

Industrial Security Tag 2022 unverschlüsselte vs. verschlüsselte Verbindungen im Anlagennetzwerk

Inhaltsverzeichnis

Zusammenfassungszoom




Industrial Security Tag 2022
unverschlüsselte vs. verschlüsselte
Verbindungen im Anlagennetzwerk

SIEMENS

Digitalization creates ...

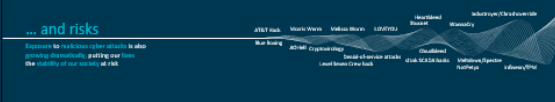
Opportunities

Efficient processes are being connected by the Internet of Things, and on the basis of our infrastructure and security.



... and risks

Explosion of devices and systems also creates new risks, putting our the stability of our society at risk.



Siemens Defense in Depth concept Integrated Security




Defense in depth

- Plant security
- Network security
- System integrity

SIEMENS

Siemens Defense in Depth concept System integrity



System integrity

- System hardening
- Authentication and user administration
- Patch management
- Detection of attacks
- Integrated access protection in automation

SIEMENS

SIMATIC PLC S7 Overview Security Features

Access Protection

- Restrict access to the PLC
- Protection by password
- Security by Default

Copy Protection

- Bind the program to PLC serial number or Memory Card
- Program cannot be copied to other PLC/ MMC
- Protects your engineering know-how from being replicated

PLC Master Secret

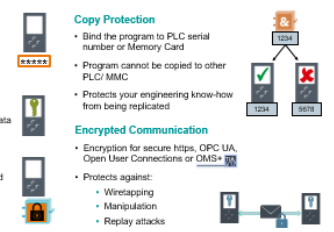
- Protection of sensitive PLC configuration data
- Security by Default

Know-How! Read-Protection

- Program blocks are protected by password
- Protects your engineering know-how

Encrypted Communication

- Encryption for secure https, OPC UA, Open User Connections or OMS+
- Protects against:
 - Wiretapping
 - Manipulation
 - Replay attacks

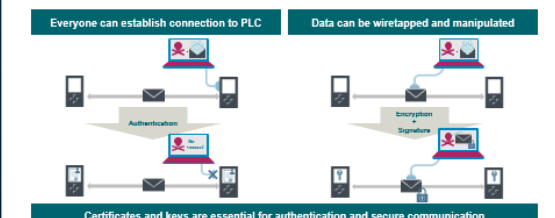


SIEMENS

Encrypted Communication What is the use of certificates and keys?

Everyone can establish connection to PLC

Data can be wiretapped and manipulated



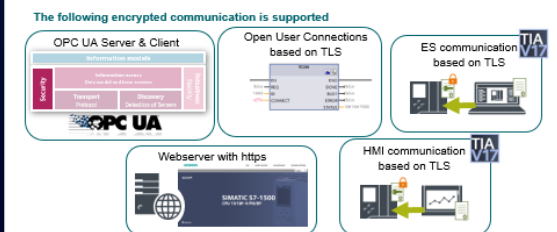
Certificates and keys are essential for authentication and secure communication

SIEMENS

SIMATIC PLC S7: Encrypted Communication Overview

The following encrypted communication is supported

- OPC UA Server & Client
- Open User Connections based on TLS
- ES communication based on TLS
- Webserver with https
- HMI communication based on TLS



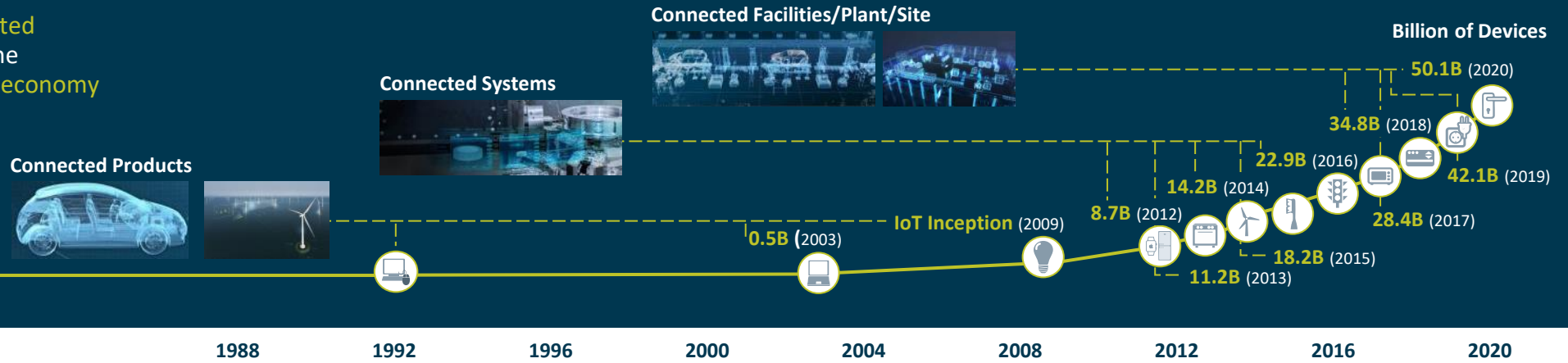
SIEMENS

DEMO

Digitalization creates ...

