New Challenges in IoT Security – How Does SAP Address Them?

Jay Thoden van Velzen, SAP
July 11-12, 2017

SAP Run Simple

Introduction

Industrial vs. consumer Internet of Things (IoT)

- Security of consumer IoT (as media can easily confirm) has been atrocious.
- It has likely set back industrial IoT adoption by several years.
- Industrial environments tend to be more controlled, and have stakeholders to whom security is important.
- Consumer IoT is largely trivial.
- The promise of IoT value is largely in the industrial space.

Machine-to-machine (M2M) communication

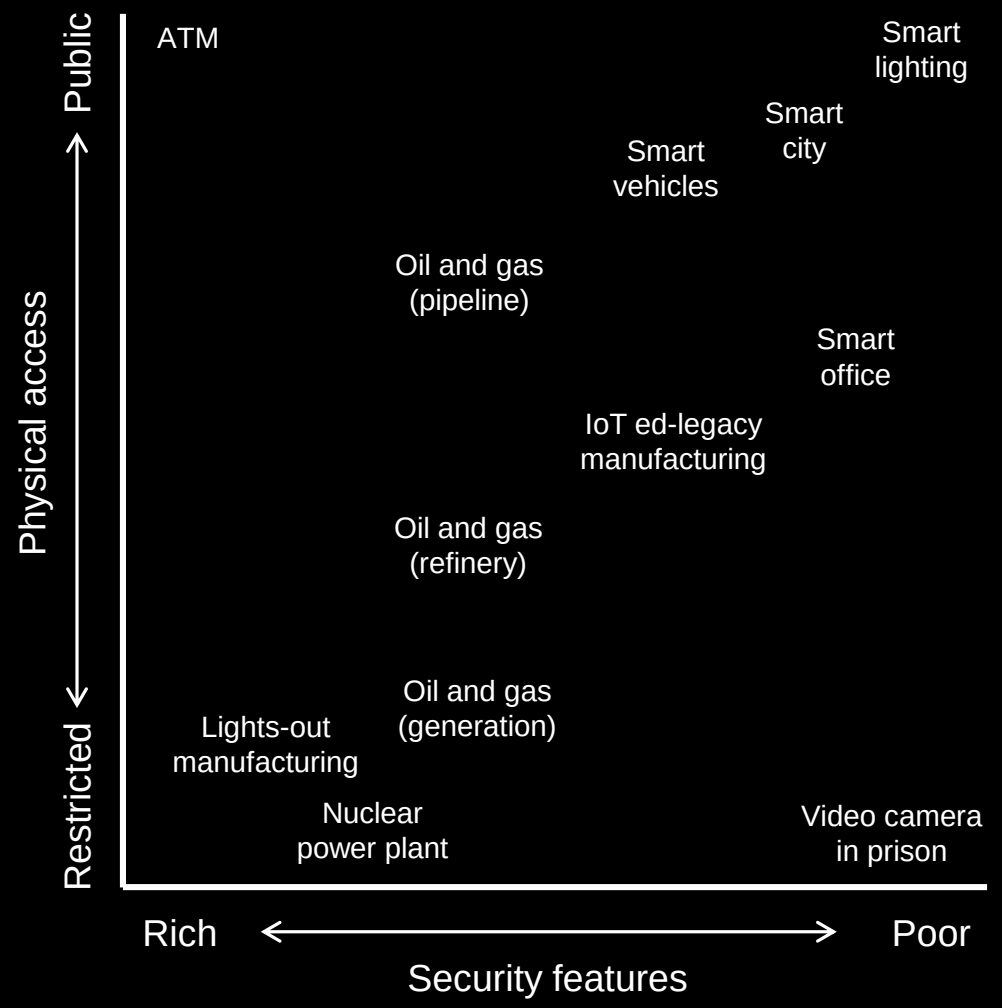
- Luckily, much of M2M communication is highly predictable.
  – Timestamp, device ID, reading
- End points and services are known in advance.
- Location is known in advance.
- Many devices are based on 32-bit Linux hosts, which come with standard security features we already know.
- 30+ years of IT security expertise
- Whitelisting

Heterogeneous environments

- In practice, though, landscapes tend to be highly varied.
- Microcontrollers < 32-bit
- OT networks: ICS, SCADA
- Cellular telephony for communications, as well as low-powered wireless
- Wildfire of IoT-unique protocols of varying strengths
- The battle may be largely lost at the choice of device infrastructure.
  – Some equipment may just not be securable.

