OPC DAY FINLAND 2019

6.–7.11.2019 @ EXPO AND CONVENTION CENTRE MESSUKESKUS HELSINKI

#OPCUA #OPCDAY #OPCDAYFINLAND #AUTOMAATIO

OPC UA Security Overview

Jouni Aro

Chief Technology Officer

jouni.aro@prosysopc.com

FINNISH SOCIETY OF AUTOMATION

SUOMEN AUTOMAATIOSEURA RY

SPONSORS:

atvise® BECKHOFF NAPCON kepware NOVOTEK PROSYS OPC SIEMENS Ingenuity for life Unified Automation Valmet FORWARD

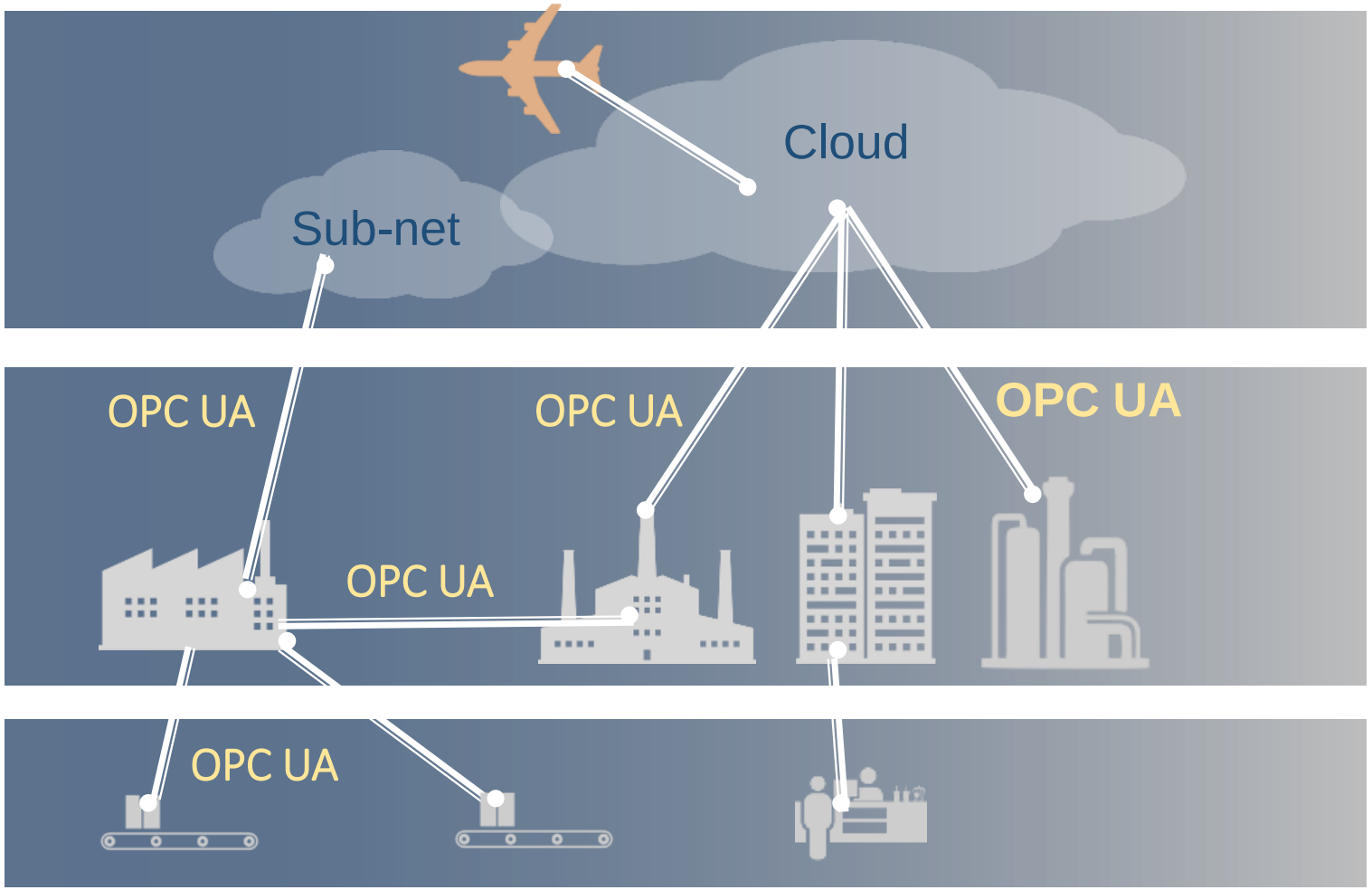
With Connectivity Comes the Need for Security

