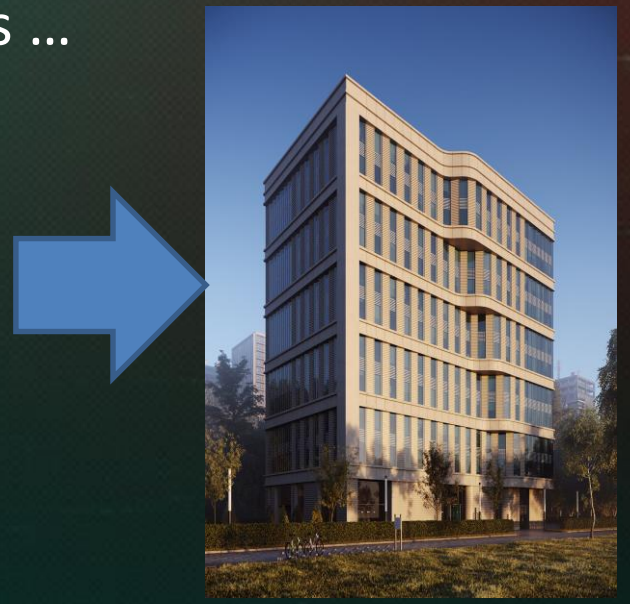
Conducted by:
- HR Service suppliers
- Vendors of HW and SW
- Servicemen unintentionally
- Intentional-planned attack

Structuring the cyber defense 1/2

- **Define the operation zones**
  - The DC, where critical information is stored
  - Underground zone where utility equipment resides
  - External utility equipment monitored by the BMS
  - Utility services: water, electric power, fuel, etc.
- **Define the building function by criticalities**
  - CRAC operation for the data centers
  - HVAC for offices and underground areas
  - Smoke and fire detection in all zones
  - Elevators, air-conditioning, site security, etc.

Structuring the cyber defense 2/2

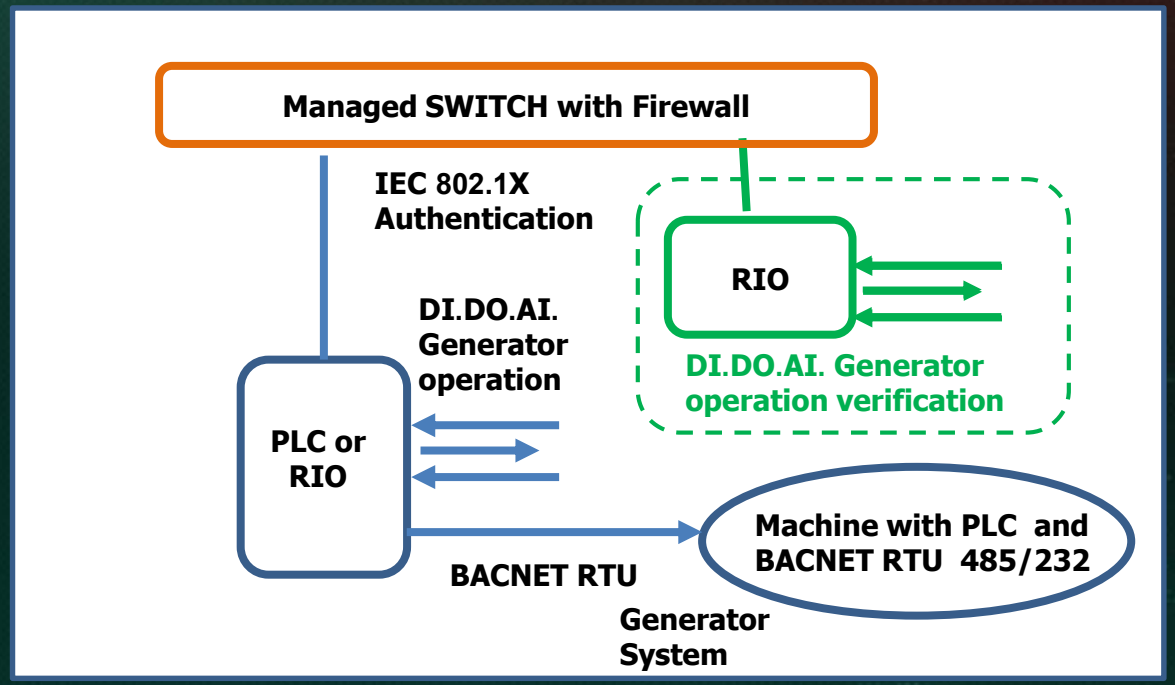
- **Conduct assessment (start with most critical zones)**
  - Attack-incentives of each group: Outage, Damage, Losses …
  - Attack vectors: External, Internal, Supply Chain
  - Impact and probability of occurrence for each vector
  - Effectiveness of already installed defense measures
- **Link the "probability of occurrence" to "impact"**
  - Link each attack vector to an estimated probability
  - Evaluate the worst-case impact for each vector and zone
  - Calculate the risks for each vector : R (risk)= P (probability) * I (impact)
  - Evaluate the applicable completing/compensating measures for each risk



