Latest News on OPC UA PubSub and Security Configuration

Matthias Damm
Executive Director, Unified Automation   **matthias.damm@unifiedautomation.com**

Editor OPC UA Part 4 – Services & Part 14 – PubSub
**Chairman OPC UA for Devices WG**
OPC Foundation Technical Control Board
OPC Foundation Board of Directors

News on OPC UA PubSub and Security Configuration

▸ Enhancements for OPC Unified Architecture
  ◦ Optimized release process
  ◦ 1.05.x releases

▸ Support for users of OPC Unified Architecture
  ◦ Harmonization Working Group
  ◦ Specifications, templates, guideline and best practice documents
  ◦ Standardization of configuration workflows

→ OPC Foundation continuously improves the OPC UA platform

Transition to Agile OPC UA Specification Development
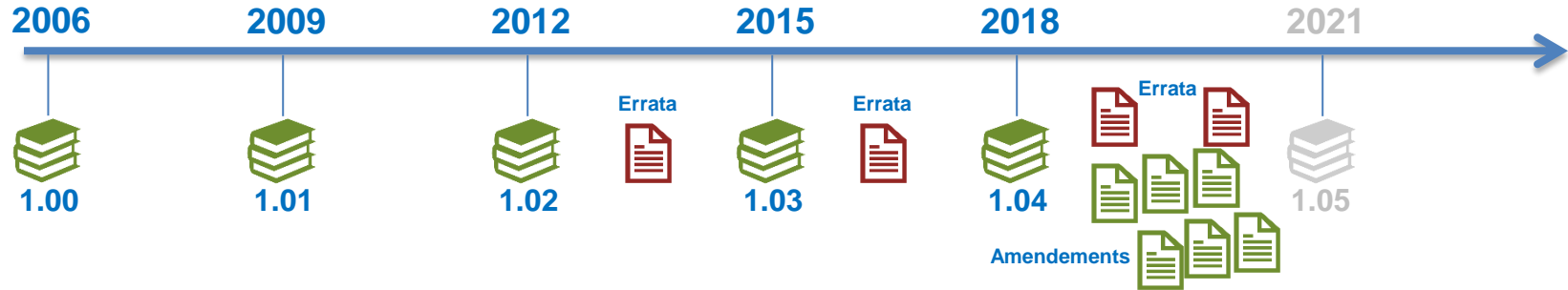
- ▸ OPC UA (OPC 10000) Specification Release Cycle is three years
- ▸ Errata handled as additional document since 1.02
- ▸ Minor enhancements are often requested short term
  - ◦ Companion working harmonization (common information model types)
  - ◦ TSN / 5G
  - ◦ Security
- ▸ OPC UA WG released Amendments to OPC UA 1.04
  - ◦ Enhancements as feature releases between major spec releases
  - ◦ Dedicated Amendment per feature
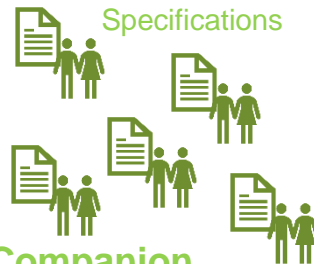
Harmonization Working Group

OPC UA

Specification

Based on OPC UA

Information Model Specifications

OPC UA Working Group

Requirements

Specifications

Common Definitions

Review

Requirements

Companion Working Groups

Members

Harmonization Working Group
(Started 2019)
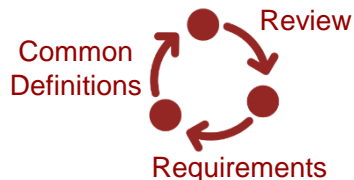
Tasks

- Review companion specifications
- Manage template for companion specifications
- Collect common features and feature requests
- Prepare information model drafts for common features
- Coordination integration of drafts in existing or new specifications

Membership

- OPC UA experts from OPC UA working group
- Representatives from all companion working groups

Version 1.05 start of continuous release process

▸ Further enhancement of release process
  ◦ Errata and amendments will be released as update to 1.05 with additional version number
  ◦ Initial release will be 1.05.0 – features and errata will be released as 1.05.x
  ◦ Only one document relevant for each OPC UA Part going forward
  ◦ Starting point for continuous update process including **online reference**
▸ New parts introduced as amendments to 1.04
  ◦ **10000-15 Safety**
  ◦ 10000-17 Aliases
  ◦ 10000-19 Dictionary References