- Industrial Control System (ICS) Cyber attacks are accelerating

Stuxnet - Iran, 2010

Crash Override - Ukraine, 2016

OPC UA: Essential End-to-End Security



IIoT Standards Are Converging on OPC UA

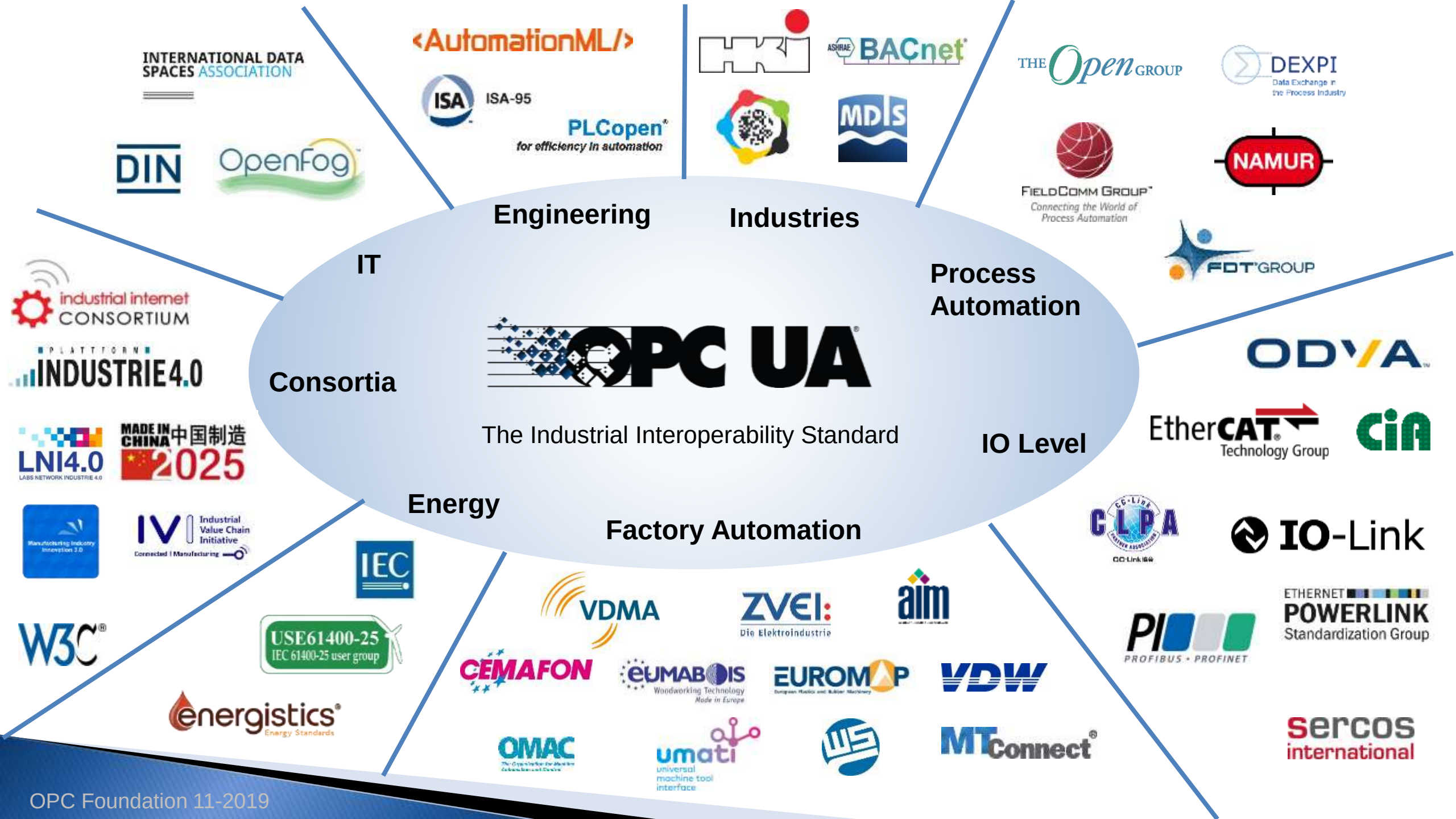
Plattform INDUSTRIE 4.0

industrial internet CONSORTIUM

Made in China 2025
Internet +

OPC UA

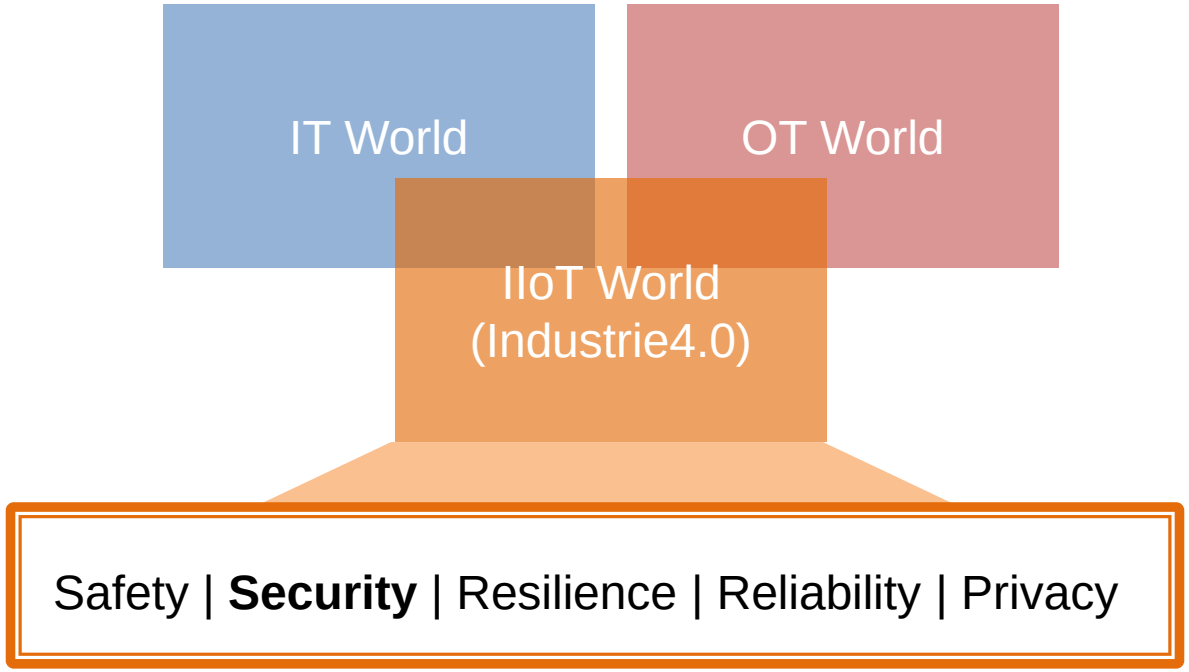
OPC FOUNDATION


INTERNATIONAL DATA SPACES ASSOCIATION
AutomationML
ISA
ISA-95
PLCopen
for efficiency in automation
DIN
OpenFog
HKI
ASHRAE BACnet
MDIS
THE Open GROUP
DEXPI
Data Exchange in the Process Industry
FieldComm Group
Connecting the World of Process Automation
NAMUR
FDT GROUP
Engineering
Industries
IT
Process Automation
industrial internet CONSORTIUM
PLATTFORM INDUSTRIE 4.0
OPC UA
The Industrial Interoperability Standard
Consortia
IO Level
ODVA
LNI4.0
LABS NETWORK INDUSTRIE 4.0
MADE IN CHINA 2025
EtherCAT Technology Group
CiA
Industrial Value Chain Initiative
Connected | Manufacturing
Energy
Factory Automation
CC-Link
CLPA
IO-Link
IEC
VDMA
ZVEI: Die Elektroindustrie
aim
ETHERNET POWERLINK Standardization Group
W3C
USE61400-25
IEC 61400-25 user group
CEMAFON
EUMABOIS Woodworking Technology Made in Europe
EUROMAP
VDW
PI PROFIBUS · PROFINET
energistics
Energy Standards
OMAC
umati universal machine tool interface
MTConnect
sercos international

