Industry security requirements on IoT devices

Toni Ericsson
Automation Solutions
Agenda

► What we do
  - Tetra Pak
  - Automation Solutions

► Our history in IoT

► Our future in IoT

► Our IoT security challenges and requirements
What we do
Automation Solutions

Tetra Pak Automation Solutions

Tetra PlantMaster™

Production Control

IoT

ERP

Building Automation intelligence

TM
Integration of systems & information based on one automation platform

Service Infrastructure

Systems Integration

Tetra PlantMaster

Automation Solutions
Core Development

Technologies

Technologies

Line level
Tetra …enso

Unit level
TA Flex

Business Unit DBPF

Business Unit CPS

Business Unit IC

TDN

TDN

Carton Value

Carton Economy

Carton Bottle + GT

Tetra ReCart

Line level
iLines

Unit level
A6 Evero
A3 Flex

Service Enablers

PDN / TDN

Tetra Pak
Automation Solutions
Automation Solutions
Strategic scope

MES
Plant control
Line Solutions
Equipment - Embedded Automation
Tetra PlantMaster
High level IoT based services

- Food safety & quality
- Performance & planning
- Life-cycle management
- Environment
Our history in IoT
Way back when.....

a very small team set out to bring digital information and connectivity into a very mechanical, manual and non-connected world...
... with an integrated IoT infrastructure
Connectivity across the globe

In total appr 800 connected plants and 4200 connected filling lines. Data captured from appr 75% of all lines with performance logging.
Key strategies employed

- Treat networks as insecure → VPN/SDN approach
- Keep a central, distributable data repository. Reuse data building contextual relationships
- Make applications off-line capable where possible. Connectivity may be intermittent or absent
- Build on open standards and protocols, useable on commodity components
- Build in tracebility wherever possible and make it transparent to our customers
- Protect confidentiality and integrity of critical components and IPR, Tetra Paks and our customers
- Usability....simplify, simplify, simplify.......
Our future in IoT
Key value drivers in the food industry

TRACEABILITY AND TRANSPARENCY

Secure food safety and quality

Optimise plant and supply chain

Customize consumer experience

EFFICIENT HANDLING AND AUTOMATION
Future drivers for IoT

TRACEABILITY AND TRANSPARENCY
- Secure food safety and quality

EFFICIENT HANDLING AND AUTOMATION
- Optimise plant and supply chain
- Customize consumer experience

Suppliers

Producers

Distributors

Retailers

Consumers
Values delivered through IoT

Capture data

Act on data

Share data

Analyse data

Targeted marketing

Know why

Product information, Quality

Supplier

Know when

Performance, Maintenance, Product information, Quality

Producer

Know where

Logistics, Transportation conditions, Claims

Distributor

Preferences, Demographics, Consumption, Claims...

Retailer

Legal

Drive Recycling

Minimise errors

Increase profit

Purchase the right product

Know why

Act on data

Know when

Act on data

Know where

Share data

Act on data

Analyse data

Analyse data

Analyse data

Analyse data

Analyse data

Analyse data

Analyse data

Capture data

Capture data

Capture data

Capture data
Our IoT security challenges and requirements
Our IoT Scene

IoT Service Provider

IoT Service Customer

Tetra Pak Automation Solutions
A real world service visit…
...and as it happens in the digital world.
Industrial IoT security areas

Information

Execution

Safety
Our IoT information acquisition & usage
Requirements for trusted information exchange

- IoT devices shall be capable of submitting data for customer verification before transmission or mirror data flow.

- Encryption & signing must be supported at both data level and preferably at transport level.

- IoT devices shall be able to keep non-alterable local log of events available for audit.

- Support interfaces of established and trusted 3rd party authorities.
Requirements for trusted interactions with execution systems

- Support multi-party trust, access and authorization control

- Updates of device software shall be handled by a secure, hardened and static nucleus

- Successful update of a device shall be verified by the nucleus and otherwise fully reverted

- IoT devices shall be able to only run code or implement change signed by one or more parties

- IoT devices shall not rely on periodic or online updates for security
Requirements for trusted interactions with safety regulated systems

- IoT devices connected to safety controlled must be able to instantly react on safety related signals

- IoT devices must be able to instantly generate proper signals of relevance to the safety system

- Execution of safety related events must be done by hardware circuitry not depending on software state

- IoT hardware must be able to interact with the native signals of equipment automation and safety systems
Need of an IoT Security framework

IT security
- Confidentiality
  - Integrity
  - Availability

IoT security
- Transparency
  - Confidentiality
  - Availability
  - Integrity
  - Traceability

OT security
- Availability
  - Integrity
  - Confidentiality

Confidentiality
Availability
Integrity
Transparency