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

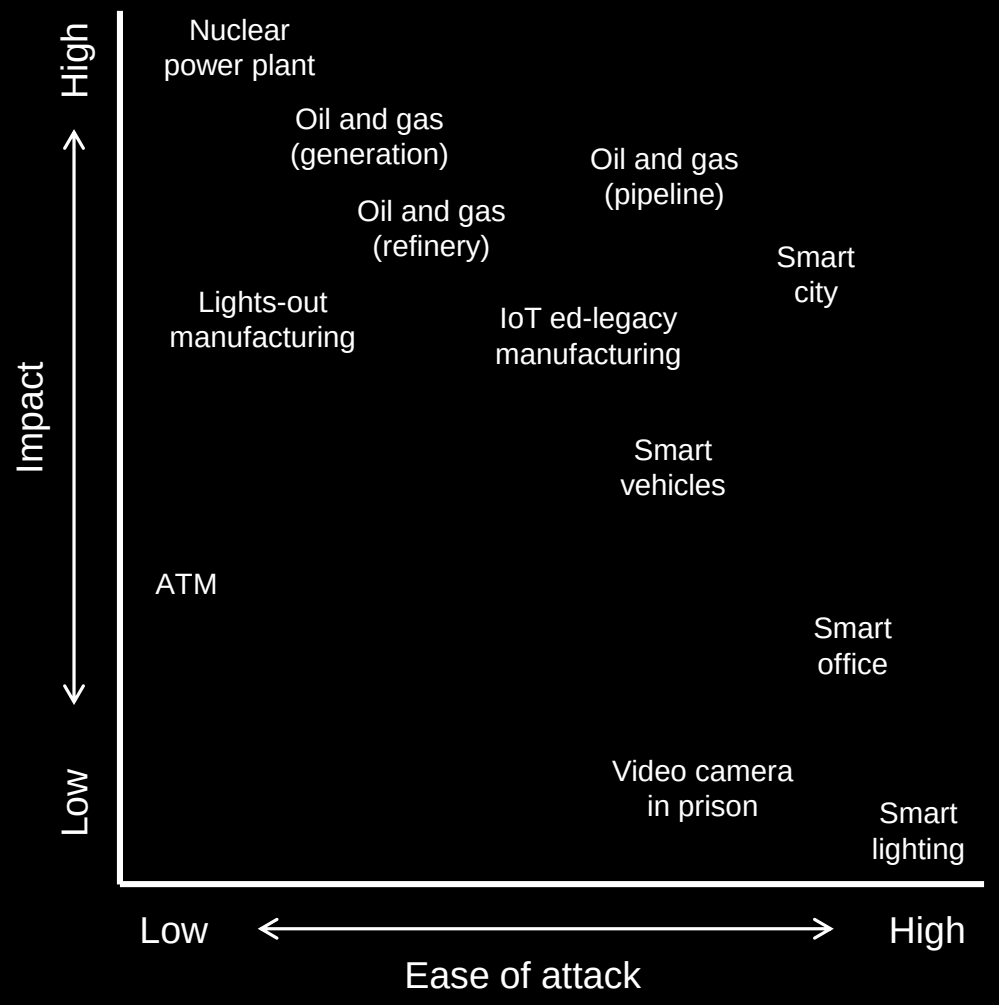
Technical and physical security both play a role in industrial IoT (IIoT)



- Security of many IoT devices and protocols leave much to be desired.
- In IIoT, we also have to consider the physical security and ability to access the infrastructure.
- Ideally, we have both rich security features and restricted physical access, but that is rarely the case in IIoT.
- Many IIoT scenarios depend on insecure hardware in rather public places.
- ATMs are public-facing but have a good security track record (with some spectacular exceptions).
- A Mirai-vulnerable video camera, not connected to the Internet and deployed in a supermax prison, is unlikely to be compromised.