Data Security

Key Concepts

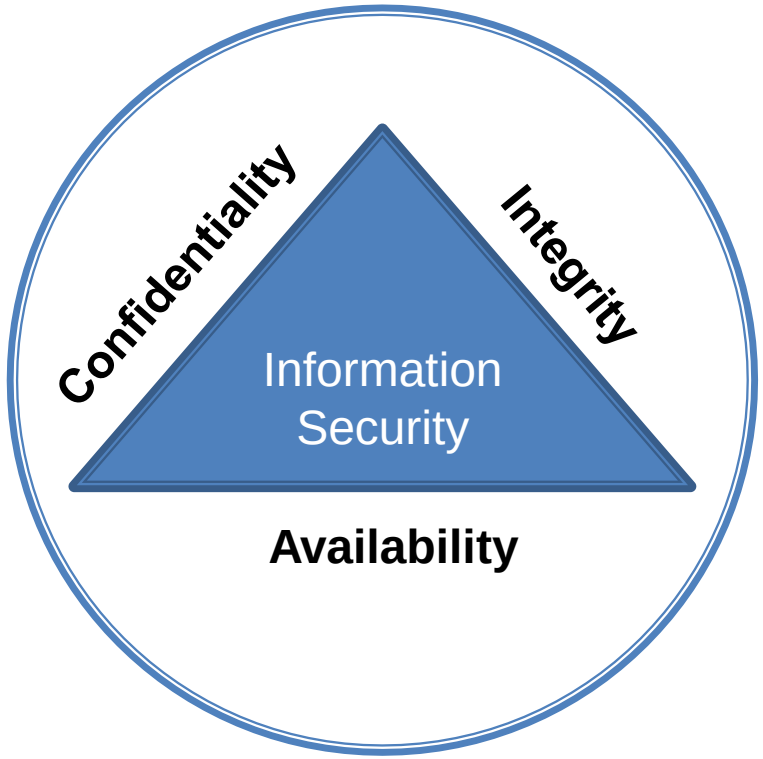
Trustworthiness: Key System Characteristics



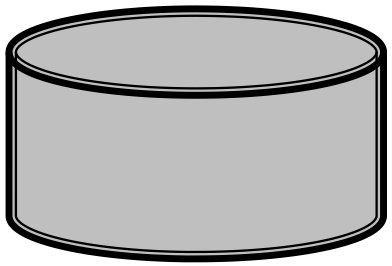
Key Security Concepts

- **Trusted Information (CIA triad)**
  - Confidentiality
  - Integrity
  - Availability

- **Access Control (AAA principle)**
  - Authentication
  - Authorization
  - Accounting (Auditability)