OPC UA 1.05 Release Status

1.05.00 release completed (10/2021)

- Split of 10000-5 annex chapters to own Parts 10000-16 State Machines, 10000-18 Role-Based Security, 10000-20 File Transfer

**1.05.01 release completed (03/2022)**

- New 10000-22 Base Network Model
- New 10000-23 Common ReferenceTypes
- New features in 10000-14 (PubSub) for FLC/FX and QoS/TSN
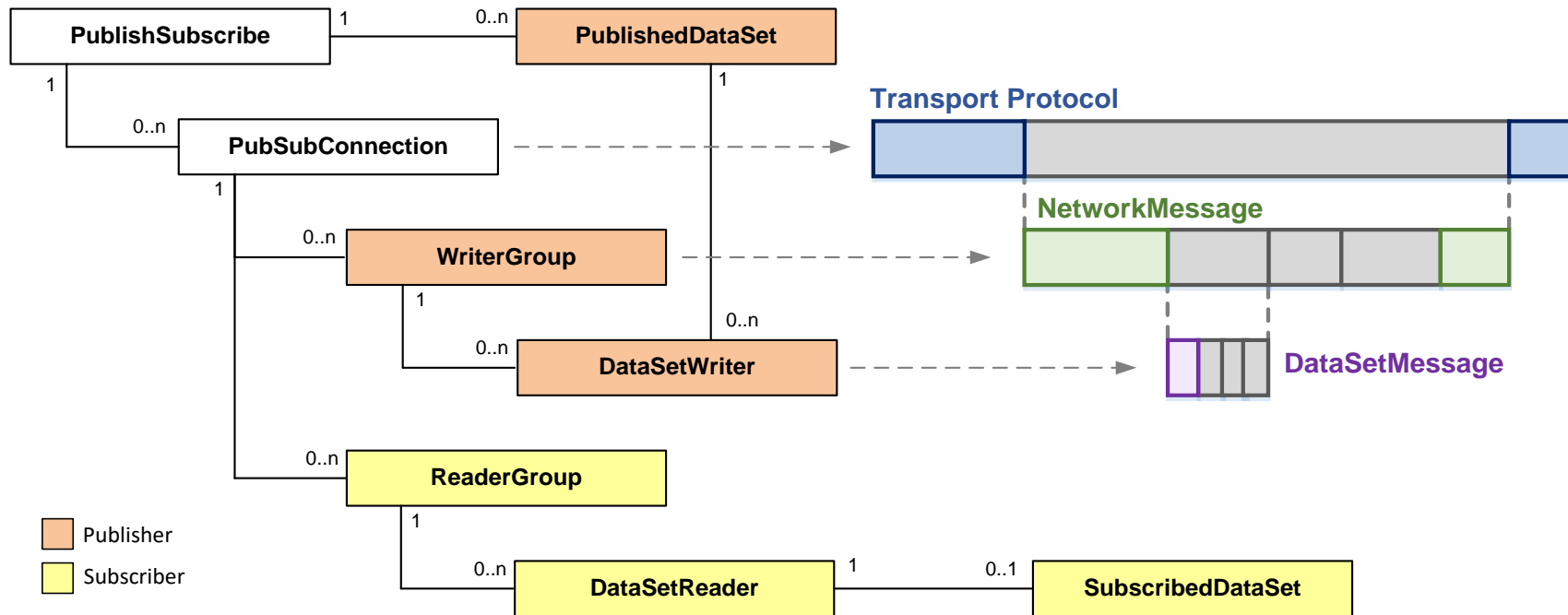
1.05.02 release completed (10/2022)

- With the 1.05.02 release, all Parts will have a 1.05 version except Part 11 Historical Access (scheduled for 1.05.03)
- New 10000-21 Device Onboarding
- New 10000-24 Scheduler
- Many clarifications and enhancements for 10000-12 (Discovery and Global Services)