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

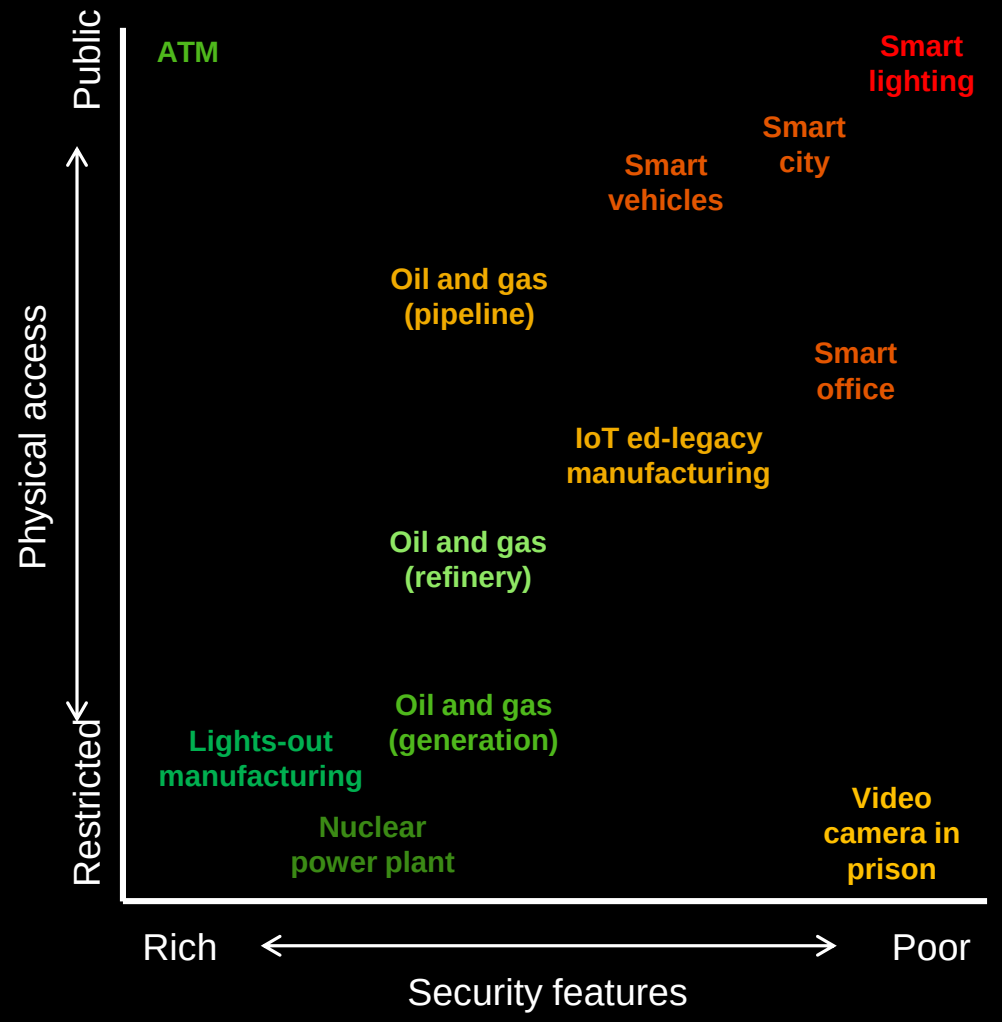
Impacts of various IIoT scenarios are very different, however

