UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L14 Communication and Security in Current Industrial Automation

György Kálmán,
ITS@UiO
gyorgy.kalman@its.uio.no

Josef Noll
ITS@UiO
josef.noll@its.uio.no

http://IoTSec.no , #IoTSec, #IoTSecNO

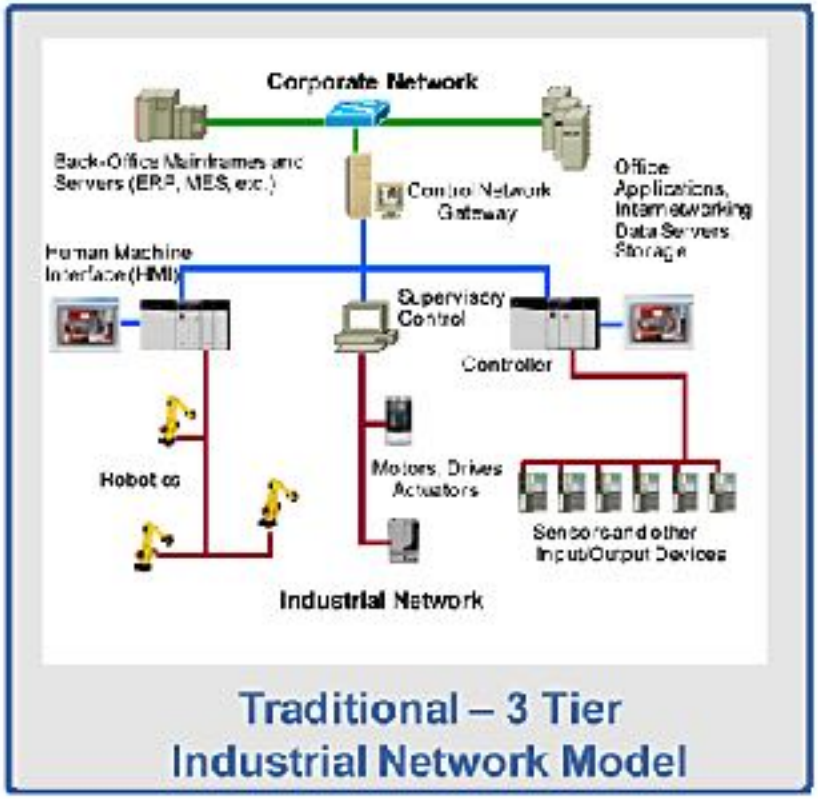
Agenda

- Connected systems – historical overview
- Current trends, concepts, pre and post Stuxnet
- Risks and threats in a connected automation system
- Security – logical (cyber) and physical security. Relation to Safety
- Network security (defense-in-depth, restrictions, remote access)
- Hardening best practice
- Common effort
- Connection to office solutions
  - Managed security
- Current example: smart grid
- Outlook: Internet of Things