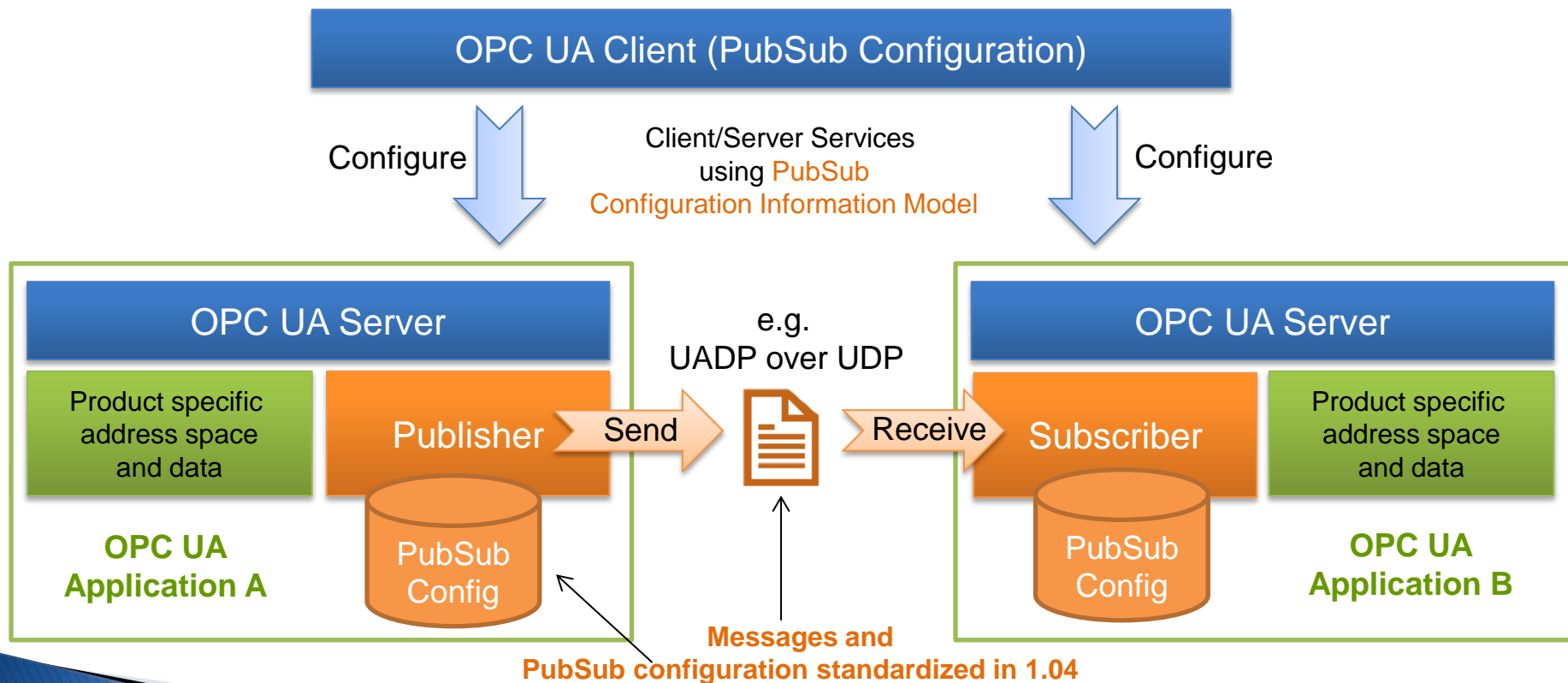| OPC Number	Title	1.03	1.04	1.05.00	1.05.01	1.05.02
10000-1	Part 1: Overview and Concepts	☑	☑	☐	☐	☑
10000-2	Part 2: Security	☑	☑	☐	☐	☑
10000-3	Part 3: Address Space Model	☑	☑	☑	☑	☑
10000-4	Part 4: Services	☑	☑	☑	☐	☐
10000-5	Part 5: Information Model	☑	☑	☑	☑	☑
10000-6	Part 6: Mappings	☑	☑	☑	☑	☐
10000-7	Part7: Profiles	☑	☑	☐	☐	☑
10000-8	Part 8: DataAccess	☑	☑	☑	☐	☐
10000-9	Part 9: Alarms and Conditions	☑	☑	☐	☑	☑
10000-10	Part 10: Programs	☑	☑	☐	☐	☐
10000-11	Part 11: Historical Access	☑	☑	☐	☐	☐
10000-12	Part 12: Discovery and Global Services	☑	☑	☐	☐	☑
10000-13	Part 13: Aggregates	☑	☑	☐	☐	☑
10000-14	Part 14: PubSub	☐	☑	☐	☑	☑
10000-15	Part 15: Safety	☐	☑	☑	☐	☑
10000-16	Part 16: State Machines	☐	☐	☑	☐	☑
10000-17	Part 17: Alias Names	☐	☑	☑	☐	☐
10000-18	Part 18: Role-Based Security	☐	☐	☑	☑	☑
10000-19	Part 19: Dictionary References	☐	☐	☑	☐	☑
10000-20	Part 20: File Transfer	☐	☐	☑	☑	☑
10000-21	Part 21: Device Onboarding	☐	☐	☐	☐	☑
10000-22	Part 22: Base Network Model	☐	☐	☐	☑	☑
10000-23	Part 23: Common ReferenceTypes	☐	☐	☐	☑	☑
10000-24	Part 24: Scheduler	☐	☐	☐	☐	☑