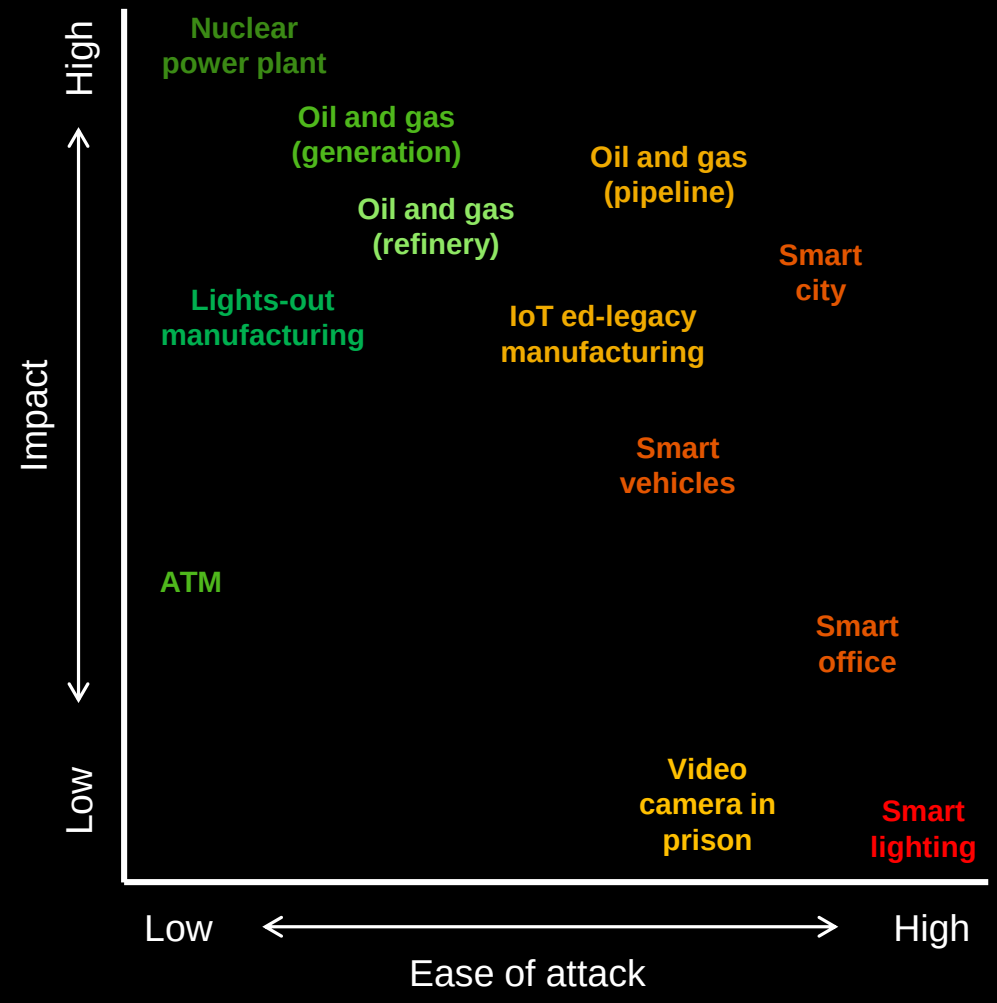


- Beyond access and security features, the impacts of various use cases differ widely.
- Hacking smart lighting is annoying but is unlikely to lead to loss of life or injury.
- Compromise of an oil refinery or nuclear power plant could lead to catastrophic disasters.
- Use of insecure devices might therefore be acceptable in trivial scenarios – though even there a compromise could lead to loss of reputation, lost customers, or government intervention.
- In IIoT scenarios in critical infrastructure, energy, transportation, manufacturing, and the like, it most certainly would not be, and security for IIoT should be carefully designed in, including device choice, encrypted communication channels, security and monitoring tools, …

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Security must be stronger where impact is higher

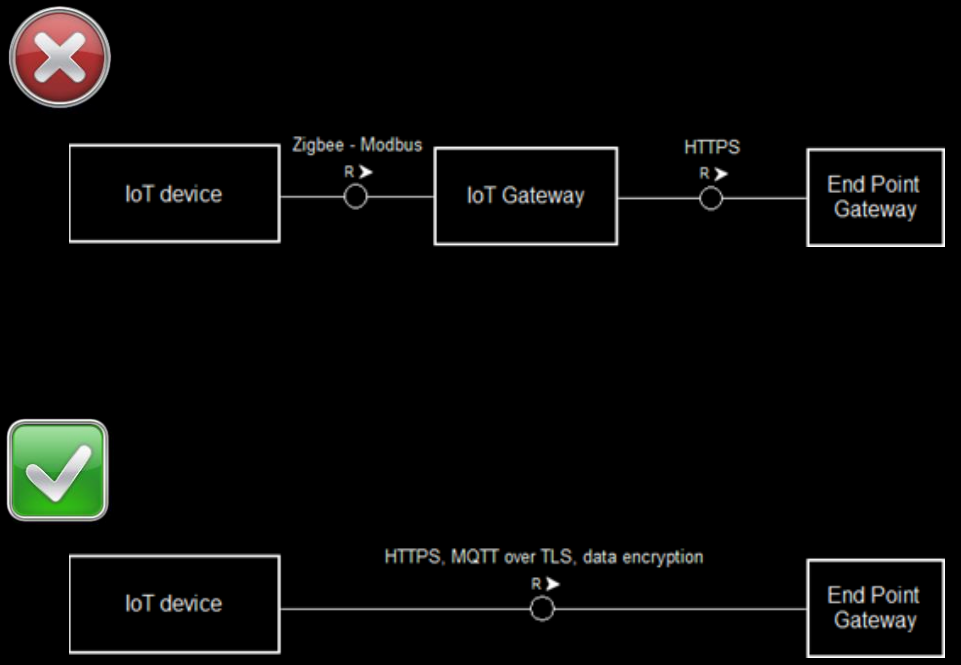




© 2017 SAP SE or an SAP affiliate company. All rights reserved.

The criticality of end-to-end encryption

- Many IoT devices (especially consumer) use an IoT gateway model, using IoT-specific protocols such as Zigbee, Z-wave, BLE, Modbus, …
- Strong encryption is usually only from the IoT gateway.
- Unfortunately, security of these protocols is often proven to be poor and can be subject to manipulation.
- **End-to-end encryption is the only way to guarantee data from the device is received without eavesdropping, tampering, or spoofing and comes from the device we believe it comes from.**
- Where the device is not capable of modern PKI/TLS, the gateway problem can be avoided by on-device data encryption, where the device design (and manufacturer) allows it.
- Registration and onboarding are still a bit of an issue.



See also: *[SAP Community] The importance of client certificates in IoT*

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Threat modeling

Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application. […]

The concept of threat modeling is not new, but there has been a clear mindset change in recent years. Modern threat modeling looks at a system from a potential attacker's perspective, as opposed to a defender's viewpoint.