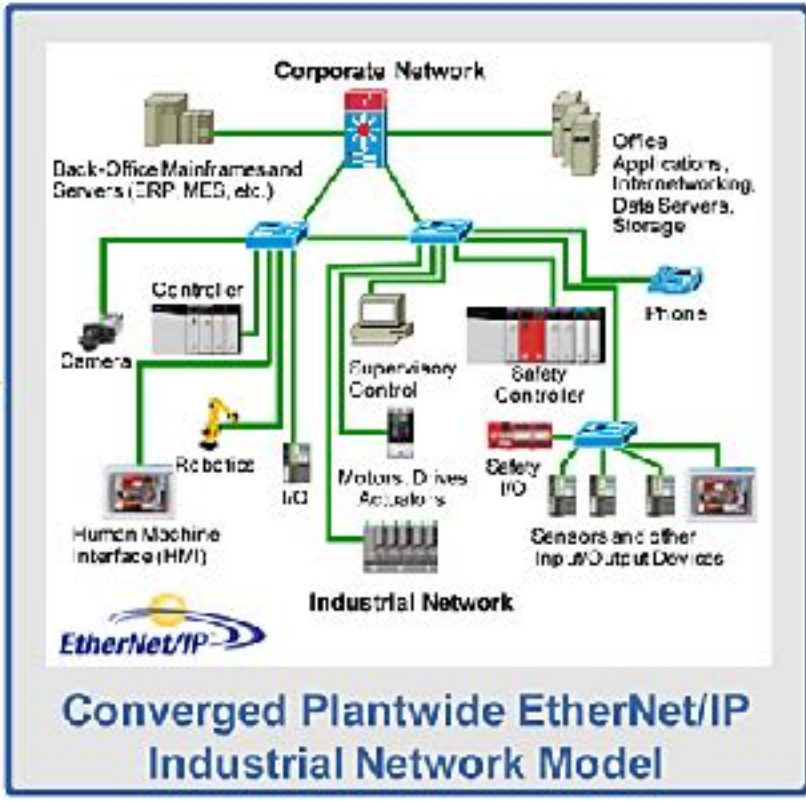
Connected Systems

- Components
  - PLCs, controllers
  - End nodes: Sensors, actuators, drives
  - Workstations
  - Servers
  - Infrastructure components: switches, routers, firewalls
- Evolution from serial lines to connected plant
- Information aggregation creates value!
  - Connection to ERP, customers, suppliers etc.
  - Metrics, scheduling, history, maintenance, quality assurance

Architecture Overview



Traditional – 3 Tier Industrial Network Model



Converged Plantwide EtherNet/IP Industrial Network Model

Risks and Threats in a Connected Automation System

- Safety as reactive protection, security as preventive protection.

- Physical: theft, disasters, unauthorized access, sabotage
- Logical: Denial of Service, Management, worms and viruses, sabotage, access control, unintended actions
- Safety, risk and consequences in industrial systems

- Safety: freedom from unacceptable risk. Safety systems work against natural processes, not against e.g. sabotage
- Pre- and Post-Stuxnet: fall of the myth of the air gap
- Stuxnet: targeted attack on Siemens equipment: invalid operation envelope, results in catasthrophic failure of the equipment. Disables alarms.
- Should address both cyber and physical threats and include interfaces to non-automation related parts of the system.
- Mobile or temporary nodes
- More than just access control and communication security:
  - Tamper resistance
  - Intellectual property protection
  - Data confidentiality

Security of a system

- A combination of network solution, software environment and applications used.

- Security is a process, not a one-time delivery
- Defense-in-depth: approach the full picture:
  - Device
  - Application
  - Computer
  - Network
  - Physical
  - Policies/Procedures/Management
- Restrictions
- Remote access

Managing risk in industrial deployments

- Main goal of (industrial) security is to reduce risk
- To reach this goal, it can cooperate with other industrial solutions: redundancy in installations or safety systems.
- React on security breaches – if possible, in cooperation with the automation equipment (safety)
- In this case, one can use also physical safety: burst disc, protective casing, automatic fire extinguisher, intrinsic safety, containment, plant or community emergency response etc.
- Common cause failures: interaction between safety and security
- Very similar tactics: separation, diversity, verification and validation

Physical security

- Limit access to authorized personnel
- Physical security:
  - door, wall, fence, lock, protective casing
  - security guard,
  - Includes protection of communication channels (e.g.: cabling, but also USB ports).
- Procurement
- Destruction of used equipment

Network security

- Not a long history in industrial automation
- Most devices have no features for communication security
- Adaptation of office solutions to the industrial environment
  - Traffic composition -> mostly L2, some L3
  - Cost and openness
- Interesting connection point between the industrial applications and financial operations: data integrity, QoS and protection of devices.
- Problematic to have IDS/IPS down to control/field level
- Configuration and protection of ports (including physical)

Hardening Best Practice

- Policies
  - Typical accept-all to allow coexistence, secured with configuring for the actual system -> hard to create a standard setup (will show a bit later, why this is not completely true)
- Access for third parties

- Computer management:
  - Patching
  - Antivirus: all suitable computers shall be scanned regularly. It is a question how to implement without impact to performance.
  - Policy for usage and software installation
  - Configuration of intefaces, physical security
- Access and Account management
- Backup
- Topology