OPC UA PubSub Communication Model
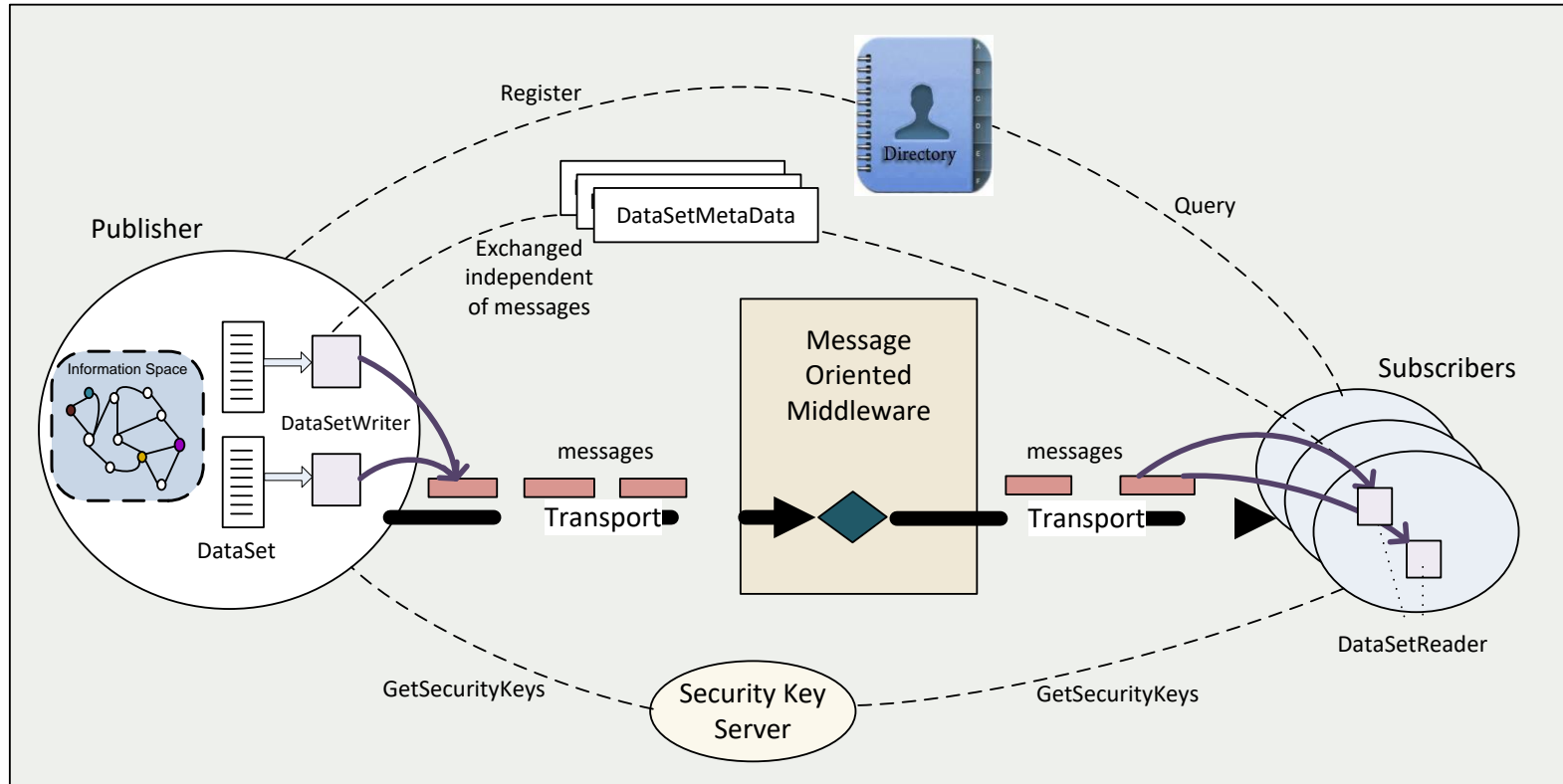
OPC UA PubSub Configuration and Messages