Source: OWASP.org Application Threat Modeling

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

STRIDE mnemonic

Spoofing identity

Tampering

Repudiation

Information disclosure

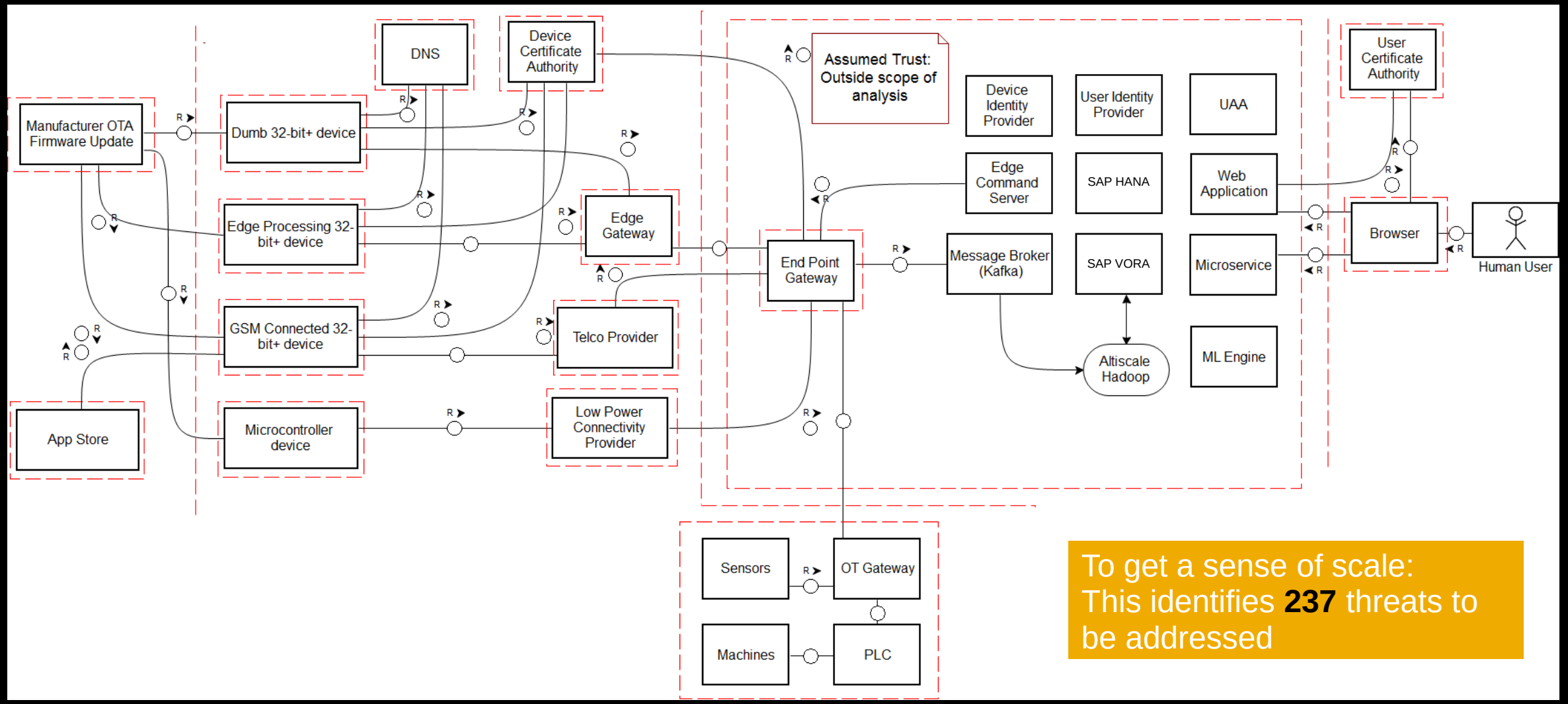
Denial of service

Elevation of privilege

- Attacks pretending to be someone else (e-mail spoofing, impersonation attacks, replay attacks)
- Malicious modification of data (rewriting Web requests using proxies, transaction modification, database corruption)
- Attacks that allow an action that cannot be proven, or cannot be proven to be malicious
- Exposure of information that should not be (exfiltration attacks, wiretapping, database dumps)
- Attacks that make the system or service unavailable to legitimate users
- Attacks allowing an unprivileged user (OS user, application user, ...) to gain privileged access (root privileges from a nobody or standard user account, admin role escalation from regular user)

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Threat modeling a heterogeneous IoT landscape



To get a sense of scale:
This identifies **237** threats to be addressed

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Qualitative difference in risk profile between 32-bit+ devices

1 Dumb 32-bit+ device

- Is almost certainly unidirectional
- Reads value from internal memory, and passes on to end point
- Has no data storage