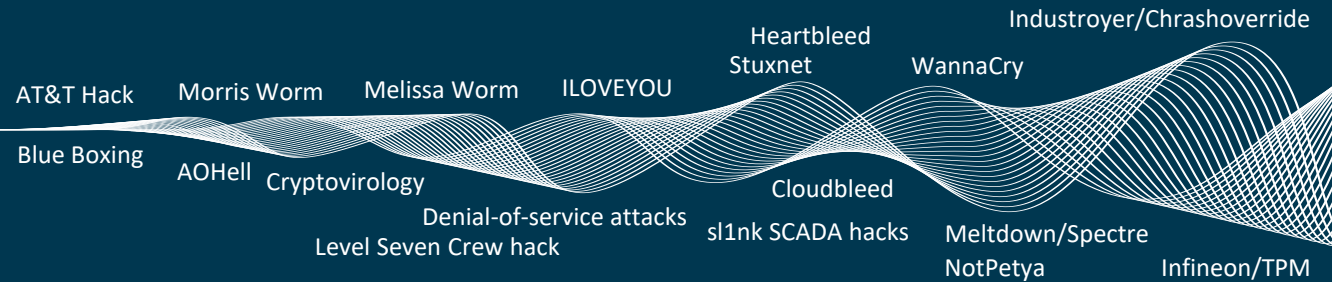
Opportunities

Billions of devices are being connected by the Internet of Things, and are the backbone of our infrastructure and economy