OPC UA PubSub Configuration

OPC UA Client (PubSub Configuration)

Configure

Client/Server Services
using PubSub
Configuration Information Model

Configure

OPC UA Server

Product specific address space and data

Publisher

PubSub Config

OPC UA Application A

Send

e.g.
UADP over UDP

Receive

OPC UA Server

Subscriber

PubSub Config

Product specific address space and data

OPC UA Application B

**Messages and
PubSub configuration standardized in 1.04**

Enhanced OPC UA PubSub Configuration

Requirements for configuration enhancements

- Easy read access to complete configuration
- Consistent read access
- Delta changes without communication interruption
- Modifications as one consistent and atomic change

Enhanced configuration

- Configuration access uses OPC UA FileType with OPC UA Binary encoded PubSub configuration
- Read transfers the complete PubSub configuration
- Write transfers partial configuration and a change list Options: Add, Modify, Remove

- Mechanism with partial configuration and change list is also used by OPC UA FX
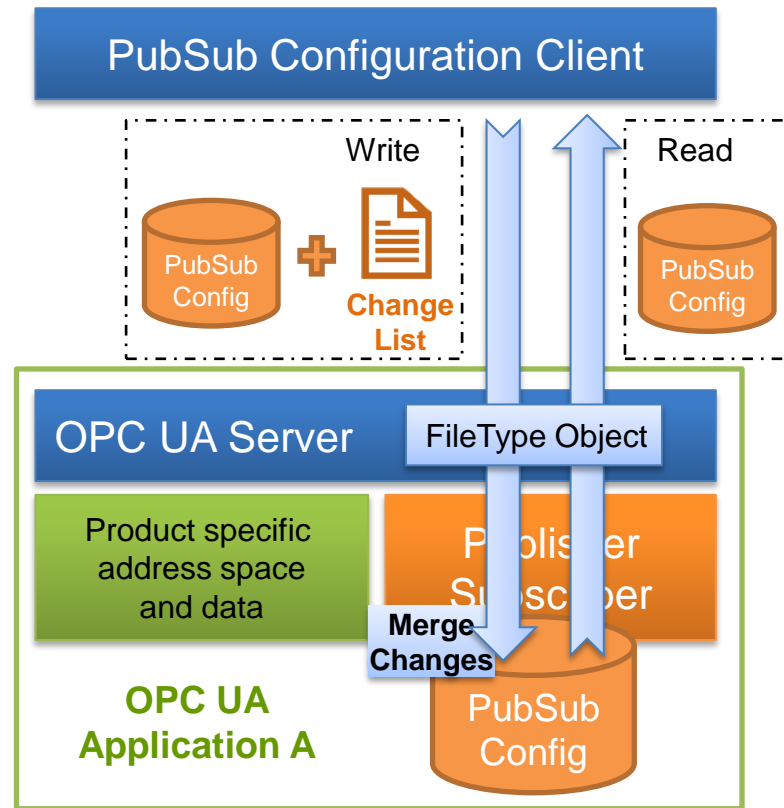
GDS for OPC UA Security Management

10000-12 Discovery and Global Services (GDS)

- OPC UA Application registration for managed applications and discovery
- Central certificate and trust management for OPC UA Applications
- Initial rollout and automatic update from central GDS application
- Interaction GDS to OPC UA Clients with Pull and OPC UA Servers with Push

Standard Security Management Model Implemented

- Multivendor Demo at trade shows
  GDS from Unified Automation, PLCs from Beckhoff and Siemens, device Leuze
- Testing at interoperability test events
- Integrated in OPC UA SDKs → easy integration in OPC UA Applications

