PROSYS OPC

OPC UA (Unified Architecture)

Jouni.Aro@prosysopc.com

10.11.2015

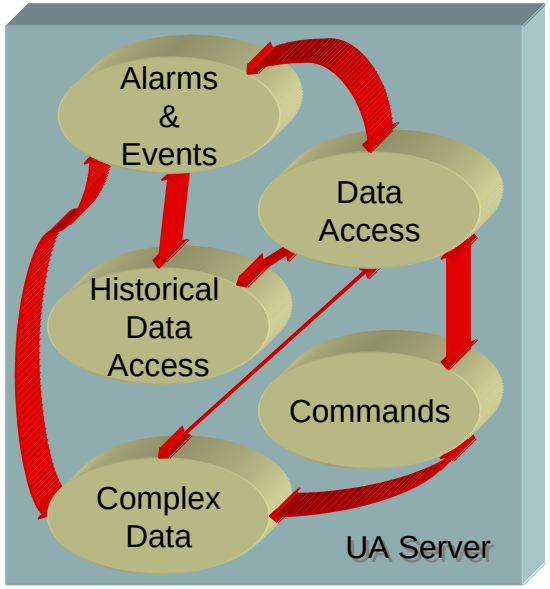
Microsoft Partner ORACLE PARTNER BECKHOFF Partner OPC FOUNDATION MEMBER

Contents

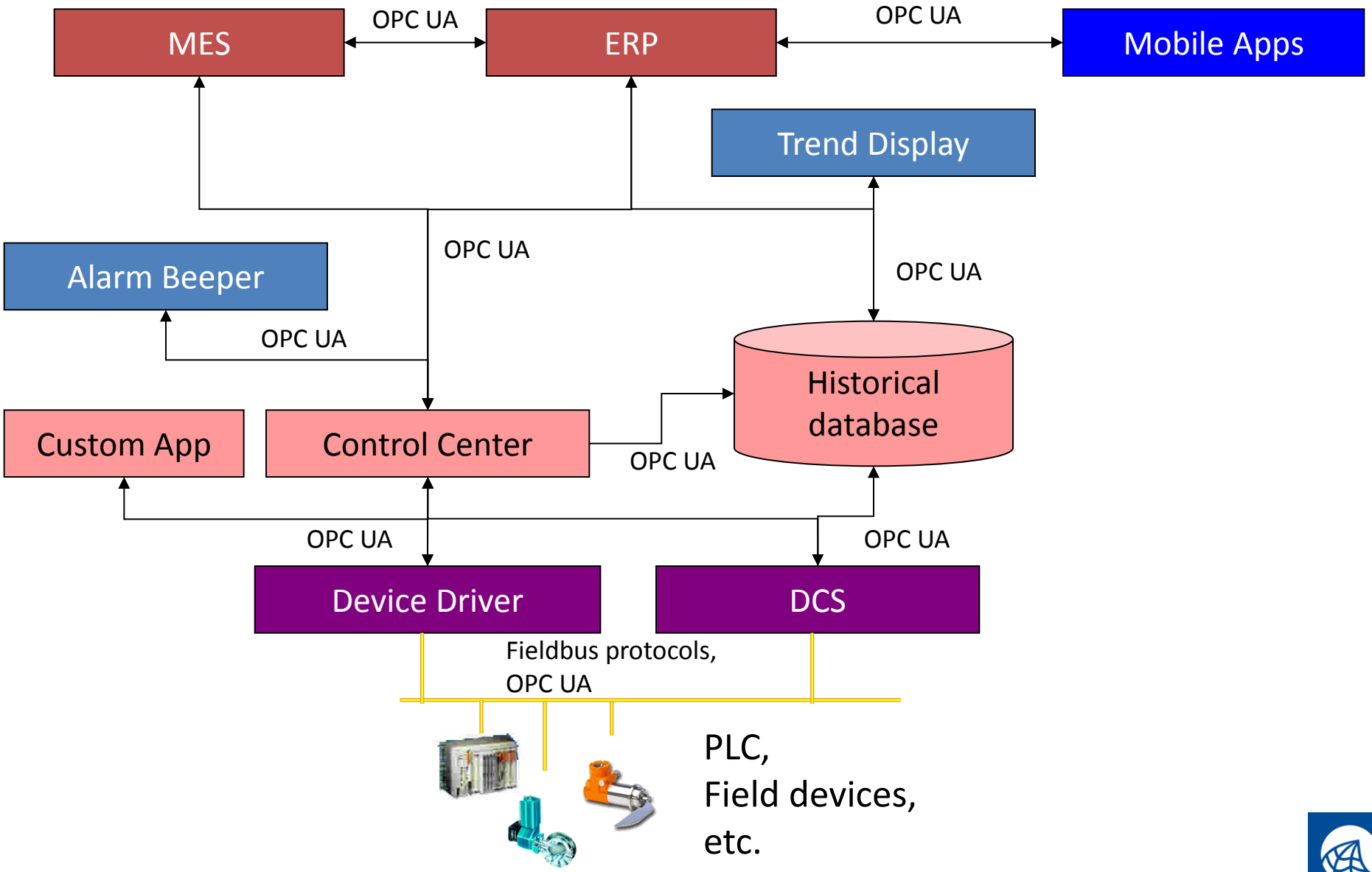
- 1. OPC Unified Architecture
- 2. Applications
- 3. Specification
- 4. Information Models
- 5. Communication Model
- 6. Development / Usage