Data Security



Data at Rest

Data in Process

OPC UA

Data in Motion

OPC UA

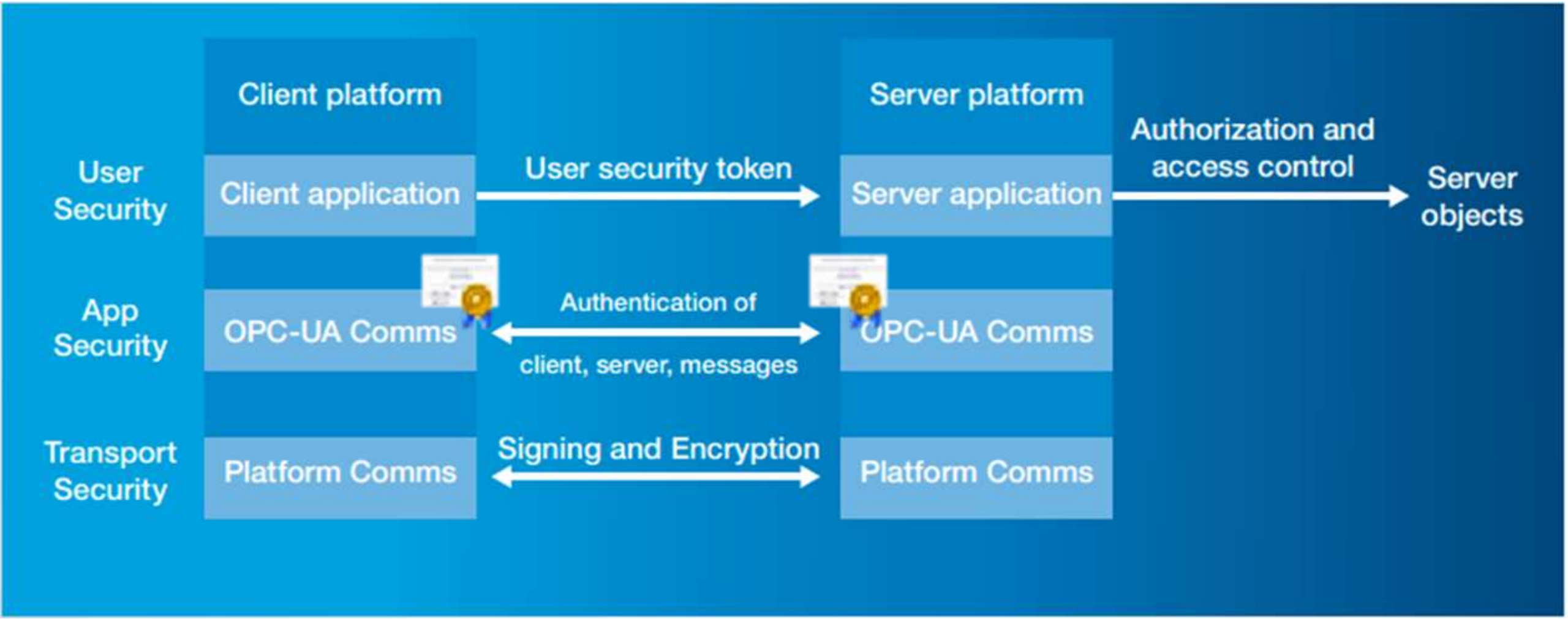
Secure by Design

OPC UA: Secure By Design

1) Concepts
2) Security Model
3) Address Space Model
4) Services
5) Information Model
6) Mappings
7) Profiles
8) Data Access
9) Alarms and Conditions
10) Programs
11) Historical Access
12) Discovery
13) Aggregates
14) PubSub

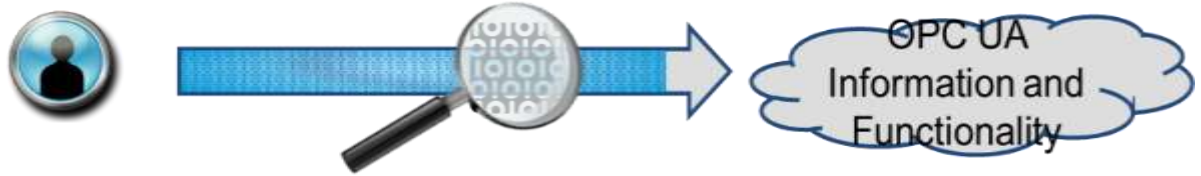
Red: directly relevant for IT security

OPC UA Security: Bringing It All Together

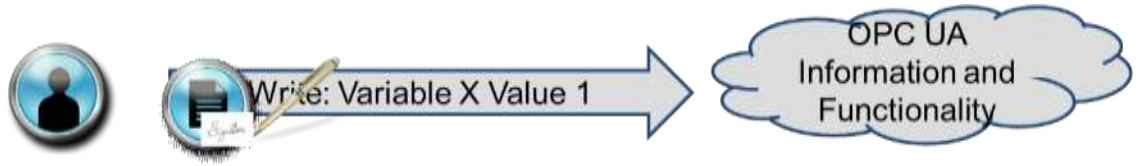


Communication Layer Security

- **Confidentiality** → Encrypting of Messages



- **Integrity** → Signing of Messages



- **Availability** → Minimal message processing before authentication

Examples:
- Restricting message size
- No security related error codes returned

Communication & Application Layer Security

- Authentication of applications
  - Application instance certificates
  - Certificate Authority (CA)
- Authentication of users
  - Username / password, WS-Security Token or X.509 certificates,OAuth
  - Fits into existing infrastructures like Active Directory

- Authorization (Server Specific)
  - Fine-granular information in address space (Read, Write, Browse)
  - Writing of meta data, calling methods
- Auditability
  - Generating audit events for security related operations

Outside OPC UA Scope

- **User Management**
  - User Roles not standardized: server-specific or in companion specifications
  - No rules for password policies
  - Authentication mechanisms not addressed (ex. biometric authentication)
- **Data Ownership**
- **Organizational issues**
  - Physical access control, definition of zones, security lifecycle or security policies
  - Personnel training
- **These are addressed by other specifications** like
  - IEC 62443 (ISA 99)
  - NERC CIP
  - Regulations and Corporate Standards
  - …

