UiO Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L11 - Communication in Smart Grid, Smart Home and IoT

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

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

https://its-wiki.no/wiki/TEK5530

TEK5530: Lecture plan

- **21.01**
  - L1: Introduction (Josef Noll)
  - L2: Internet of Things (Josef Noll)
- 28.01 (Gyorgy Kalman)
  - L3: Security of IoT + Paper list
  - L4: Smart Grid, Automatic Meter Readings
- 04.02 (Josef Noll)
  - L5: Practical implementation of ontologies
  - L6: Multi-Metrics Method for measurable Security
- 11.02 (Josef Noll)
  - L7: Multi-metrics
  - L8: System Security and Privacy Analysis
- 18.02 (Josef Noll, Gyorgy Kalman)
  - L9: Paper analysis with 25 min presentation
  - L10: Security Controls
- **25.02 (Gyorgy Kalman)**
  - **L11: Communication in Smart grid, home and IoT**
  - **L12: Intrusion Detection Systems**
- 04.03 (Gyorgy Kalman)
  - L13: Cloud Basics
  - L14: Cloud security and IoT
- 11.03
  - L17: Selected recent topics from IoT security
  - L18: Wrap-up of the course
- 25.03
  - Exam? or after Easter

Overview

- Threat Modeling
  - A practical example using the Microsoft Threat Modeling tool
- Communication challenges in grid, automation and home
- Hardening best practice

Threat modeling

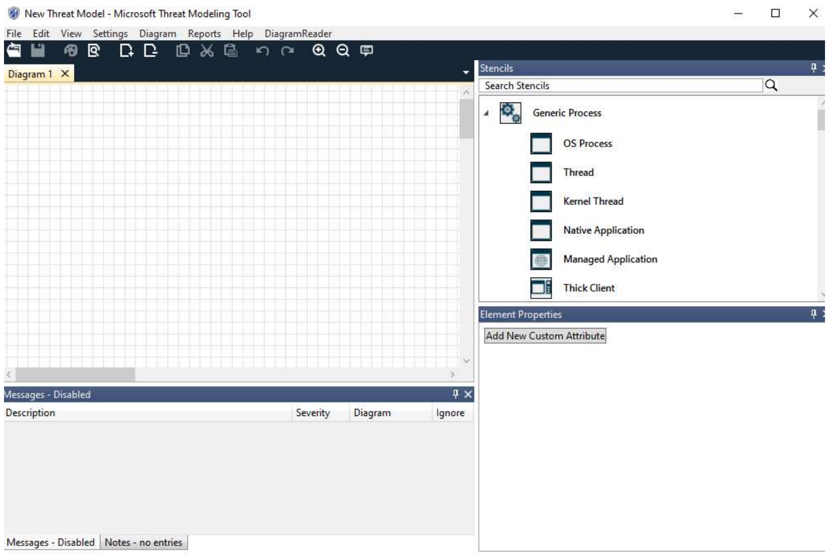
- An exercise helping to get an overview of the threats early
- Earlier detection means reduced costs for reducing the threat
- Microsoft released a free tool: Microsoft Threat Modeling Tool
- Follows MS' STRIDE:
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of Service
  - Elevation of privileges

- https://owasp.org/www-community/Application_Threat_Modeling
- https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Microsoft Threat Modeling Tool

- Provides basic stencil set for creating dataflow diagrams
- Wide range of additional stencils and support material
- Free, but requires some Microsoft presence
- Single-user tool (no collaborative function)

- Builds on iterative refinement of the diagrams and the data flow



Demo

Threat modeling conclusion

- Helps to catch some threats early on
- Design support to avoid unnecessary threats
- Supports the process-nature of security
- Allows custom extensions to cover specific needs

Communication in Grids and other networks

- Quality of Service: transmission and other parameters
- Communication metrics: bandwidth, delay, jitter, burstiness, redundancy
- Automation metrics: sampling frequency, delay, jitter, redundancy
- LAN-WAN-Sensor network comparison
- Time synchronization
- Security focus on integrity and authenticity
- Availability

The problem of QoS

- Evolution of communication networks
- Best effort is the most efficient and is dominating in virtually all segments
- Typical communication with at least one human party tolerates very much
- Works quite well.