1. OPC Unified Architecture

- New generation of OPC
- Replaces DCOM communication specific TCP/IP protocols
  - Enables OPC in any OS and language
  - Enables OPC in devices (embedded software)
  - Enables WAN (Secure Internet/Intranet/Extranet)
  - Improves Security Management
- Combines all previous protocols to a common (unified) data model
- Standardised 2011 as IEC 62541

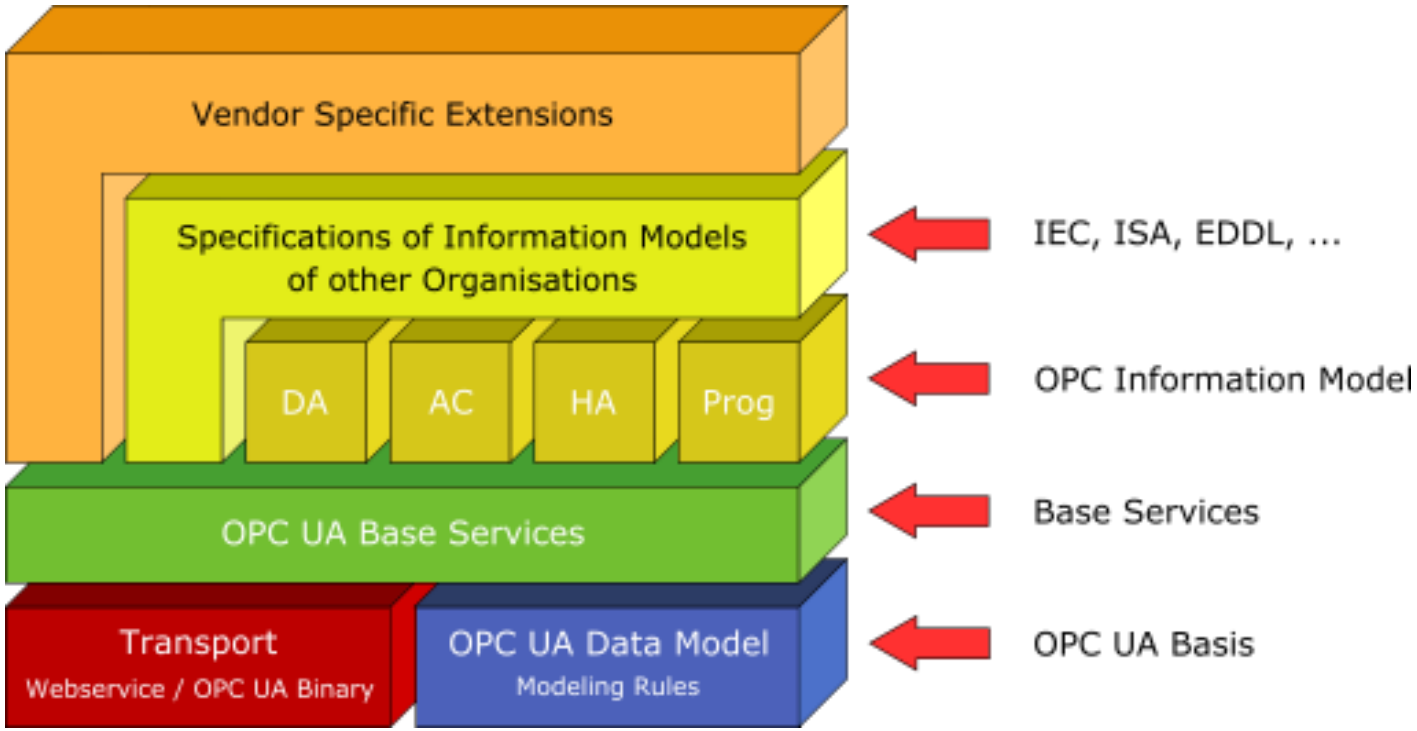


2. Applications



3. Specification

- Layered design



3.1 Base Specifications

- Part 1 – Concepts
  - A short white-paper like overview of UA
- Part 2 – Security
  - A non-normative introduction to the threats and countermeasures
- Part 3 – Address Space Model
  - Building block constructs of UA (Nodes, Objects, Events …)
- Part 4 – Services
  - Service methods exposed by UA Servers and called by UA Clients