OPC UA Security

Testing & Evolution

OPC UA Security evaluated by German Federal Office for Information Security (BSI)

Threats according to OPC UA Part 2

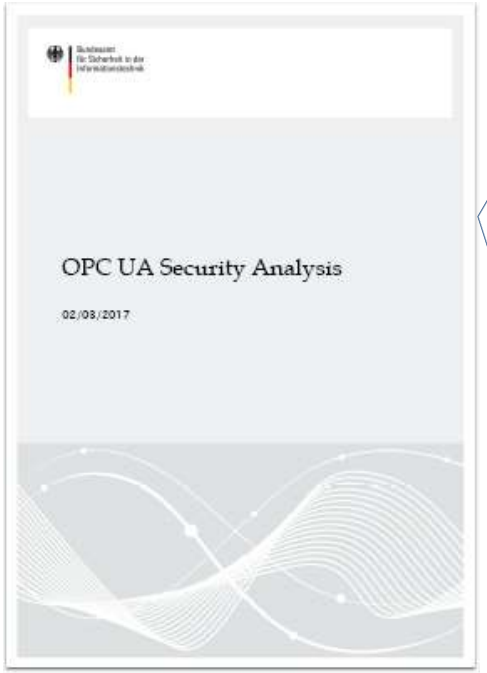
	Authentication	Authorization	Confidentiality	Integrity	Auditability	Availability
Message Flooding						X
Eavesdropping			X			
Message Spoofing		X		X		
Message Alteration		X		X		
Message Replay		X				
Malformed Messages				X		
Server Profiling	X	X	X	X	X	X
Session Hijacking	X	X	X			
Rogue Server	X	X	X		X	X
Compromising User Credentials		X	X			

Threats and Impact on Security Objectives

Examples of Attack Types Addressed

- **Message Flooding**
  - Minimize processing of packets before they are authenticated
- **Eavesdropping** – record and capture packets
  - Encryption
- **Message Spoofing** – attacker forges messages from client/server
  - Message signing, valid Session ID, Channel ID, timestamp, …
- **Message Alteration & Replay** – messages captured, modified, resent
  - Session IDs, *Secure Channel* ID, Timestamps, Sequence# and Request IDs
- **Malformed Messages**
  - Validating message structure and valid parameter values or discard
- **Server Profiling, Session Hijacking**, etc…

Effectiveness of OPC UA Measures



security-Mode	Layer or Service	Denial of Service	Eaves-dropping	Message Spoofing	Message Alteration	Message Replay	Malformed Messages	Server Profiling	Session Hijacking	Rogue Server	Compromising User credentials	Repud-iation
None												
Sign												
SignAndEncrypt												

: no protection

: low protection

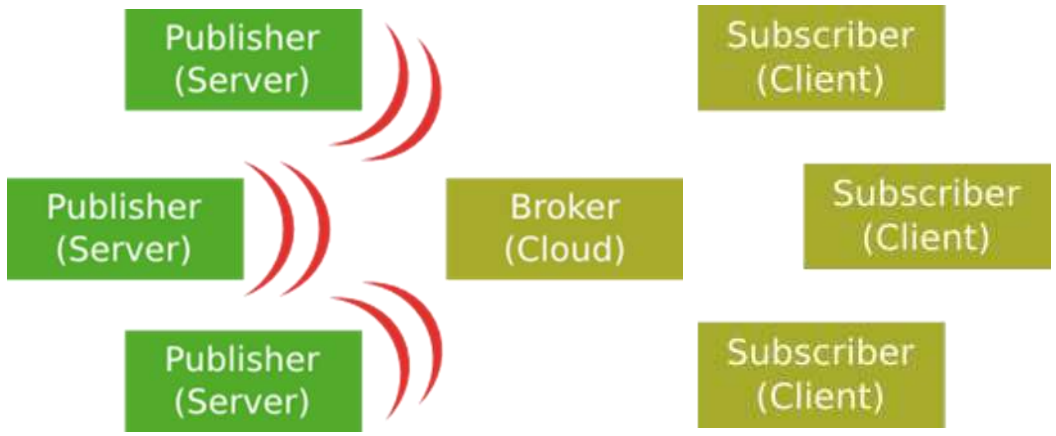
: Protection which restricts the possibilities of an attacker, but does not prevent this type of attack