Dual BMS Monitoring : Main & 2nd Verification

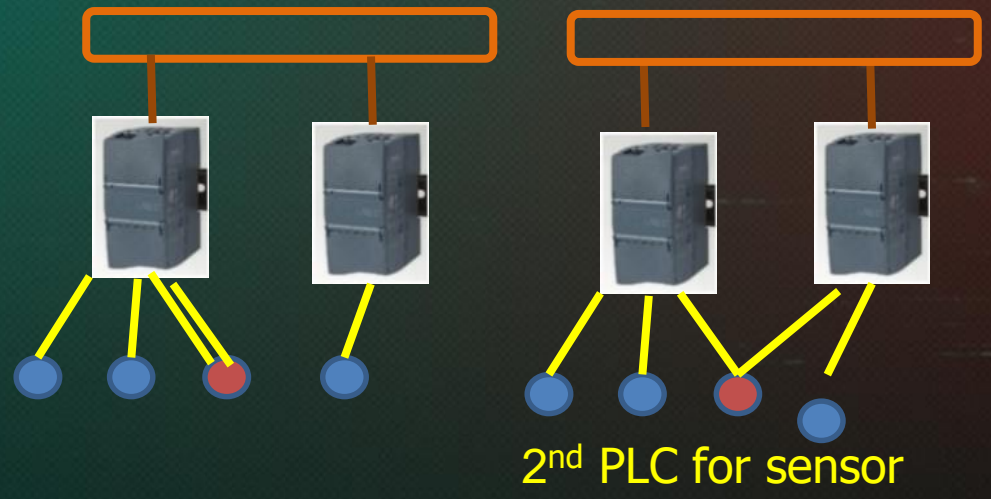
- **Role of the main monitoring**
  - Interfacing to embedded PLCs via Modbus or BACnet (serial port)
  - Monitoring parameters produced by the integrated equipment sensors
  - Interfacing to a PLC, via serial to TCP protocol conversions
- **Role of the 2nd verification**
  - Interfacing to a different set of Analog & Digital sensors
  - Monitored by a dedicated PLC – an integrated part of the Verification ICS

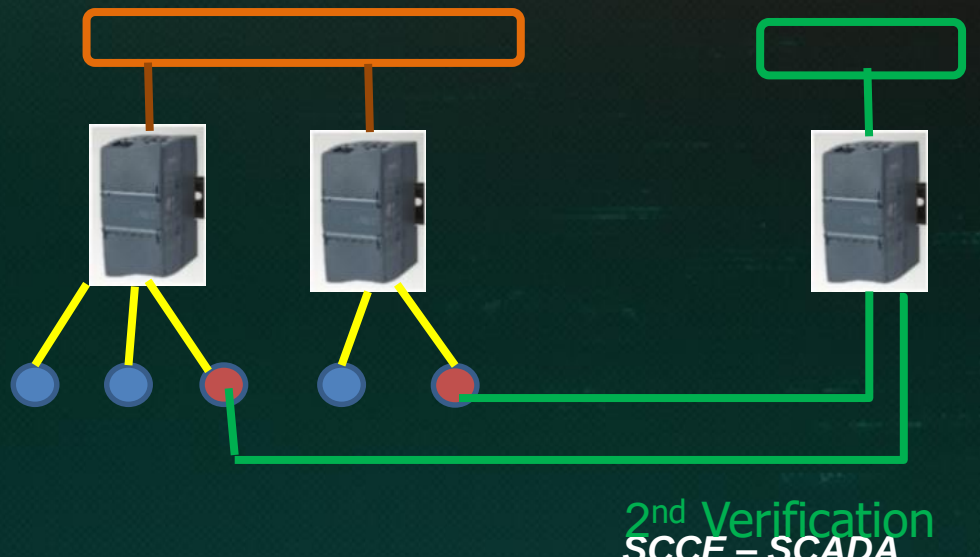
- **Use of separate Networks**
  - Main monitoring system
  - Verification Monitoring