- Part 5 – Information Model
  - UA defined objects (e.g. Diagnostic Object, Audit Events)
- Part 6 – Mappings
  - Details that allow implementation on current technology (e.g. UA Binary, HTTPS)
- Part 7 – Profiles
  - Defines conformity groups for implementation and certification

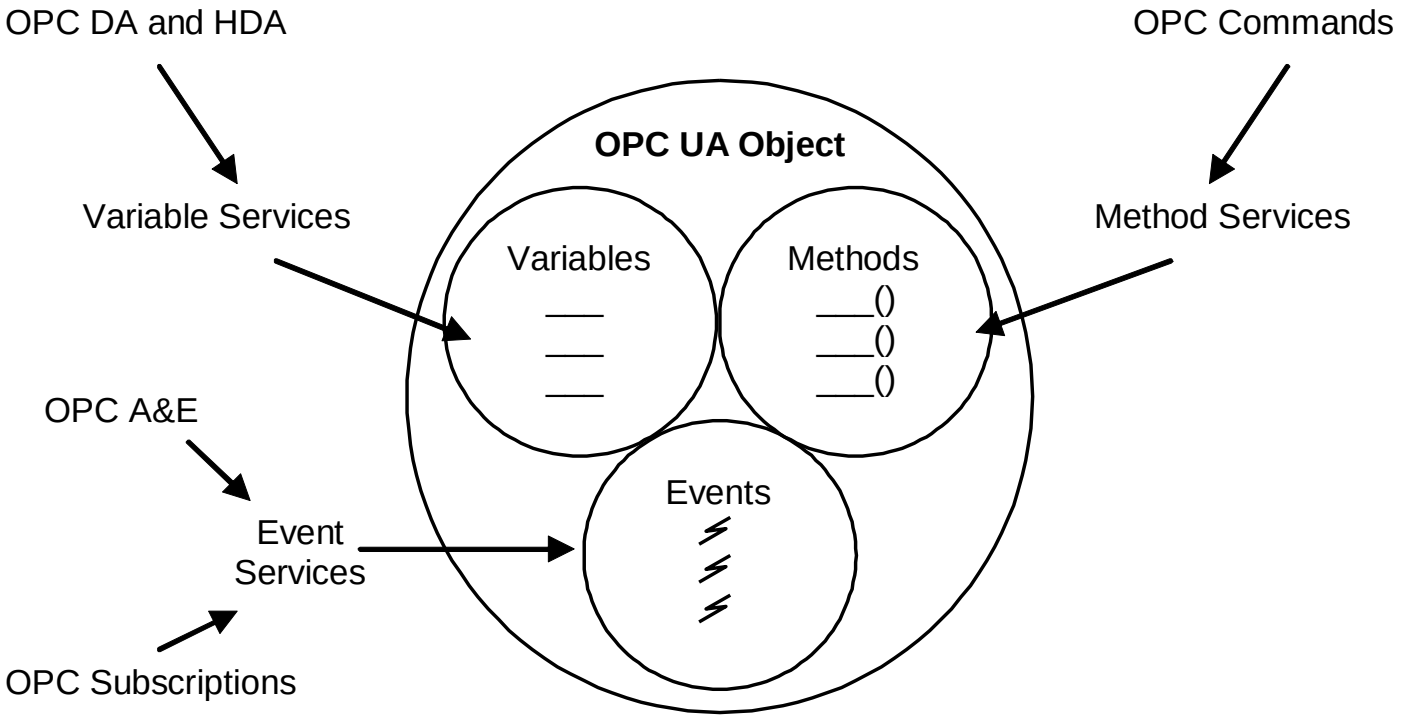
3.2 Information Model Specifications

- Part 8 – Data Access
  - Adds OPC-DA constructs (e.g. Engineering Units, Ranges…)
- Part 9 – Alarms and Conditions
  - Adds stateful Alarm and Condition types
- Part 10 – Programs
  - Adds long running executable entities
- Part 11 – Historical Access
  - Adds Historical Data and Event constructs
- Part 12 –Discovery
  - Details about UA Discovery Servers and interaction with UA apps
- Part 13 – Aggregates
  - Aggregating functions for e.g. Historical Data

