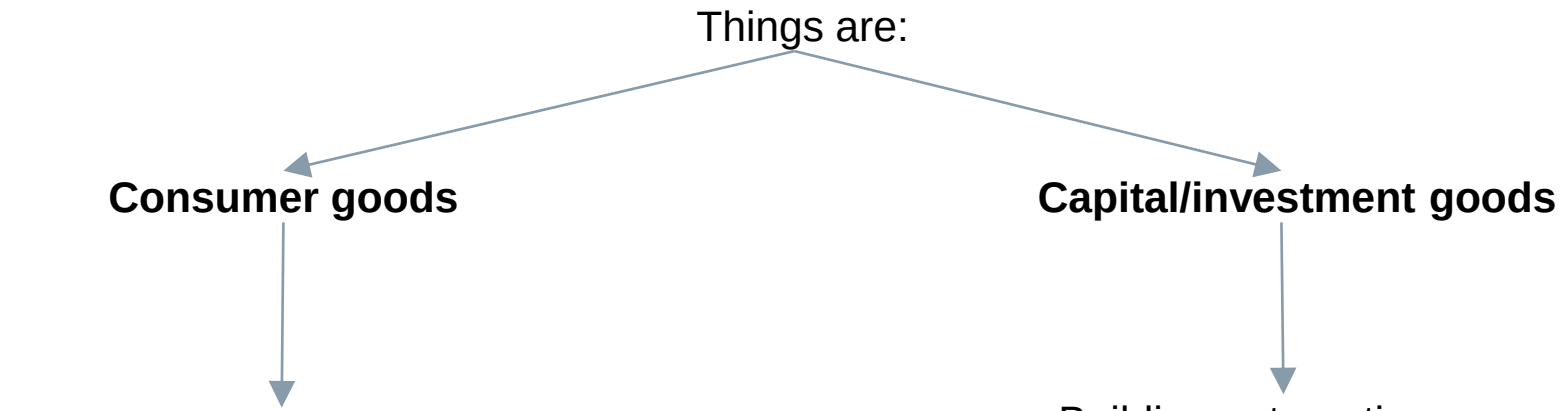
SIEMENS

Siemens Corporate Technology | July 2015

Joint IRTF T2T RG / W3C WoT IG Meeting 18-19 July 2015, Prague

Security & Privacy Features in Current IoT Projects

There Is a Continental Divide

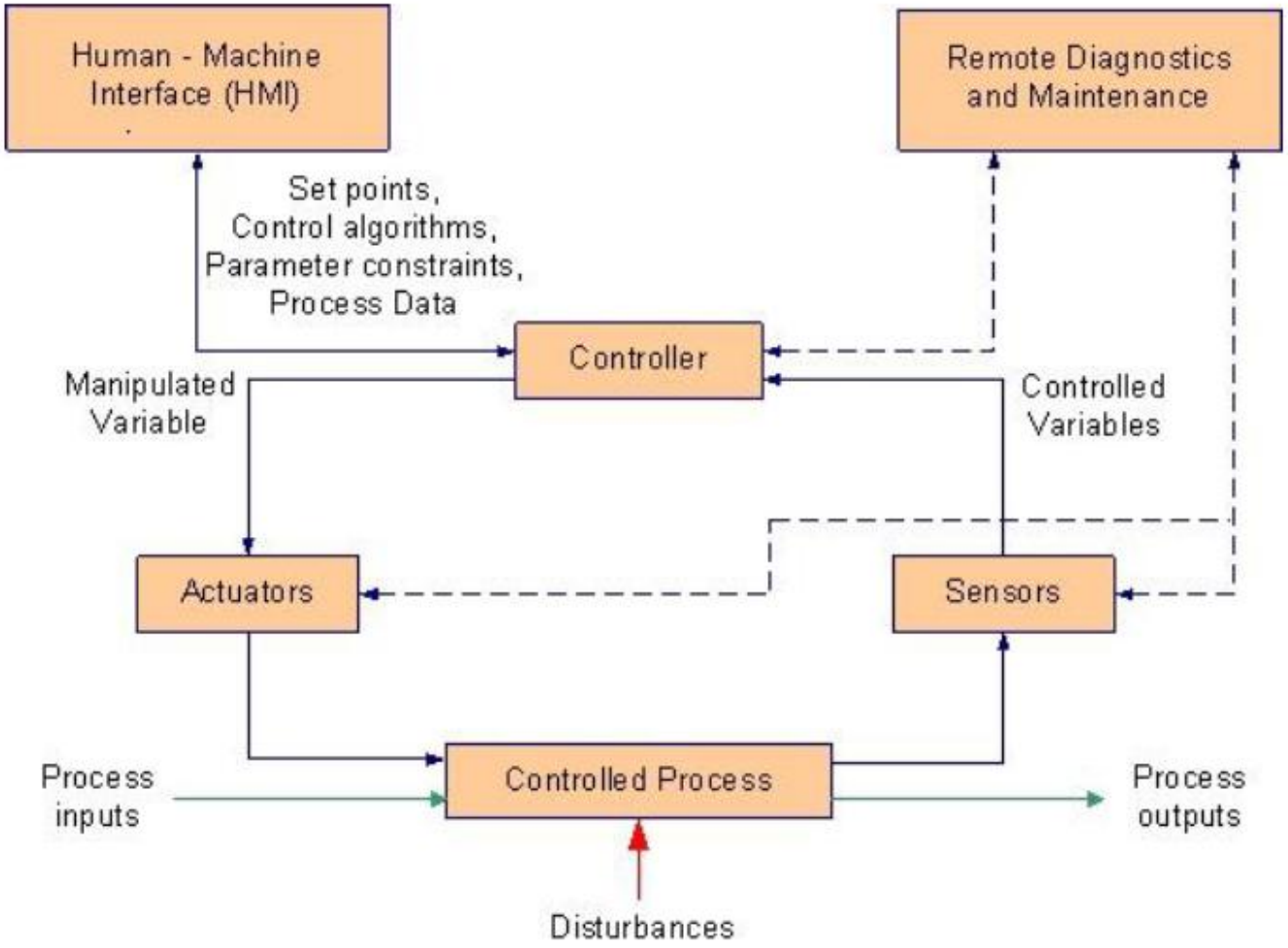


Rule-of-thumb:
Industrial Internet=IoT/WoT@capital/investment goods

What Is the Problem? Here: For Industrial Internet