: effective protection (attacks of this type require cryptographic attacks)

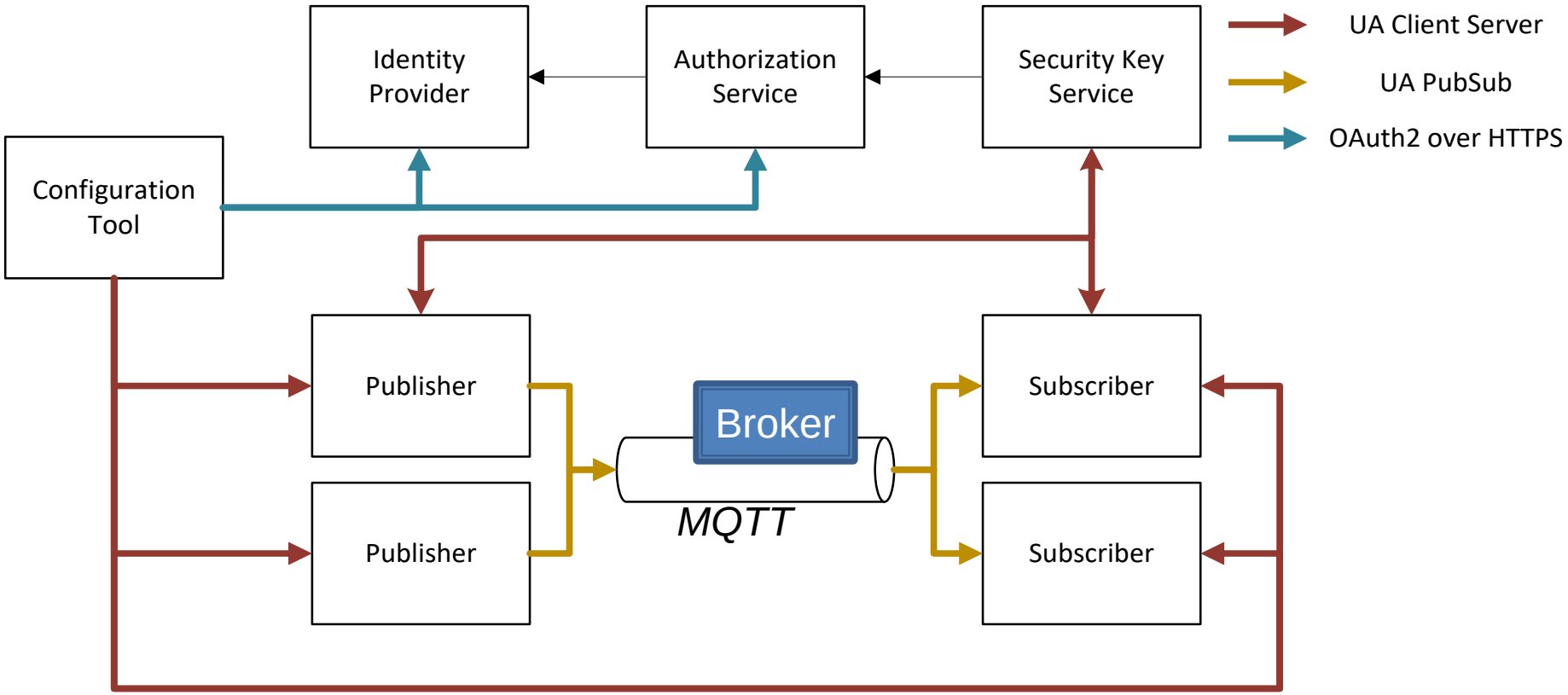
Source: BSI, “OPCUA Security Analysis” (02/03/2017)

New Security related features in 1.04

- Pub / Sub
  - JSON Web Token (JWT)
- Roles & Claim Based security
- Security Management
- Session-less Service calls
- ReverseHello