2 Smart/Edge processing 32-bit+ device

- Often bidirectional, can receive commands – therefore has its own interface that can be attacked
- Reads value from internal memory, collects and stores it on-device (temporarily), processes the data, and generates results that are sent to end point
- Data storage required, so will include a writable file system

3 Over GSM

- Adds a new party, including potentially use of app store or marketplace
- Networking outside of our regular network, by definition – complicates monitoring
- Billing, SIM management, provisioning, and more

Features in common

- Modern PKI capable
- Full OS and tooling
- Should have OTA firmware update capability (or a self-destruct mechanism)

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

General guidelines: Utilize existing tooling and whitelisting

Use existing tooling where we can

- Many IIoT devices are essentially just Linux hosts.
- This allows us to use standard security tooling we are already familiar with:
  - TLS/PKI transport encryption
  - Iptables firewall baked into the kernel
  - Software-defined networks (SDN) and Network Access Control (NAC)
  - IPS/IDS
  - SIEM incident response and monitoring tools
  - Honeypots
  - DNS
- Standard tooling administrators are familiar with should be more secure than tools nobody knows…

Whitelisting

- M2M communication is highly predictable.
- We should know in advance what are legitimate services and end points in the landscape that devices should communicate with.
- We can configure firewall rules that only allow the device to communicate with known legitimate services.
  - Data ingestion point
  - Time server
  - DNS
  - Update server
  - Certificate authority

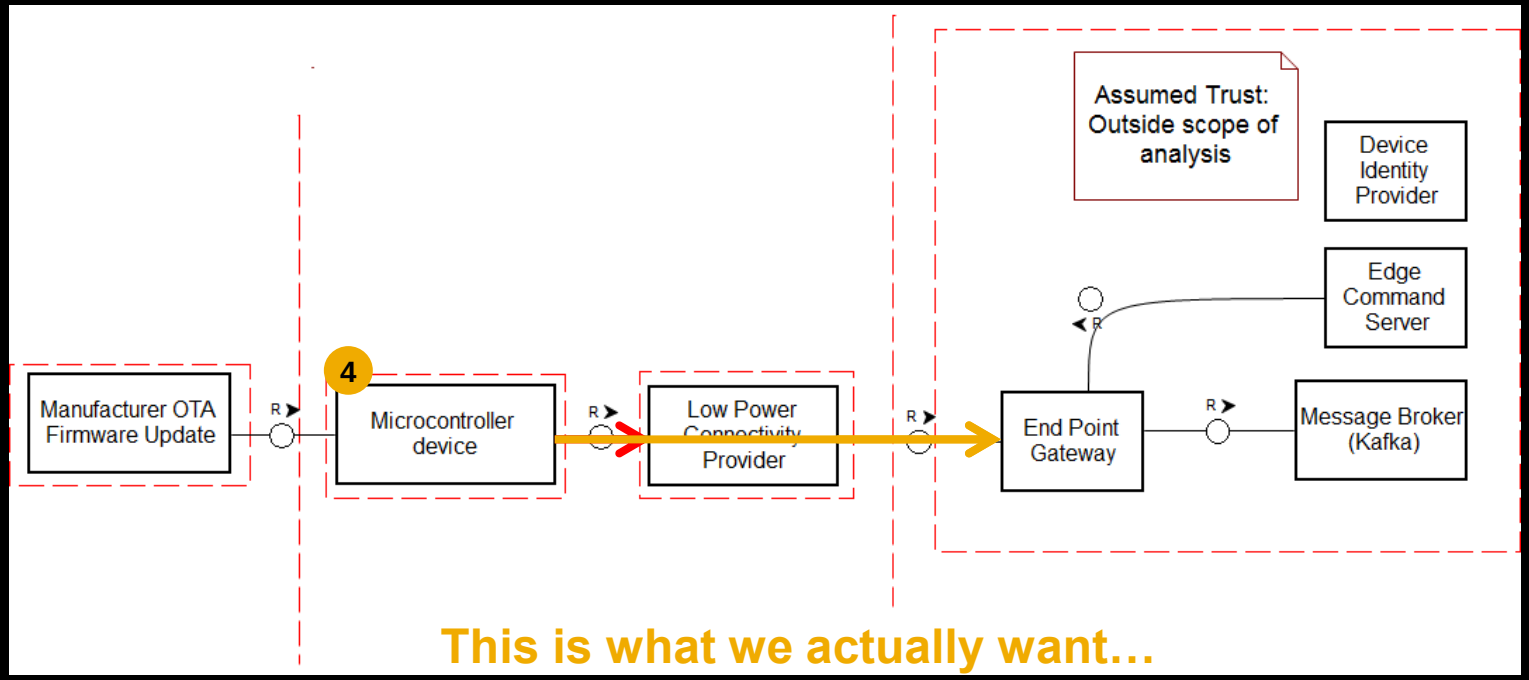
See [SAP Community] A proposed template for more secure IoT edge architectures