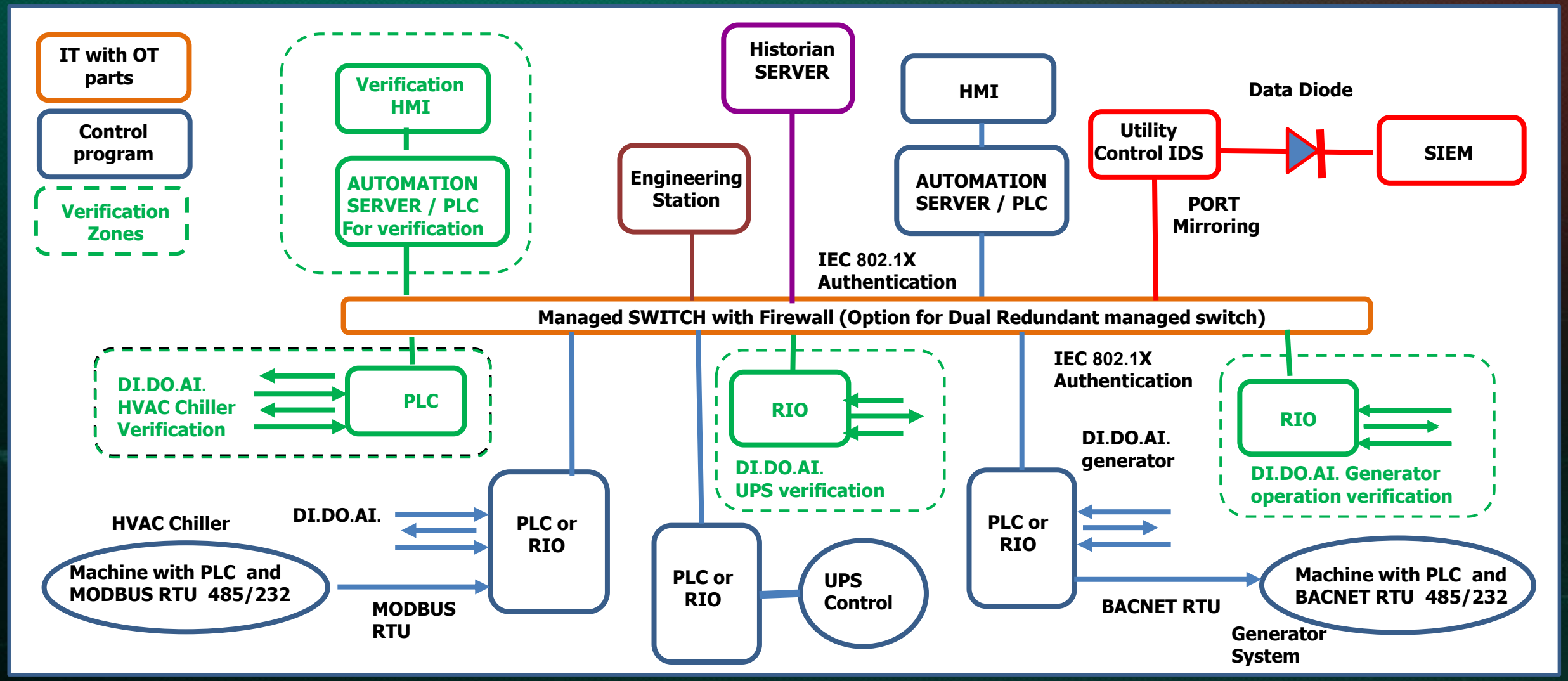
Structuring redundant architecture

- **Redundancy at the PLC level**
  - Monitoring a sensor via 2 separate ports
  - Monitoring the same sensor with 2 PLCs
  - Monitoring parallel (similar) sensor
  - Verification with different sensors
- **2nd Verification of measured values**
  - Deploy a separate ICS for verification
- **Redundancy at the Server level**
  - Dual Hot standby servers
  - Dual redundant managed switch