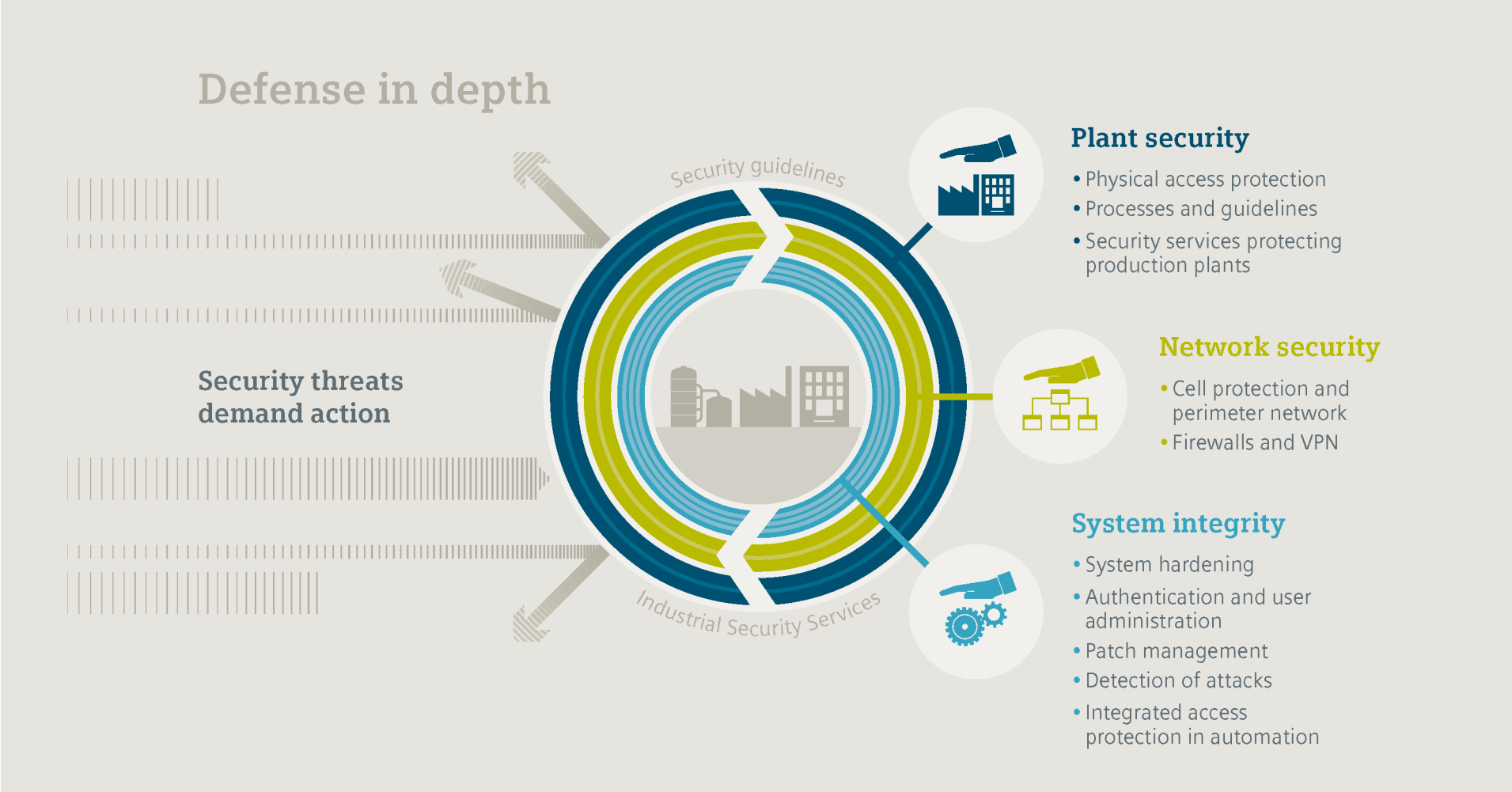
... and risks

Exposure to malicious cyber attacks is also growing dramatically, putting our lives the stability of our society at risk



Siemens Defense in Depth concept

Integrated Security



Siemens Defense in Depth concept

System integrity




System integrity

- System hardening
- Authentication and user administration
- Patch management
- Detection of attacks
- Integrated access protection in automation

SIMATIC PLC S7

Overview Security Features

Access Protection

- Restrict access to the PLC
- Protection by password
- Security by Default 



PLC Master Secret

- Protection of sensitive PLC configuration data
- Security by Default



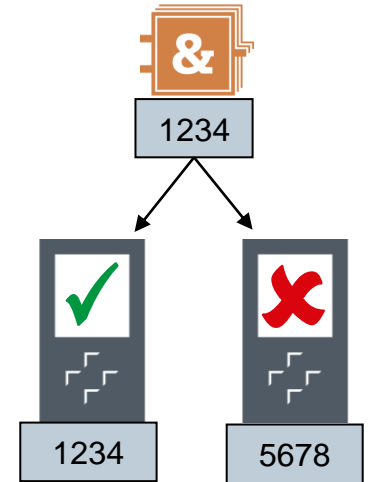
Know-How/ Read-Protection

- Program blocks are protected by password
- Protects your engineering know-how




Copy Protection

- Bind the program to PLC serial number or Memory Card
- Program cannot be copied to other PLC/ MMC
- Protects your engineering know-how from being replicated



Encrypted Communication

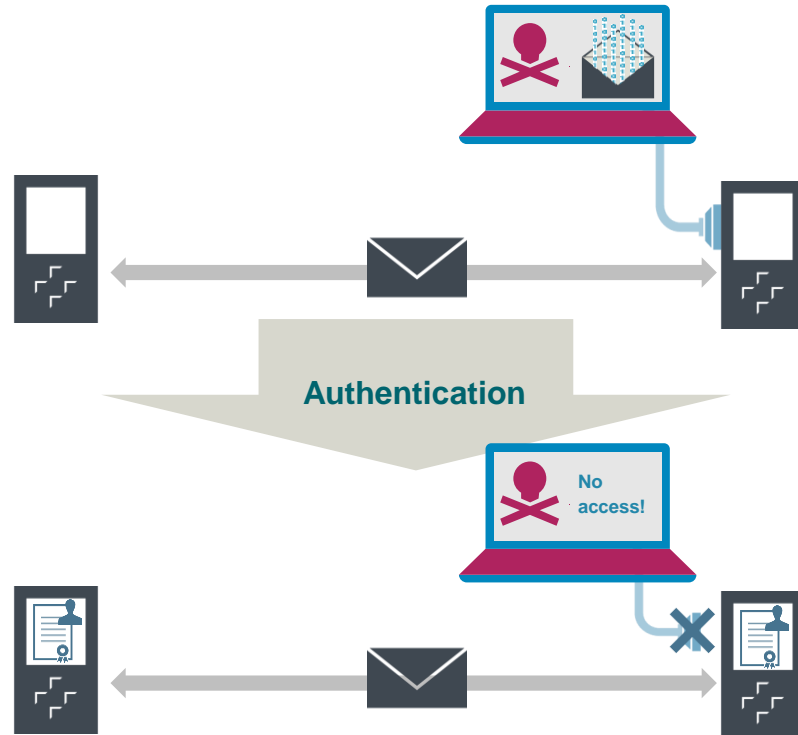
- Encryption for secure https, OPC UA, Open User Connections or OMS+ 
- Protects against:
 - Wiretapping
 - Manipulation
 - Replay attacks