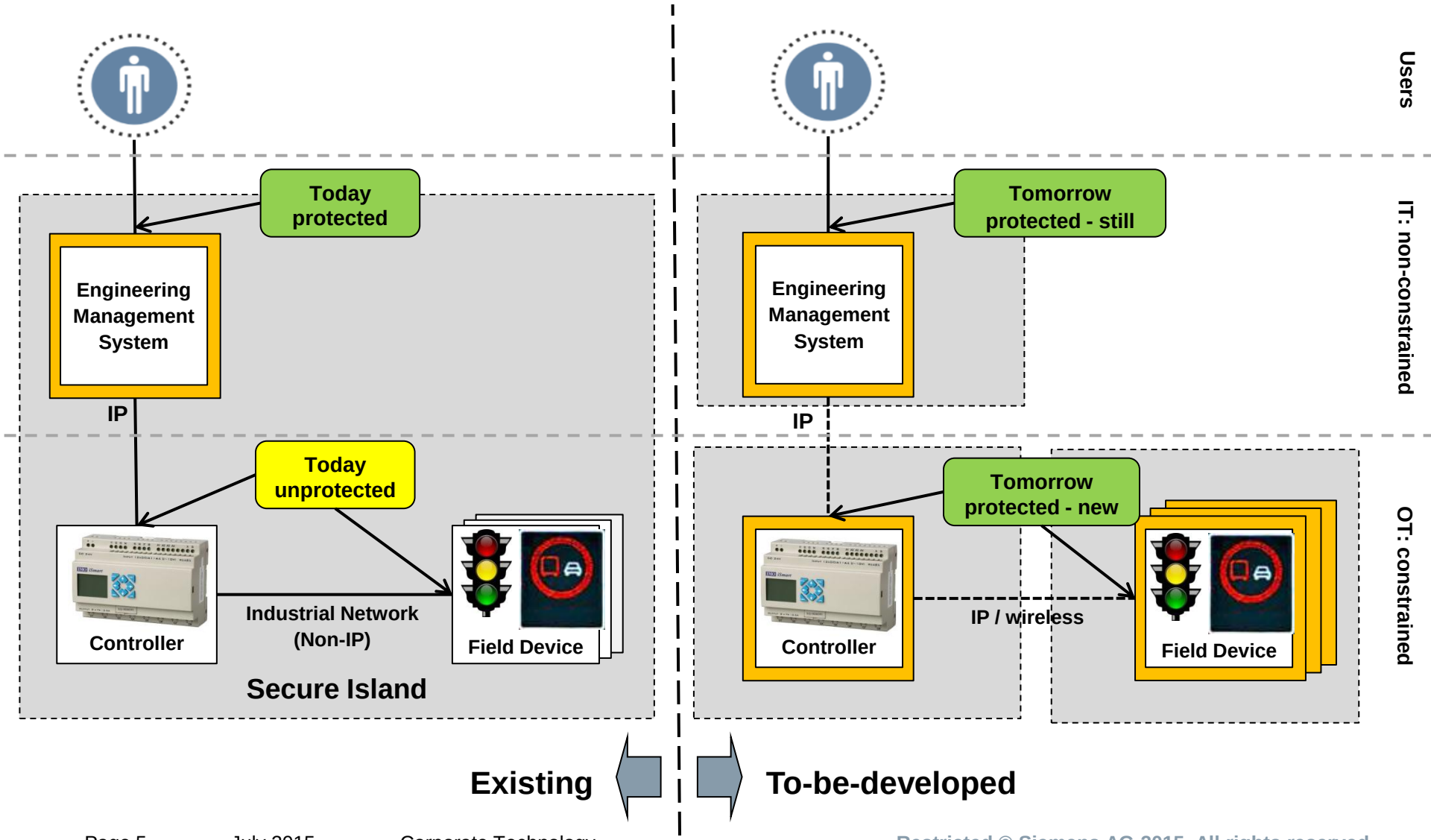
- Statement by the IIC (IIRA, p. 18):
  - *Security of industrial control systems today often relies on physical security, the isolation of the systems and the obscurity of proprietary communication protocols*
  - *Industrial Internet Systems, on the other hand, are, by nature, connected and distributed.*
- Q: what does that actually mean?