Cyber secured BMS operation



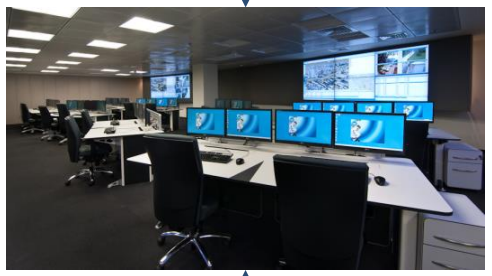
IT components for cyber secured BMS

BMS operators

Utility System Monitoring

Verification System Monitoring

Utility SIEM

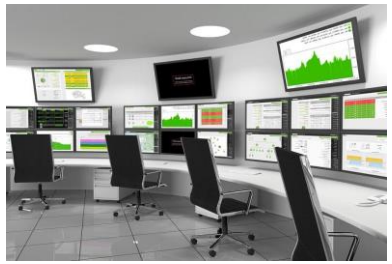


Underground Security System (cameras, doors, etc.

Underground Security Monitoring

Security SIEM

SOC for BMS, Utility System, Underground and Office level's Monitoring



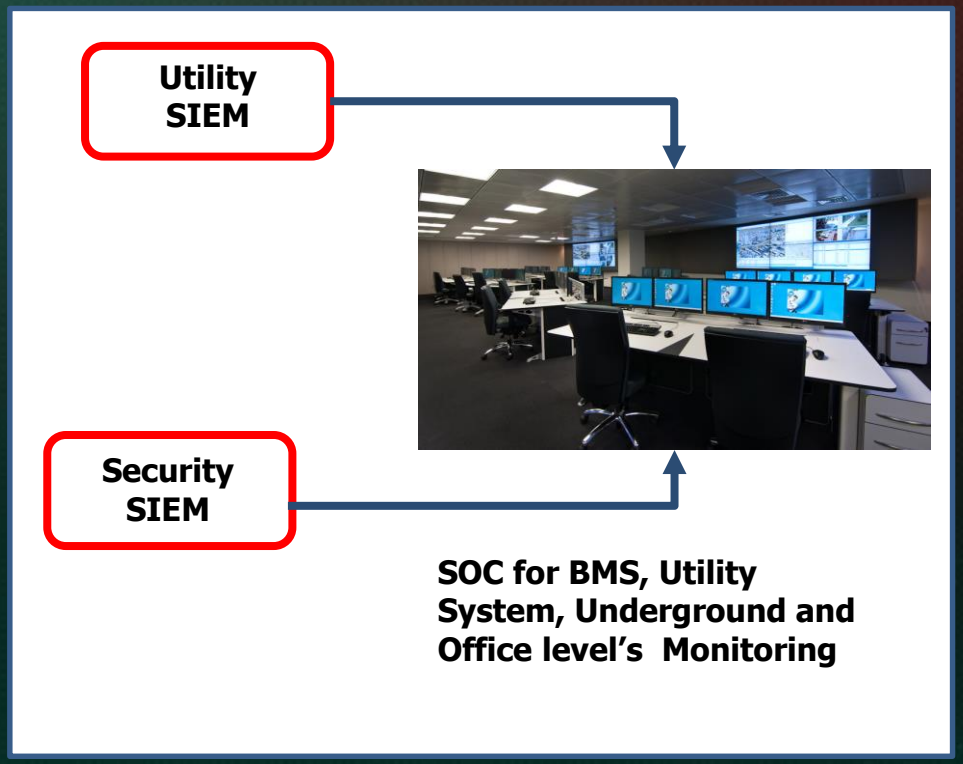
Office level Security System (cameras, doors, etc.