- Automation: has requirements because of the physical connection
- Many requirements are only heritage from old times
- Are very much ”nothing” for an acceptably modern GE network

- QoS for the control loop
- QoS over the internet

QoS in communication

- Long tradition with high QoS neworks (SDH, PDH, traditional circuit switching)
- ATM has failed because of excessive cost
- Carrier Ethernet is the current choice of technology
- Overprovisioning works
- Diffserv-intserv
- In a multi-provider path, it is problematic to quarantee QoS
- Technologies are available, like MPLS – industrial problems are either related to cost or inability to identify requirements (and have higher cost because of that)

- Current status: we are trying to implement services, which made ATM expensive and fail, maybe this time it will be OK
- IEEE 802.1 TSN
- Typical metrics: bandwidth, delay, jitter, burstiness, redundancy

QoS in industry and IoT

- Connectivity
  - Direct wiring
  - Low speed serial buses
  - Ethernet
- Key in the local automation network
- Very fast reaction times
  - Substation automation
- Fast reaction times
  - Factory automation
- Slow reaction times
  - Process automation
- Upper levels are more a telco question
- Ethernet is everywhere
- Typical metrics: sampling frequency, delay, jitter, redundancy
- Time synchronization

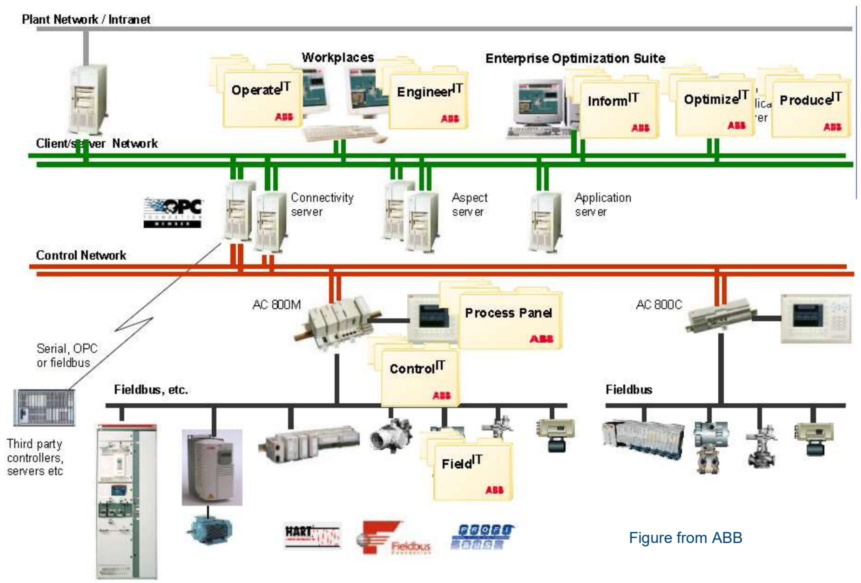
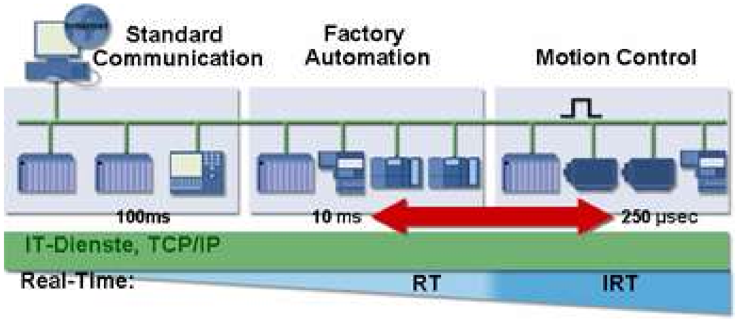


Figure from ABB

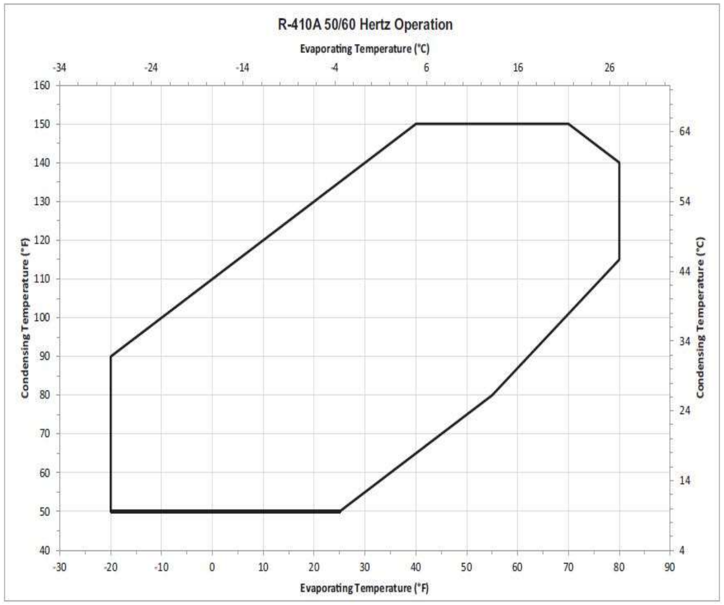
Intrinsic QoS

- Taking the most problematic part of the automation QoS
  - E.g. Profinet IRT or EtherCAT
- Relaxed QoS
  - Supervisory Control and Data Aquisition
  - Remote management
- High QoS
  - Electric grid
  - Electrified production platforms