What Is an Industrial Control System?



Source: Figure 2-1 in NIST SP 800-82, REVISION 2 DRAFT

What Is the Need? Here: For Industrial Internet



What Is the Problem? Here: For Consumer Goods

- Translation left to the audience

Questions – General (1)

- ***Q1: What is the nature of your undertaking in IoT/WoT?***
  - Analysis, observation
  - Research, prototyping
  - Product/solution creation
  - System integration or services
- ***Q2: What is the type of things or devices?***
  - Consumer goods
  - Capital/investment goods
- ***Q3: Who is the owner of these things or devices?***
  - Individual users (human beings)
  - Legal entities
- ***Q4: What is the economic value of an individual thing or device?***
  - High – say >1000 $ e.g. cars
  - Medium – say 100-1000 $ e.g. controllers
  - Low – say <100 $ e.g. wearable devices

Questions – General (2)

- ***Q5: What is the strategy of device/things exposure?***
  - Internal-facing
  - Partner-facing
  - Public-facing
- ***Q6: What is the designated device/things connectivity?***
  - Near-field
  - Local area
  - Wide area
- ***Q7: How are interactions with devices/things conducted?***
  - Direct interactions with devices/things
  - Mediated interactions via gateway/proxy components

Questions – Contextual Security

- ***Q8: Are throttling resp. rate limitation mechanisms provided?***
  - Enforcement of rate-limits
  - Dynamic determination/adjustment of such limits
- ***Q9: Are intrusion detection/prevention mechanisms provided?***
  - Detecting suspicious traffic
  - Blocking suspicious traffic, other counter-measures
- ***Q10: Are risk-based entity authentication means used?***
  - Authentication scheme depending on source network
  - Authentication scheme depending on device properties (OS, software version)
  - Authentication scheme depending on caller velocity

Questions – Communication Security

- ***Q11: Are communication security mechanisms implemented?***
  - None
  - Message encryption
  - Message authentication
- ***Q12: Which security protocols are utilized?***
  - Transport-bound: IPSec, TLS, DTLS, DICE, SSH, others
  - Information-bound: PKCS/CMS or S/MIME, XML Encryption/Signature, JOSE, COSE, others
- ***Q13: What are the endpoints of secure communications?***
  - Upstream gateway/proxy components
  - Actual things/devices
- ***Q14: Which initial keying associations are used?***
  - Public key certificates , private keys
  - Raw public keys, private keys
  - Shared secret keys or shared secrets e.g. TLS-SRP

Questions – Authorization

- ***Q15: Are authorization mechanisms implemented?***
- ***Q16: Which component is responsible for authorization decision enforcement?***
  - Actual things/devices?
  - Upstream components such as gateways/proxies
- ***Q17: Which component is responsible for authorization decision making?***
  - Actual things/devices?
  - Supplementary components such as authz servers
- ***Q18: What is the relation between authorization decision making component and caller?***
  - *Same domain: the authorization decision component assumes to be able to authenticate callers by itself*
  - *Cross domain: the authorization decision component does not assume to be able to authenticate callers by itself*
- ***Q19: Which entity is responsible for authorization policy making?***
  - Individual user
  - System admin
- ***Q20: Is the change-of-owner use case addressed?***

Questions – Entity Authentication

- ***Q21: How is the authentication of callees addressed?***
  - *On transport-security level?*
  - *On application-level*
- ***Q22: How is the authentication of callers addressed?***
  - *On transport-security level?*
  - *On application-level*
- ***Q23: Against which component do callers authenticate?***
  - Directly against individual devices/things
  - Against an upstream component such as a gateway/proxy that acts as an intermediary (inline authority)? Inside or outside the device-domain?
  - Against a dedicated security component? Inside or outside the device-domain?
- ***Q24: What is the peer that a caller can authenticate?***
  - Individual devices/things that are called
  - An upstream component such as a gateway/proxy that acts as an intermediary (inline authority)?
  - A dedicated security component?

Questions – Entity Identification

- ***Q25: Which metadata is stored per caller or callee?***
  - Identifiers (number, type)
  - Attributes (number, type, meaning)
  - Affiliations such as group memberships or role assignments (number, type)
- ***Q26: When is this data provisioned?***
  - During manufacturing
  - During deployment
  - During operation
- ***Q27: How is it stored?***
  - Centrally
  - Distributed
- ***Q28: What is the relation between caller and callee?***
  - *Same domain: caller and callee entity identity belong to the same domain*
  - *Cross domain: caller and callee entity identity belong to different domains*

Author

Oliver Pfaff, Siemens AG, CT RTC ITS