Upper floors Security Monitoring

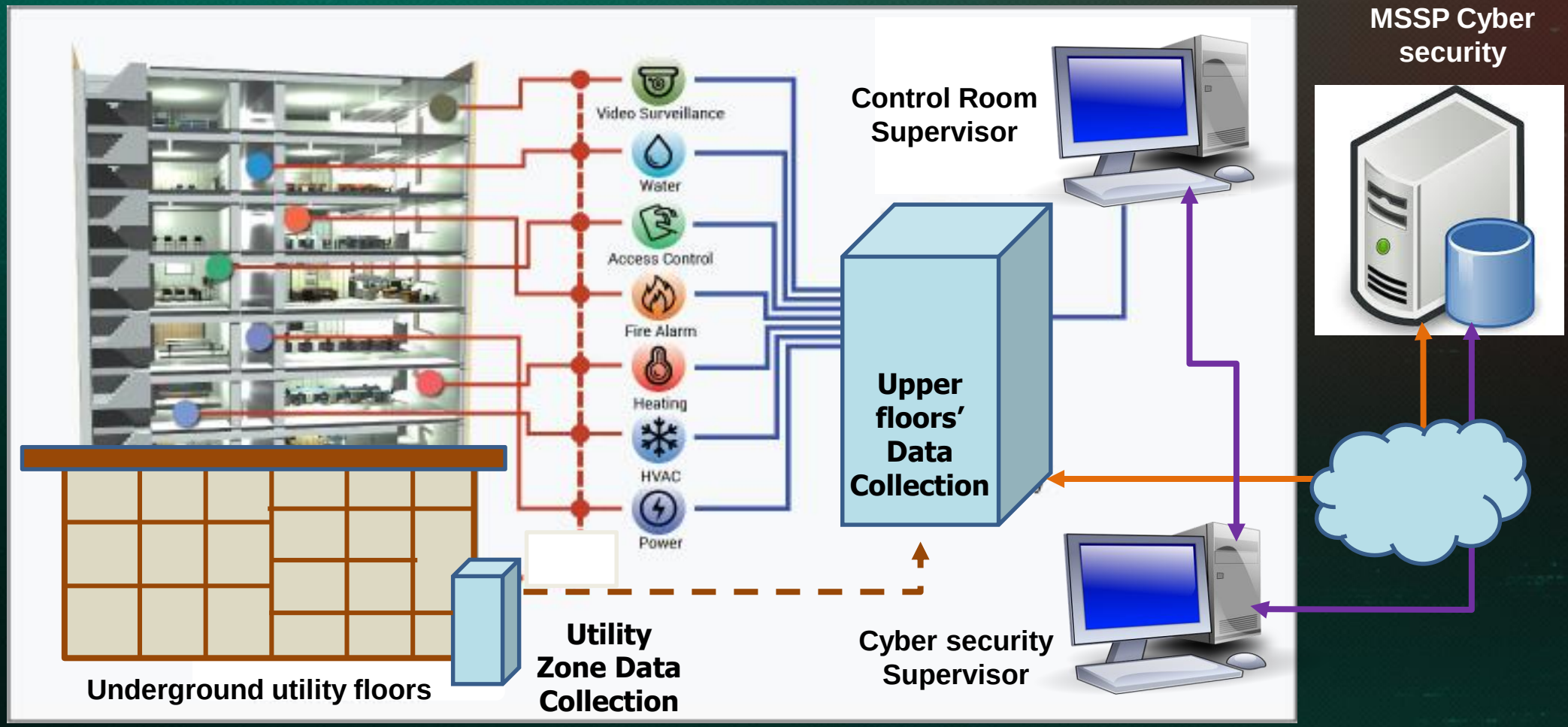
NAC and IT operators

Cyber security methodologies

- **BMS health analysis using SIEM collectors**
  - The collected data is constantly analyzed for flaws and anomalies
  - The SIEM output is forwarded to the SOC room for further analysis
- **BMS Integration with building security**
  - Information from CCTVs, door sensors, gates sensors in corridors, etc.
  - Smoke and fire detectors remain isolated and communicated via I/O ports
  - Operator initiated activation of fire-blocking doors from the security room



MSSP Cyber secured BMS Supervision



MSSP- Managed Security Service provider

RDC and PPT based BMS defense principles

- **People**
  - Train your team at all levels
  - Verify their technical knowledge
  - Conduct periodic drill
- **Policies**
  - Physical perimeter security
  - Use of credentials by people
  - Prevent 3rd party owned equipment
- **Technologies**
  - IDS data filtering & detection based on understanding of the process
- **Redundancy**
  - Fault not affecting business continuity
  - Critical items get special attention
  - Utility supplies 24-7-365 operation
  - Duplication of sensors and PLCs
- **Diversity**
  - Difference cyber defense measures
  - Attacker must learn several FW types.
- **Complexity**
  - PLCs perform protocol conversion and analyze the operation boundary

Reaching strongly secured BMS

Define the main goals into your BMS specifications

Deal with vendors who take cyber risks seriously

Do not compromise on cyber Security requirements

Always be ready for tomorrow's surprising challenges

Presented by:

Daniel Ehrenreich

Secure Communication and Control Experts

Daniel@scce.co.il