3.3 Companion specifications

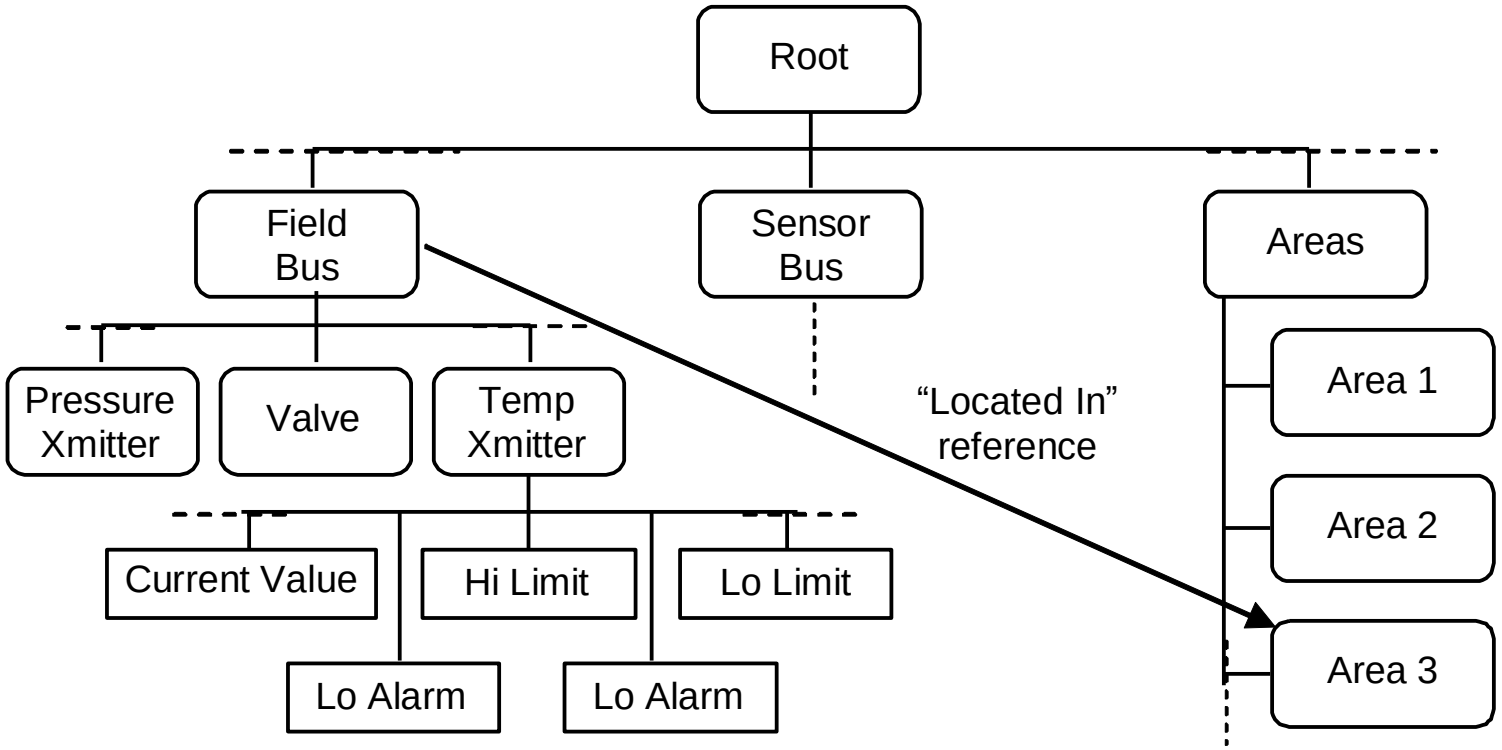
- OPC UA For Devices (DI)
  - Common model for devices and components
- OPC UA For Analyser Devices (ADI)
  - Information model for analysers (spectrometers, chromatographs, etc)
- OPC UA For IEC 61131-3 (PLCopen)
  - Information model for PLC devices
- OPC UA For ISA95
  - Information model for MES/ERP data
- BACNet, AutomationML, AutoID, MDIS, etc.