Hardening Best Practice

- Security policy: standards compliance (IEC 62443, ISO 27000)
- Patch management and AV (centralized AV solution, own update server for patch mangagement)
- Default settings and hardening (OS setup, firewall, user settings, ports, intefaces, mobile storage)
- Access and account management (RBAC, password policy)
- Backup and recovery (disaster recovery strategy, also test)
- Plant network topology (security zones)
- Secure remote access
- Security monitoring and diagnostics (IDS/IPS, network management)
- Hardware and software inventory
- Application whitelisting
- Validation: scan with e.g. Nmap, Tenable Nessus

Communication setup

- Separate industrial network from office network
- (Mutually) don't trust third partner connections
- If needed, secure the communication path as far down towards the controller as possible. Typical for SCADA applications: VPN is only terminated inside the remote station or even only at the controller (depending on type).
- Use network zones: create DMZ for data exchange, deny-all default policy for firewalls
- Use security functions in protocols where available
- Security shall not compromise network QoS
- Use secure protocols for network management
- Office-features are being introduced also in the automation domain: incldung smart switches, network management systems, patch management, traffic monitoring
- Development direction: cut engineering costs: automatic configuration, mass configuration, use of templates

Access Control Lists

- Access Control Lists (ACLs) are commonly used for configuration of network equipment: the lists lead to easier and more consistent setup of devices.
- Can be applied on network equipment, servers and other nodes, which will all follow the (same) rules defined by the list.
- Key setting: if something is not defined in the ACL, then it will be denied.

Firewalls

- Office solutions are not directly applicable: different traffic requirements and traffic composition
- Stateful packet inspection: fast and can be effective in an industrial environment, sometimes the only automatic solution which can meet delay/latency/jitter requirements
- For larger installations: follow the same standard policy for all remote stations and use the same rule set as much as possible
- Allow communication directly between zones only if required.
- Set up security zones – implement defense-in-depth (IEC 62443)
- Users shall not be able to access services, which are not necessary for the operation. Access to these can be granted through a less secure network.

Virtual Private Networks

- Historically most of the automation protocols ran on L2 (still today, mostly in the control and field networks)
- If one needed a shared setup, where e.g. the controller was in a different location than the actuators and sensors, the non-routeable protocols were a problem (earlier with leased lines this was not an imminent problem)
- VPN is a solution for an L2 protocol to be carried over an L3 network transparently
- On the other side, it can also provide integrity and confidentiality
- Cost press leads to use shared networks to convey information from automation sites: VPN is today a necessity.

Network Segmentation

- Segmentation of networks is by default required by the automation products (sometimes «weird» behavior and sensitivity)
- Separation of network traffic and shared infrastructure
- Routers and firewalls (including controllers) shall be configured with being aware, that L2 segmentation is not separating L3 traffic.
- Bad practice: but sometimes required because of configuration cloning:
  - Two electric substations having exactly the same L2/IP/server setup, only being different in the physical location, but connected to the same higher network
- Use VLANs for segregation of traffic and easier network management
- use IEEE 802.1X on the edge ports.
- No direct communication between the office and the automation network -> DMZ between office and industrial.

Computers

- Centralize management

- AV where required and possible
- Remove unnecessary file shares, services
- Disable physical interfaces not in use
- Firewall, where QoS requirements allow. Deny all as default.
- Role Based Access Control recommended

- System management: central patching, no unauthorized software deployment, limit or disable the use of removable storage

Controllers

- Adequate protection of communication: integrity, confidentialy on demand, change management, access control
- Availability is more important than confidentiality
- Physical security: protect interfaces and access to the actual device (local inteface always available, at least a DoS attack is possible

- Always change default username and password
- Protect the program, if possible enable firmware fingerprint checking
- Disable all unused features (including services and ports)
- Protect agains unintentional threats
- The controller acts as a router/gateway between the control and field networks, configure accordingly

Common Effort

- Best practice
  - ABB
  - Rockwell
  - Siemens
- Standardization
  - IEEE 1588 v3
  - IEC 61850
  - IEC 62443 (ISA-99) Industrial Automation and Control Systems Security
  - NIST 800-82 Industrial Control System Security
- ICS-CERT
- KraftCERT
- Laws protecting the infrastructure and requiring actors to exchange security incident information

Comparison to office environments

- An automation system has a connection to the physical world.
- Loss of information or other QoS violation might lead to physical consequences
- Security focus is more spread: central elements like servers, controllers and sensors/actuators