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Microcontrollers communicating over low-power networks

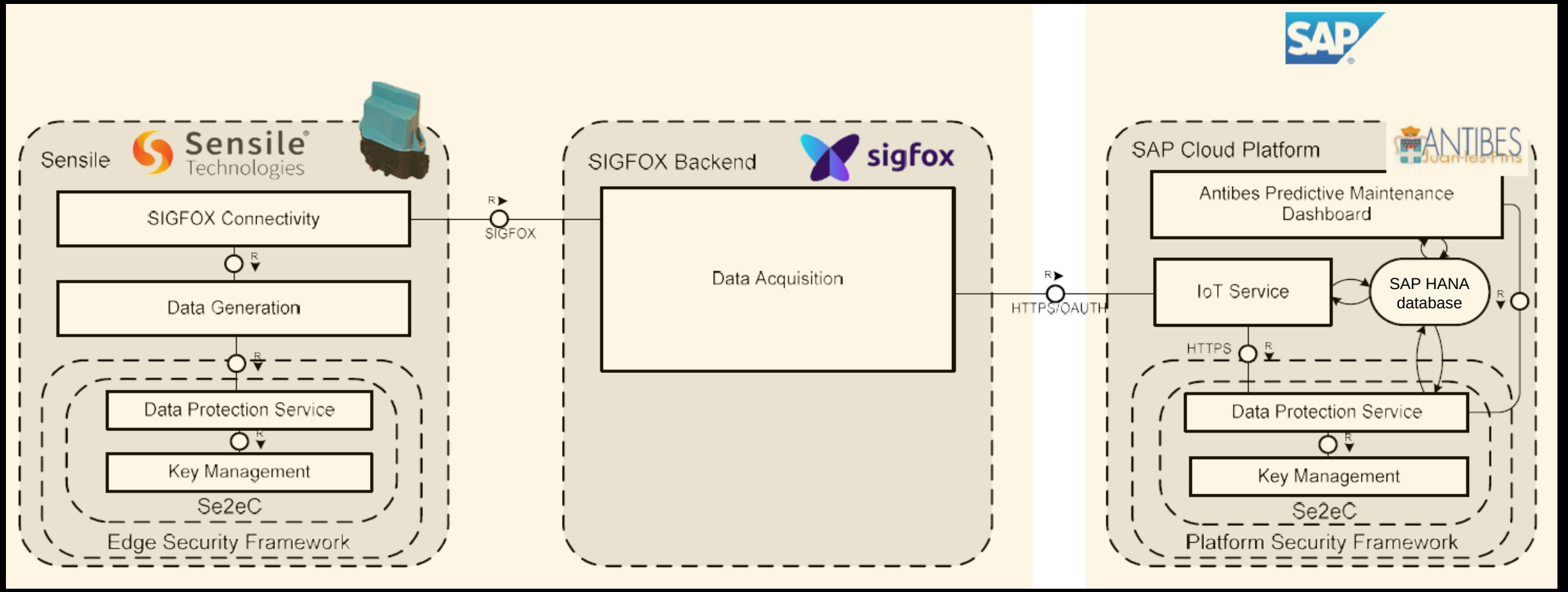
Lifetime vs. security

- Typically battery operated – the less the device does, the longer it lives
- Deployed out in the real world: smart cities, utilities, …
- No or rare physical maintenance
- Severe constraints on data size and message volume (see later)
- Connectivity provider typically offers no end-to-end encryption capabilities
- Standard PKI does not work (device not capable of the required math)
- May or may not have an OTA firmware update capability



© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Architecture



More information: Laurent Gomez, José Marquez

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Device identity

Onboarding and registration

- For all devices, but especially microcontrollers, secure onboarding and registration at scale are complex and cumbersome, and if the manufacturer doesn't allow access, may be impossible.
- Often, the entire code is shipped as "firmware," without a writable file system or SSH/SCP access.
- Many manufacturers do not open source their software; many do not allow to run custom firmware.
- Certificate or key-based: somehow need to place certificate files onto the device – difficult to manage
- Current easiest-to-manage option: registration certificate that on first contact pulls down a certificate for the unique device – but makes initial trust harder to establish

Identity baked into the chip itself

- New R&D by chip manufacturers (in which SAP plays a role) to bake secure keys directly into the silicon of the chip itself
- Can only be accessed by secure computing module on the chip, so secret is never shared
- Secret key is then used to derive device keys for authentication.
- On first contact, with a lookup provided by the manufacturer, we can identify individual devices directly without needing to distribute certificates or keys ourselves.
- With an identity already baked in, registration becomes automatic upon first contact with the end point.