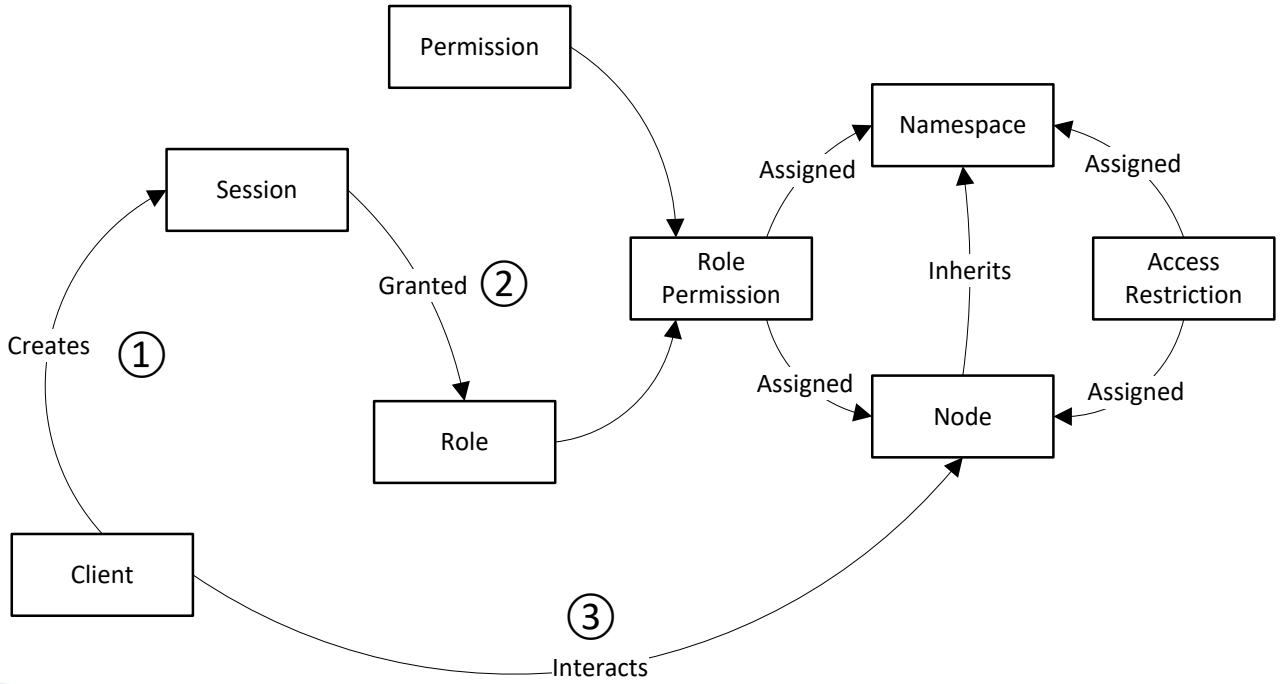


PubSub Security Overview

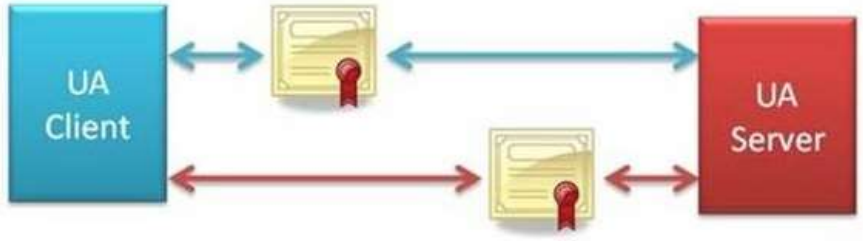


Role Based Security (C/S)

- Roles are assigned Permissions on Nodes;
- Sessions are granted Roles based on credentials;
- Access to Nodes based on the Permissions granted to the Roles assigned to the current Session;



Conclusion



OPC UA is secure-by-design:

- Implements CIA
  - **Confidentiality** and **Integrity** by signing and encrypting messages
  - **Availability** by minimum processing before authentication
- Implements AAA
  - **Authentication** and **Authorization** of Users and Application instances
  - **Auditability** by defined audit events for OPC UA operations
- Facilitates use of different levels of security to match application/hardware
- OPC UA continually evolving to meet new threats and capabilities

Use of OPC UA security enhances overall system security (defense in depth)

OPC Day Seminar: 13:00-17:30 Meeting room 203, 2nd floor

atvise®

BECKHOFF

NAPCON

kepware

NOVOTEK

PROSYS OPC

SIEMENS
Ingenuity for life

Unified Automation

Valmet
FORWARD