4. Basic Information Model



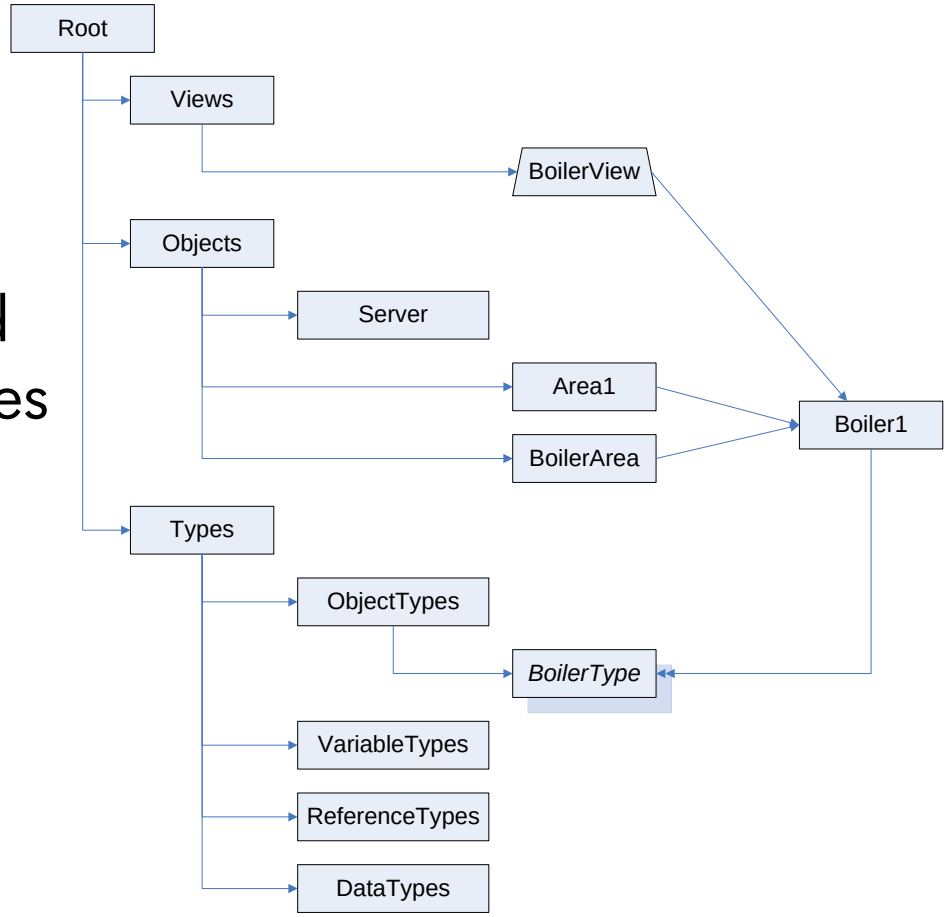
4.1 Address Space

- Combines the old DA & AE address space information
- Network, Plant & other hierarchies available at the same time

