OPC UA

Understanding OPC Unified Architecture

OT Security Learning Series

Document 201 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

OPC Unified Architecture (OPC UA) is a platform-independent, service-oriented architecture for industrial communication. Developed by the OPC Foundation, it was designed to replace legacy OPC Classic and address its limitations, including security.

Information

OPC UA is increasingly adopted as the standard for Industry 4.0 and IIoT applications. Unlike most legacy protocols, it includes built-in security features—but proper configuration is essential.

1.1 OPC Classic vs OPC UA

Aspect	OPC Classic	OPC UA
Platform	Windows only (COM/DCOM)	Platform independent
Transport	DCOM (dynamic ports)	TCP, HTTPS, WebSockets
Security	Windows security only	Built-in encryption & auth
Firewall	Difficult (DCOM)	Simple (single port)
Data Model	Separate specs (DA, HDA, A&E)	Unified information model
Released	1996	2008

2 Architecture Overview

2.1 Communication Stack

OPC UA defines a layered communication architecture:

OPC UA Stack Layers

- **Application Layer:** Client/server application logic
- **Service Layer:** OPC UA services (Read, Write, Subscribe, etc.)
- **Security Layer:** Authentication, encryption, signing
- **Transport Layer:** TCP binary, HTTPS, WebSockets

2.2 Information Model

OPC UA uses a rich, object-oriented information model:

- **Nodes:** Basic building blocks (Objects, Variables, Methods)
- **References:** Relationships between nodes
- **Address Space:** Hierarchical namespace of all nodes
- **Companion Specs:** Industry-specific data models (e.g., for robotics, PLCs)

2.3 Communication Patterns

Pattern	Description
Client-Server	Traditional request-response model
Publish-Subscribe	Event-driven data distribution (OPC UA PubSub)

3 Security Features

3.1 Security Model

Key Point

OPC UA includes comprehensive security features:

- Authentication (user and application identity)
- Authorization (role-based access control)
- Confidentiality (encryption)
- Integrity (message signing)
- Auditability (event logging)

3.2 Security Modes

OPC UA defines three security modes:

Mode	Encryption	Signing	Use Case
None	No	No	Testing only (never in production)
Sign	No	Yes	Integrity without confidentiality
SignAndEncrypt	Yes	Yes	Full security (recommended)

Critical

Security Mode “None” disables all security. Unfortunately, many deployments use this mode for convenience, negating OPC UA’s security advantages.

3.3 Authentication Methods

- **Anonymous:** No authentication (not recommended)
- **Username/Password:** Basic credential authentication
- **X.509 Certificates:** Strong application and user authentication
- **Kerberos:** Enterprise SSO integration

3.4 Certificate Management

OPC UA relies heavily on X.509 certificates:

Certificate Trust Model

- Each application has its own certificate
- Clients and servers must trust each other's certificates
- Trust can be explicit (trusted list) or CA-based
- Certificate validation includes expiry, revocation, hostname

4 Security Concerns

4.1 Common Misconfigurations

Warning

Security features don't help if not properly configured:

- Security Mode set to "None"
- Anonymous authentication enabled
- Self-signed certificates without proper trust management
- Default or weak credentials
- Missing certificate revocation checks

4.2 Known Vulnerabilities

OPC UA implementations have had security vulnerabilities:

- **Stack implementations:** Buffer overflows, DoS vulnerabilities
- **Certificate handling:** Improper validation, path traversal
- **Authentication bypass:** Implementation-specific flaws

Tip

The OPC UA specification is complex. Implementation vulnerabilities are common. Keep OPC UA software updated and monitor security advisories.

4.3 Attack Scenarios

1. **Discovery abuse:** Enumerate servers and endpoints
2. **Downgrade attacks:** Force use of weaker security modes
3. **Certificate theft:** Steal private keys to impersonate applications
4. **DoS attacks:** Exhaust server resources with malformed requests
5. **Information disclosure:** Access sensitive process data

5 Security Best Practices

5.1 Configuration Hardening

- **Always use SignAndEncrypt** security mode
- **Disable anonymous access** – require authentication
- **Use strong security policies** (Basic256Sha256 or better)
- **Implement proper certificate management** with PKI
- **Enable audit logging** for security events
- **Apply least privilege** through role-based access

5.2 Network Security

- **Segment OPC UA traffic** in dedicated network zones
- **Use firewalls** to restrict access to OPC UA ports (4840)
- **Monitor traffic** for anomalous patterns
- **Consider additional encryption** (VPN) for cross-zone traffic

5.3 Operational Security

- **Keep software updated** – patch known vulnerabilities
- **Inventory all OPC UA endpoints** in your environment
- **Review security configurations** regularly
- **Test security settings** before deployment

6 Further Reading

Specifications

- **OPC Foundation** – OPC UA Specifications
  https://opcfoundation.org/developer-tools/specifications-unified-architecture
- **OPC UA Security Analysis** – BSI (German Federal Office)
  https://www.bsi.bund.de/EN/

Standards

- **IEC 62541** – OPC Unified Architecture (international standard)

- **IEC 62443** – Industrial Automation Security
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA** – ICS Advisories
  https://www.cisa.gov/news-events/ics-advisories