- Availability: 4-5 sigma. Much less is expected in office.
- QoS: much more strict in automation, only finance has similar, jitter is especially critical
- Typical communication: person to person vs machine to machine
- Reaction to problems: wait/reboot/call -> minute-hour range in office compared to instant failover redundancy, fail-safe or fail-operational paradigm, repair in operation.
- More deterministic communication can make some office solutions more effective

Reactive security: Managed Security Services, continous vulnerability analysis

Smart Grid example

- The power grid is a typical example for a SCADA operation
- Continentwide critical infrastructure
- Smart grid is expanding this infrastructure
- Smart meters introduce a device located in the home network, but also connected to the grid control
  - Physical security
  - Tampering
  - Secure communication channel
  - Maintenance
- Unusual attack vectors with one interface in the home, one at the utility
- Time synchronization is a challenge: heterogenous networks, problematic timing measurement in multihop wireless.

  Balance between reliability and security, ABB White Paper

Internet of Things

- Still automation: M2M, QoS, predictable behavior, restricted resources
- Managed security and active defence solutions from office
- New market possibility for 5G mobile
- It is already here with consumer electronics
- Coming in SCADA, transportation, process control and healthcare
- SDN

- Literature: IoT overview, Ericsson, Accenture

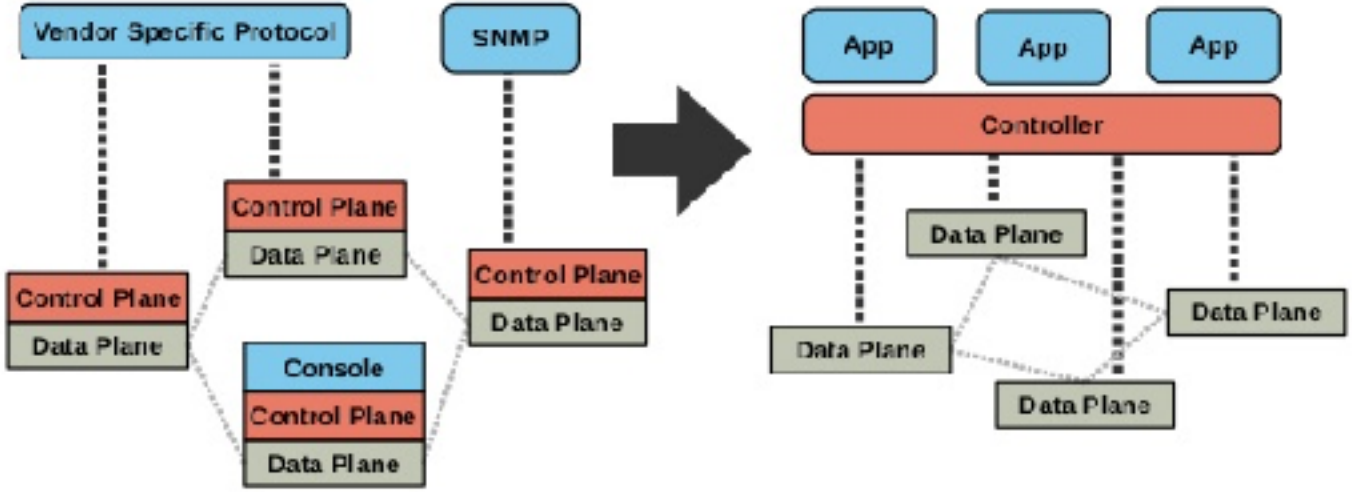
Applicability of SDN to industrial automation

- Cost press and manual configuration
- Network Management System is typically not used
- Examining the possibility to use SDN
  - Single point of failure -> safety
  - Reaction on security issues
  - Mass configuration, as-built analysis, network management
  - Provides utilization information
  - Direct influence on forwarding

Security engineering with SDN

- Exploit the static traffic composition
- Control of the forwarding plane
- Direct QoS evaluation
- Enforcement of policies
- Reuse of previous rulesets
- Documentation generation

- Figure from RedHat



Conclusion

- Focus on the task to be fulfilled
- Drop-all / whitelisting approach
- Segmentation
- Mutually not trusting eachother
- Validation

- Future: reactive security, traffic monitoring, MSS