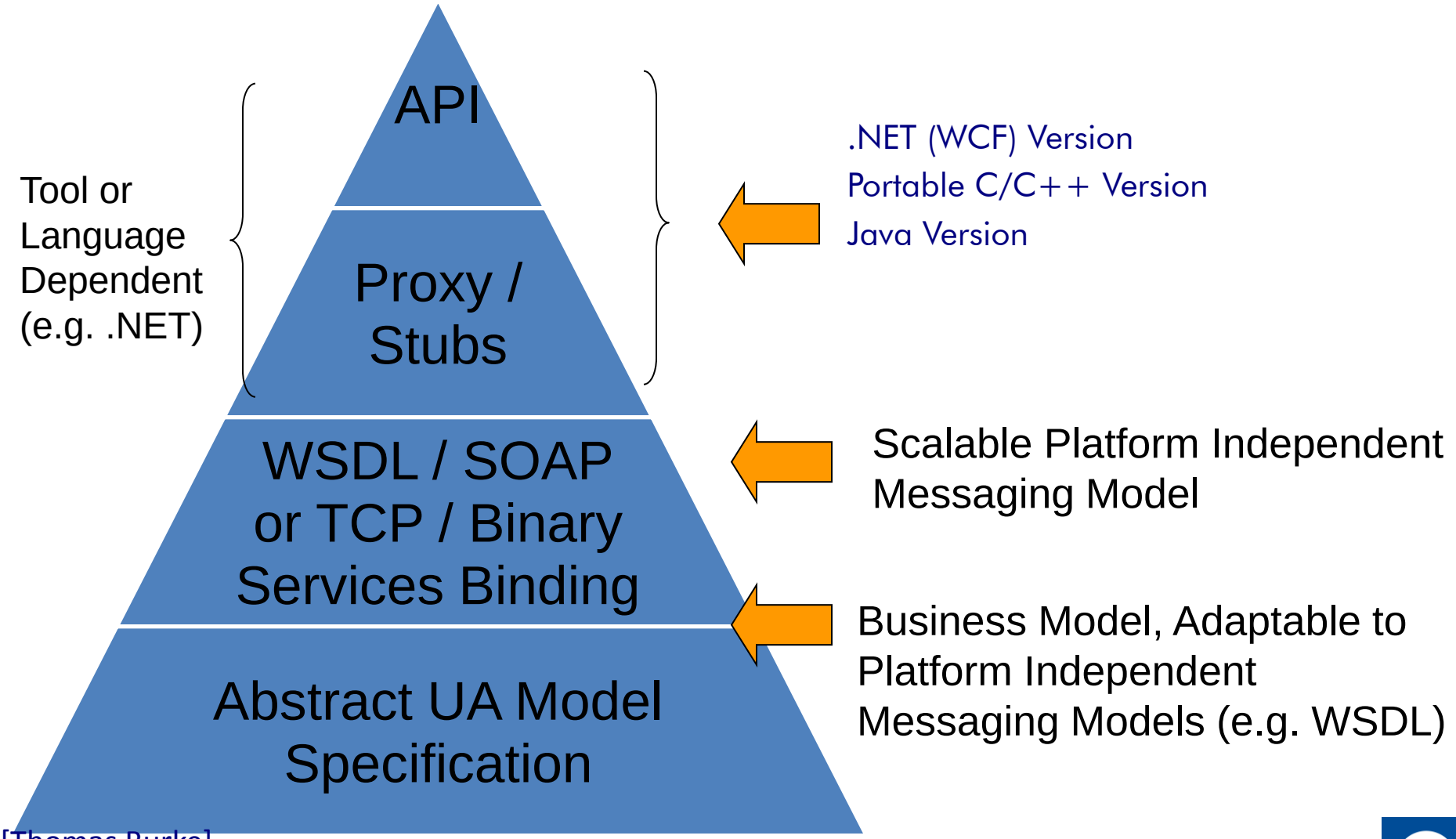


4.2 Type Information

- Servers also declare supported data types in the address space
- Servers may define custom data types
- Standard information models can be defined in server address spaces
  - FDT
  - PLCopen
  - ISA S95/88
  - MIMOSA
  - …



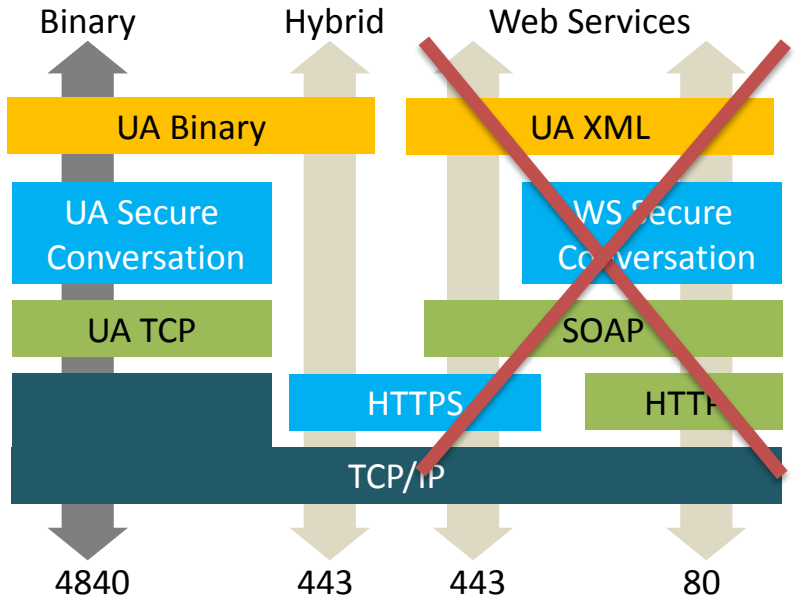
5. Communication Model



[Thomas Burke]

