Forging Trustworthy IIoT Systems Using OPC UA

Thomas Burke
President, OPC Foundation

Darek Kominek
Marketing Manager, Matrikon (Honeywell)
OPC Foundation Mission Statement

The mission of the OPC Foundation is to manage a global organization in which users, vendors and consortia collaborate to create data transfer standards for multi-vendor, multi-platform, secure and reliable interoperability in industrial automation.
Connectivity without Interoperability

Data connectivity alone not enough to realize full IIoT potential.
OPC Vision: Facilitating Industrial Interoperability
OPC UA
OPC Foundation: Board of Directors

- International board – democratic elections by members every year
  - Companies from Automation & IT
  - All over the world
OPC Foundation: Membership

- An International Organization
  - Companies from Automation & IT
  - International standard IEC62541
OPC Foundation: Class A members
OPC UA: Enabling Standards Body Collaboration

Oil & Gas
Utilities
Pharmaceutical

Building Automation
Manufacturing
Mining
“The only communication technology for industrial environments that I currently know of which provides integrated security functionality and also offers performance potential to tackle the challenges of Industrie4.0 is OPC UA.”

Holger Junker
Head of Cyber-Security in Critical IT-Systems
German Office for Information
OPC UA In The IIoT Context
OPC UA – Paving the way for the IIoT
### IIoT & I4.0

- IIoT systems affect all aspects of a business so must be considered from multiple viewpoints (example from IIRA):

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>- Business Value &amp; ROI</td>
</tr>
<tr>
<td></td>
<td>- Cost of Maintenance</td>
</tr>
<tr>
<td>Usage</td>
<td>- New device registration in plant and cloud system</td>
</tr>
<tr>
<td></td>
<td>- How information is accessed, users added</td>
</tr>
<tr>
<td>Functional</td>
<td>- Component Interoperability in and across five functional domains:</td>
</tr>
<tr>
<td></td>
<td>- Control, Operations, Information, Applications, and Business</td>
</tr>
<tr>
<td>Implementation</td>
<td>- Architecture, component distribution, topology</td>
</tr>
<tr>
<td></td>
<td>- interfaces, protocols, behaviors, etc.</td>
</tr>
</tbody>
</table>

- Few standards meet the core connectivity standard criteria set out in IIRA
  - OPC UA is a core connectivity standard (IIRA)
  - OPC UA is the main connectivity standard for I4.0 (RAMI)
Frameworks offer a structured, systematic way to discuss and evaluate solutions for IT and OT convergence.

- Seamless, reliable, and cost effective system interoperability is crucial to IIoT
OPC UA: A Core IIRA Connectivity Standard

Source: Industrial Internet Consortium (www.iiconsortium.com)
OPC UA Meets The Requirements

- Number of Core Data Standards kept as small as possible to minimize complexity

CRITERIA EXAMPLES:
- Syntactic Interoperability
- Secure
- Performant
- Scalable
- Reliable
- Resilient
- Open Standard
- International Adoption
- Vendor Agnostic
- SDKs Available
  (Open Source + Commercial)

Source: Industrial Internet Consortium (www.iiconsortium.com)
Data Security

Key Concepts
With Connectivity Comes the Need for Security

- Industrial Control System (ICS) Cyber attacks are accelerating

Stuxnet - Iran, 2010

Crash Override - Ukraine, 2016
Trustworthiness: Key System Characteristics

Safety | Security | Resilience | Reliability | Privacy
Data Security

Data at Rest

Data in Process

Data in Motion
Key Security Concepts

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

- Access Control (AAA principle)
  - Authentication
  - Authorization
  - Accounting (Auditability)
OPC UA
Secure by Design
## OPC UA: Secure By Design

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Concepts</td>
<td>8) Data Access</td>
</tr>
<tr>
<td>2) Security Model</td>
<td>9) Alarms and Conditions</td>
</tr>
<tr>
<td>3) Address Space Model</td>
<td>10) Programs</td>
</tr>
<tr>
<td>4) Services</td>
<td>11) Historical Access</td>
</tr>
<tr>
<td>5) Information Model</td>
<td>12) Discovery</td>
</tr>
<tr>
<td>6) Mappings</td>
<td>13) Aggregates</td>
</tr>
<tr>
<td>7) Profiles</td>
<td>14) PubSub</td>
</tr>
</tbody>
</table>

**Red:** directly relevant for IT security
Solid Security Foundation

- OPC UA addresses the core security aspects:

  **Client-Server Architecture**

  **OPC UA Client**
  - Application Layer
    - User Authorization
    - User Authentication
  - Communication Layer
    - Confidentiality
    - Integrity
    - App Authentication
  - Secure Channel
  - Transport Layer

  **OPC UA Server**
  - Application Layer
    - User Authorization
    - User Authentication
  - Communication Layer
    - Confidentiality
    - Integrity
    - App Authentication

  **Publish-Subscribe Architecture**

  - Identity Provider
  - Authorization Service
  - Security Key Service
  - Publisher
  - Subscriber
  - AMQP MQTT
  - OAuth2 over HTTPS
Layered Communications

- Layered conceptual communication model

OPC UA Client

Application Layer

Communication Layer

Transport Layer

OPC UA Server

Application Layer

Communication Layer

Transport Layer

Software Authentication
User Authentication
User Authorization

Execute UA Functions

App Authentication
Encryption, Signing

Protect message

TCP, HTTPS
Binary, XML
Encoding/Decoding

Transfer message

Allow to choose appropriate abilities to meet various requirements

- Level 3 Apps: Internet accessibility and Security (e.g. HTTP & XML, E & S)
- Level 2 Apps: High speed and Security (e.g. UA TCP & BIN, S)
- Level 1 Apps: High speed and Small-footprint (e.g. UA TCP & BIN)
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,
  - 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
OPC UA Security
Assessment & Evolution
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…
# Threats according to OPC UA Part 2

<table>
<thead>
<tr>
<th></th>
<th>Authentication</th>
<th>Authorization</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Auditability</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Flooding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Message Spoofing</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Alteration</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Replay</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malformed Messages</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Server Profiling</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Session Hijacking</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue Server</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Compromising User</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

## Threats and Impact on Security Objectives
# Effectiveness of OPC UA Measures

<table>
<thead>
<tr>
<th>security-Mode</th>
<th>Layer of Service</th>
<th>Denial of Service</th>
<th>Eavesdropping</th>
<th>Message Spoofing</th>
<th>Message Alteration</th>
<th>Message Replay</th>
<th>Malformed Messages</th>
<th>Server Profiling</th>
<th>Session Hijacking</th>
<th>Rogue Server</th>
<th>Compromising User credentials</th>
<th>Repudiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sign</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SignAndEncrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Red**: no protection
- **Orange**: low protection
- **Yellow**: Protection which restricts the possibilities of an attacker, but does not prevent this type of attack
- **Green**: effective protection (attacks of this type require cryptographic attacks)

Source: BSI, “OPCUA Security Analysis” (02/03/2017)
New Security related features in 1.04

- PubSub
  - JSON Web Token (JWT)
- Roles & Claim Based security
- Security Management
- Session-less Service calls
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)
Thank You.

Thomas Burke
thomas.burke@opcfoundation.org
OPC Foundation

Darek Kominek, P.Eng. (Alberta, Canada)
darek.Kominek@matrikonopc.com
Matrikon®