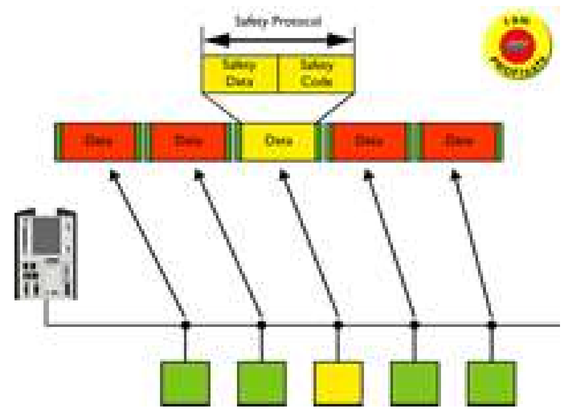
Conversion and operating envelope

- Operating envelope: the operational parameters where our network can work “well”, depends on the technology and on the task
- For traffic estimation we need it in ”communication” QoS
  - Bandwidth, delay, jitter, (redundancy)
- Often can be done with simple arithmetic with a certain confidence level



Safety integrated systems

- Imagine as yellow envelopes mixed into the traffic
- Requires software and might require hardware extensions
- The safety function is not depending on QoS!
- Safety levels: SIL 2, 3 and 4
- Until approx. SIL 3, a normal, RSTP-redundant LAN is sufficient



Safety and security

- Connected because security threats are resulting in safety threats, which have to be mitigated
- Different fields but approaching similar problems
- The process behind is completely different: safety deals with a static statistical process, while security problems are the result of an active, changing process

- Stopping somebody to do something to avoid damage
- Even if something has happened, avoid or limit damage

- Cyber-physical interactions
- IT security is not covering this field
- Safety is focusing on the physical interactions
- Safety is using extensive diagnostics to check itself
- Timescale of protection and data validity

Integrity – Authenticity – (Confidentiality)

- Endpoint security in control systems
- Identifying security risks in automation networks
- Countermeasures:
  - IDS/IPS
  - Firewall
  - Automatic updates
  - Application black/whitelisting
  - Backup
- Integrity
  - Safety is not protecting from sabotage
  - In general, no sabotage protection
- Availability
  - Alarms

Availability

- Main objective of Control System security:
  To maintain the integrity of its production process and the availability of its components
- Maps to:
  - Network redundancy
  - Software and hardware requirements
  - Device redundancy

Examples

- IEC 61850 in smart grid scenario
- AMS consists of reader (AMR), aggregator, communications, storage, user access
- AMR consists of power monitor, processing unit, communication unit
- AMR communication contains of a baseband processing, antenna, wireless link

- Requirements traceability
- Relevance for the whole communication path

Applications	Source IED	IEC 61850 Message Type	SCN Traffic Type	Destination IED	Sampling Frequency (Hz)	Packet Size (Bytes)
Sampled value data	MU IED	4	Raw data message	Protection IEDs	4800 Hz	126
Protection	Protection IED	1, 1A	GOOSE trip signal	CB_IEDs	–	50
Controls		3	Control signals	Protection IED, CB_IED	10 Hz	200
File transfer		5	Background traffic	Station server	1 Hz	300 KB
Status updates	Protection IED CB_IED	2	Status signals	Station server	20 Hz	200
Interlocks	Protection IED	1, 1A	GOOSE signal	CB_IEDs	–	200

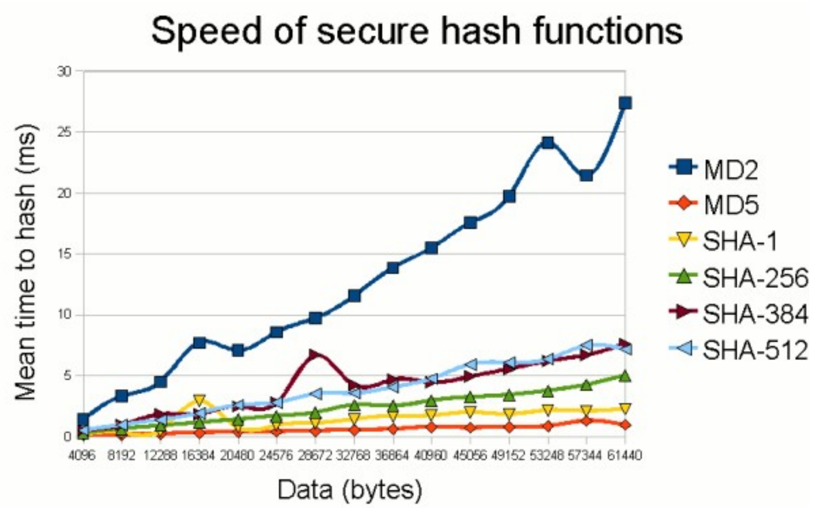
http://www.tandfonline.com/doi/pdf/10.1080/23317000.2015.1043475