5.1 Protocols

- Transport
  - TCP/IP
  - HTTPS (New: 1.02)
  - HTTP
- Messaging
  - UA TCP, optimized binary protocol
  - HTTPS, binary/XML encapsulated in standard HTTP
  - SOAP, generic messaging (Deprecated: 1.03)
- Message Security
  - UA Security (UA TCP)
  - TLS Security (HTTPS)
  - Web Service (WS) Security
- Message encoding
  - UA Binary
  - UA XML
- Open for additional protocols in future



(IP Port numbers not fixed)

5.2 Security

- OPC Unified Architecture includes full public key based security features in OPC clients and servers
  - Authentication of client & server applications by X.509 certificates
  - Authentication of users by X.509 certificates or UserName/Password or external tokens
  - Optional message signing & encryption
- Binary and HTTPS communication via one (configurable) TCP/IP port, which can be opened in Firewalls as necessary
- Alternative security algorithms defined for signing and encryption
- HTTPS protocol enables standard TLS security applied
- OPC UA Proxy and Wrapper components can be used to "tunnel" DCOM-based OPC traffic securely

5.3 Robustness

- Keep-alive (heartbeat) messages
  - Clients can detect a connection failure
- Life-time monitoring
  - Servers can detect connection failures
- Message buffering
  - Clients can detect missing data
  - Missing messages can be re-requested
- Redundancy support
  - Can be built to both clients and servers

6.1 Server Profiles

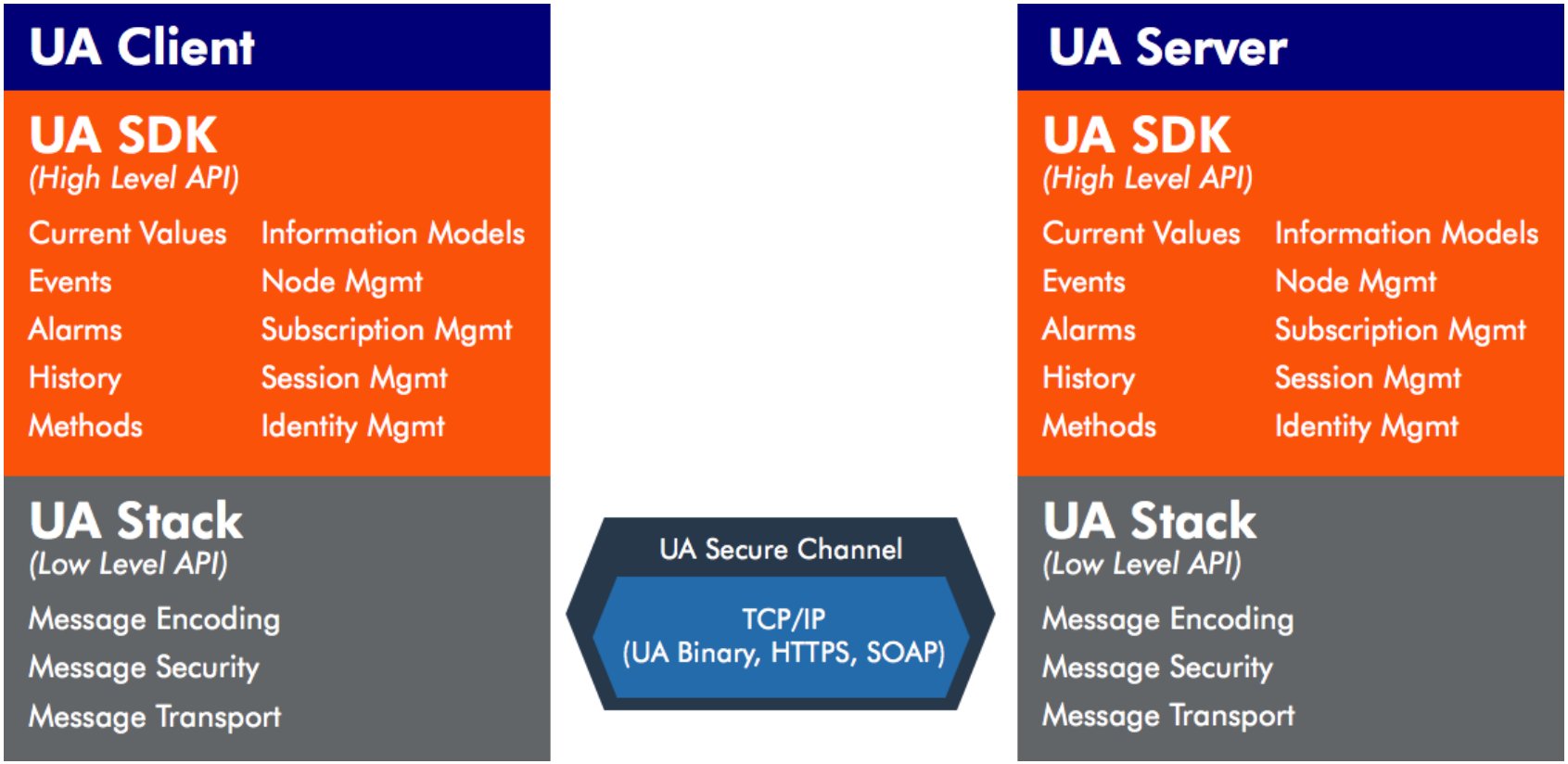
- OPC UA Profiles defined to allow clients and servers with different capability levels
- Applications define which profiles they support, e.g.:
  - Subscriptions
  - Security
  - Redundancy
  - Data Access
  - Alarms & Conditions
  - Historical Access
- Compliance testing verifies applications against the supported profiles
- End-users can purchase products that include the functionality they need by looking at the supported and certified profiles