Enhancements 10000-12

- Input from multiple application side GDS implementations and interop tests
- Detailed definition of rollout and update workflows
- Enhancement of update transactions

New: Secure Device Onboarding

Device Lifecycle

Not covered by 10000-12

‣ Secure initial identification of devices
‣ Secure device onboarding

New 10000-21 – Device Onboarding

‣ Definition of device identity provided by the device
‣ Definition of a ticket format provided by the device vendor
‣ Device authentication and validation with ticket
‣ Secure device onboarding with GDS (10000-12)

Final Goals

‣ **Secure and standardize all steps of device and application security configuration and management**
‣ **Standardize not only communication, also configuration necessary to operate a multi-vendor OPC UA environment**
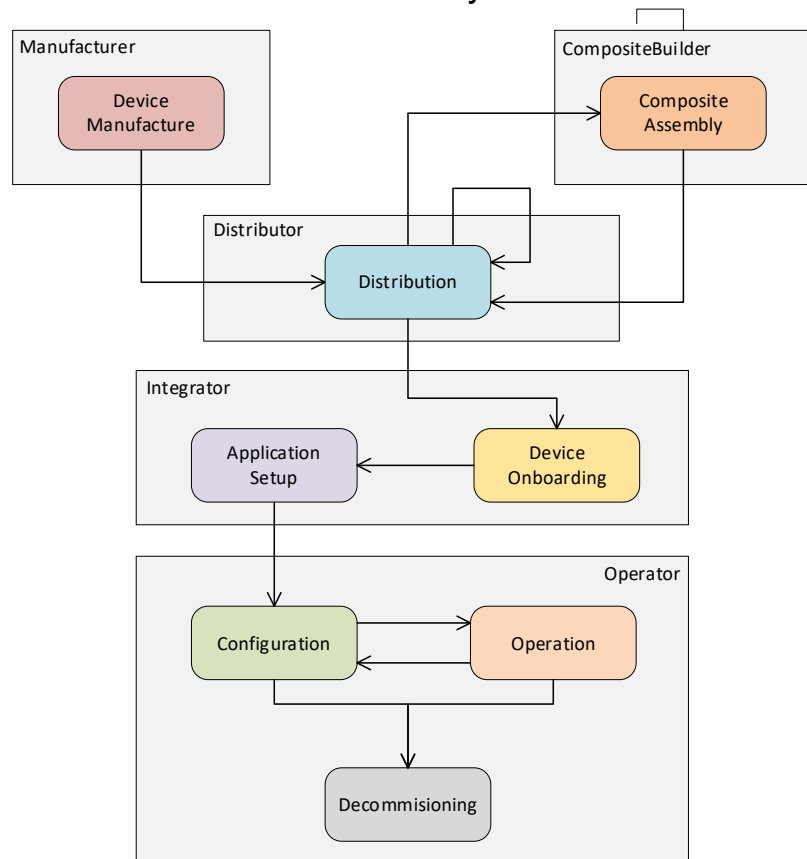
OPC UA Ecosystem

- Stable and established IIoT platform as base for many information model WGs
- Continuous improvement based on feedback and input from information model WGs
- Features for secure device lifecycle and standardized configuration

OPC 10000 – Unified Architecture

10000-1 Overview	10000-2 Security	10000-3 Address Space	10000-4 Services	10000-5 Information Model
10000-6 Mappings	10000-7 Profiles	10000-8 Data Access	10000-9 Alarms Conditions	10000-10 Programs
10000-11 Historical Access	10000-12 Global Services	10000-13 Aggregates	10000-14 PubSub	10000-15 Safety
10000-16 State Machines	10000-17 Alias Names	10000-18 Role-Based Security	10000-19 Dictionary References	10000-20 File Transfer
10000-21 Device Provisioning	10000-22 Base Network Model	10000-23 Common Reference Types	10000-24 Scheduler	

10000-100 Device Model	10000-110 Asset Management Basics	10000-200 Industrial Automation Model	10000-210 Relative Spatial Location

11020 – UA Companion Specification Template	11021 – UA Companion Specification Guideline	11030 – OPC UA Modeling Best Practice	11050 – Working Group Charter Template	11051 Working Group Guidelines

Legend:
- Existing
- New
- Restructured
- Helper documents