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

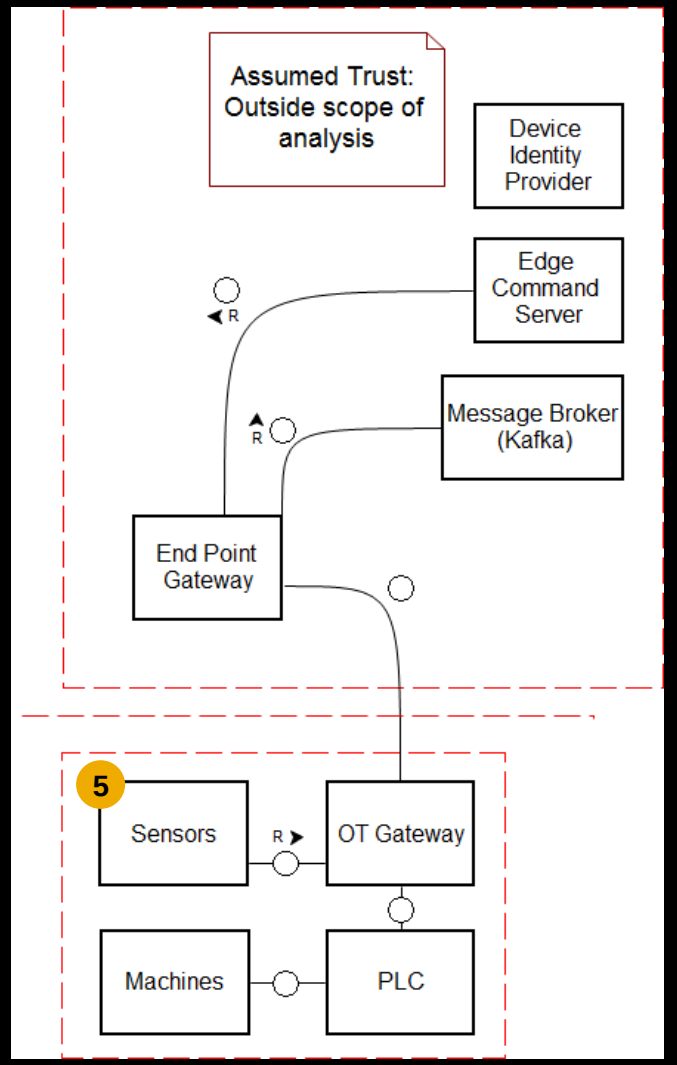
SCADA/ICS, PLC: The OT network

Safety vs. security

- Safety paramount in OT environments
- Several decades of “air-gapping” for security
- Newer machines, PLCs, and ICS are PKI capable, but machines have long lifecycles and use of encryption is still minimal.

Available security product

- OT-IT connectivity and security typically in the form of a VPN tunnel
- No end-to-end encryption, only between gateways
- Often some capability to check PLC configuration
- Passive monitoring, no active intervention at all
- Mostly startups of <20 employees: startups vs. OT long tail a severe mismatch
- OPC-UA adoption will help (allows for encryption, as well as signing)



© 2017 SAP SE or an SAP affiliate company. All rights reserved.

OPC-UA security features

- **Transport**
- **Session encryption**
- **Message signing**
- **Sequenced packets**
- **Authentication**
- **User control**
- **Auditing**

OPC-binary, SOAP-HTTPS

Messages are transmitted with 128-bit or 256-bit encryption levels.
Cryptographically signed messages guarantee they are received as sent.
Message replay attacks are eliminated or hampered with sequencing.
PKI certificates exist for each UA client and server.
Applications can require users to authenticate, as well as access rights.
Logging provides an access audit trail.

See OPC Foundation - Unified Architecture/

Overall OPC-UA security guidelines are very good, and seem to have learned a lot from IT security, including PKI, network segmentation, zone-specific DNS, individual machine and user identity, use of threat modeling and risk-based approach, …

Main question is adoption, and adopting OPC-UA securely…

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

Thank you.

Contact information:

Jay Thoden van Velzen
Director, Cloud Delivery Services & Enablement
jay.thoden.van.velzen@sap.com
+1 408 921-1301

Low power encryption:

Laurent Gomez
Security Research
laurent.gomez@sap.com
+3 361 947-7264

José Marquez
Enterprise Architect, SAP Leonardo
jose.marquez@sap.com
+49 160 90822678

SAP Run Simple

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.
See http://global.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.