6.2 Development Platforms

- AnsiC
  - UA Binary communication
  - HTTPS communication
  - Open SSL Security
  - Platform specific parts (Windows, Linux, etc)
  - SDKs for C/C++ (Unified Automation, Softing)
- .NET
  - UA Binary communication
  - HTTPS communication
  - (HTTP/SOAP communication with WS Security)
  - .NET Security
  - SDKs for .NET (Unified Automation, Softing, etc.)
- Java
  - UA Binary communication (pure Java)
  - HTTPS communication
  - Java Security
  - SDK for Java from Prosys

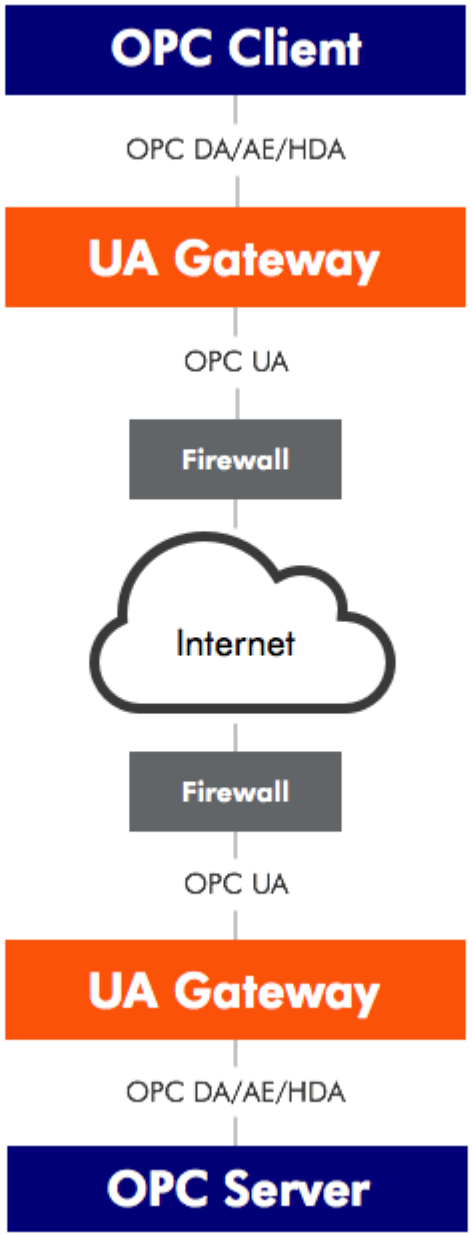
6.3 Application capabilities

- Communication Stacks provide interoperable communication
- SDKs provide standard implementation of UA services



6.4 UA & DCOM

- Smooth transfer of application technology from DCOM OPC to UA should not be a problem
- UA Proxy & Wrapper components enable communications between UA and DCOM versions of OPC applications
- UA Gateway
  - commercial implementation



References, literature

- OPC Foundation: Unified Architecture, http://www.opcfoundation.org/
- Mahnke, Leitner, Damm: OPC Unified Architecture, 2009, ISBN 3-540-68898-6

Prosys PMS Ltd

Tekniikantie 14, 02150 Espoo, Finland

Phone: +358 9 420 9007

Emails

- Team: firstname.lastname@prosysopc.com
- Sales: sales@prosysopc.com
- Technical support: support@prosysopc.com
- General inquiries: info@prosysopc.com

www.prosysopc.com

PROSYS OPC