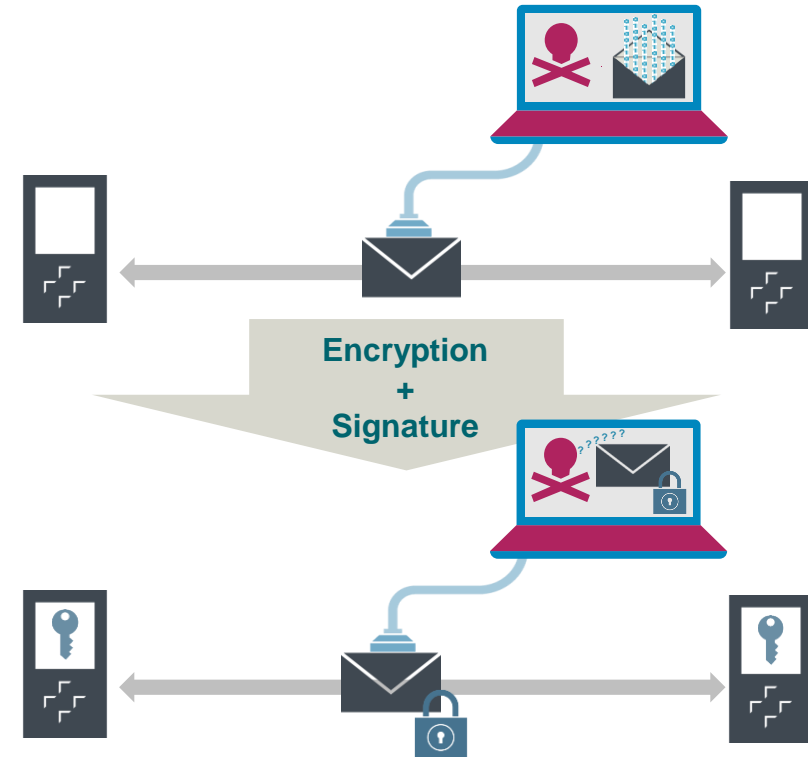
Encrypted Communication

What is the use of certificates and keys?

Everyone can establish connection to PLC



Data can be wiretapped and manipulated

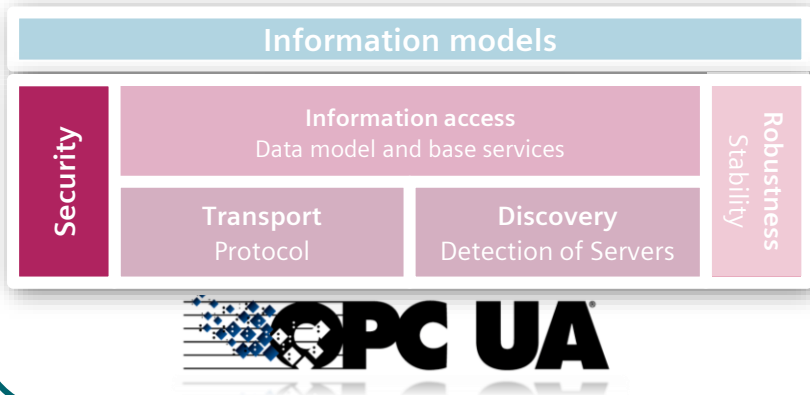


Certificates and keys are essential for authentication and secure communication

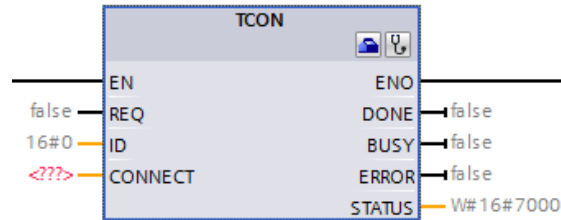
SIMATIC PLC S7: Encrypted Communication Overview

The following encrypted communication is supported

OPC UA Server & Client



Open User Connections based on TLS



ES communication based on TLS



Webserver with https



HMI communication based on TLS



Kontakt

Andreas Ettinger

RC-AT DI FA P APC&SUP

Siemensstraße 90

1210 Wien

Österreich

Mobil +43 664 88556312

E-Mail ettinger.andreas@siemens.com

Disclaimer

© Siemens 2022

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.