Identifying QoS metrics for security

- Risk analysis to identify attack surface
- Integrity – Authenticity – Confidentiality
- Data validity and reaction possibilities
- Physical security
- Whole communication path should be evaluated

Selecting technologies

- Select by mapping requirements to technology properties:
  - Hash: integrity requirement, stream speed, latency, size
  - Cipher: security requirement (includes already data validity and generic risk evaluation), delay, size – optimized ciper suites are available

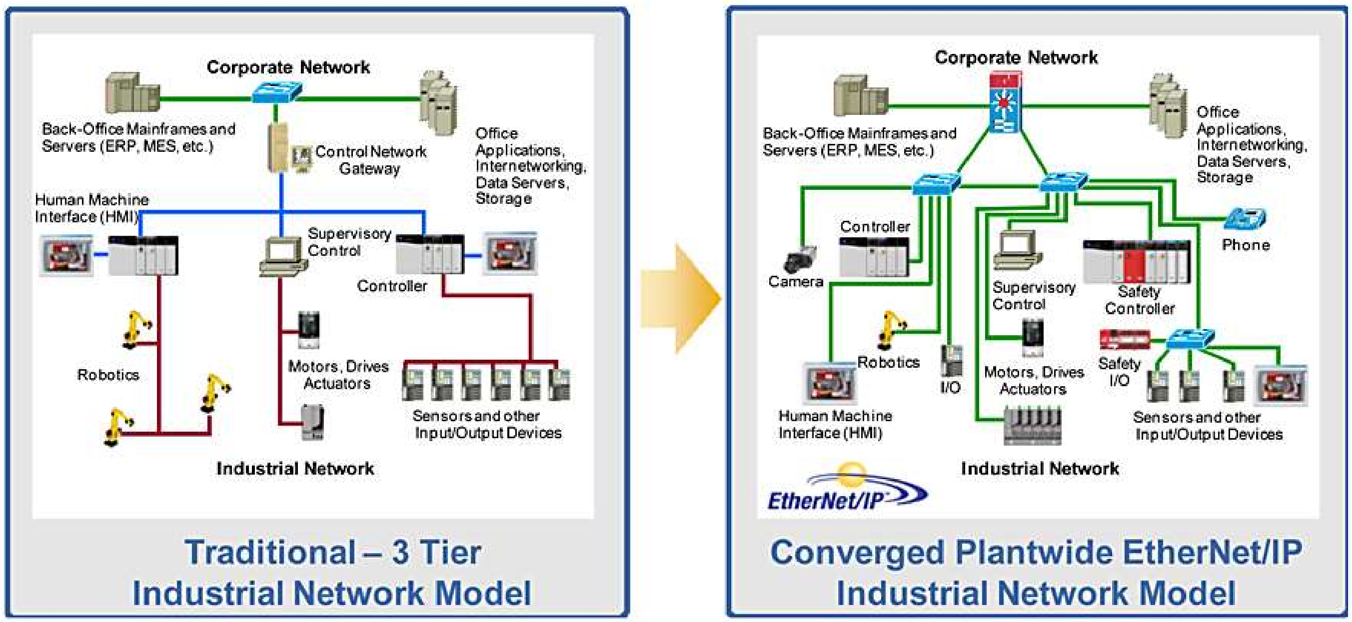


http://www.javamex.com/tutorials/cryptography/hash_functions_algorithms.shtml

Hardening, historical overview

- 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



http://www.rockwellautomation.com/resources/images/rockwellautomation/industries_applications_solutions/ethernet_ip/INM_Graphic--custom.jpg

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 - reduce frequency and consequence

- 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 topics

- 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

Securing the communication path

- Separate industrial network from other networks
- (Mutually) don’t trust third partner connections
- If needed, secure the communication path as far down towards the process 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: including 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.

Remove or disable unnecessary components

- 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

Securing controllers/automation devices

- 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

Security and privacy in the smart grid

- 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

L11 Conclusions

- Threat modeling to save costs in software development
- Quality of Service parameters and technology choice
- Hardening practice