

The Siemens logo is displayed in a white rectangular box in the top right corner of the image. The background of the entire image is a blurred industrial factory floor with two men in business attire looking over a railing. Overlaid on the image are various digital graphics, including binary code (0s and 1s) and a central blue hexagonal icon containing the text 'OPC UA', a waveform, a bar chart, and a padlock symbol.

SIEMENS

Simatic S7-1500 OPC UA server

Duben 2022

www.siemens.cz

Obsah prezentace

SIEMENS

1. OPC UA

TCP, server&klient, read&write/subscription

2. Přehled OPC UA v Siemens portfoliu

Hardware a software

Limity, licence

3. Adresní prostor

Koncept adresního prostoru, reference

4. Přístup k datům

5. Komunikační relace

6. Parametry serveru

7. Bezpečnost

8. Výkon - optimalizace

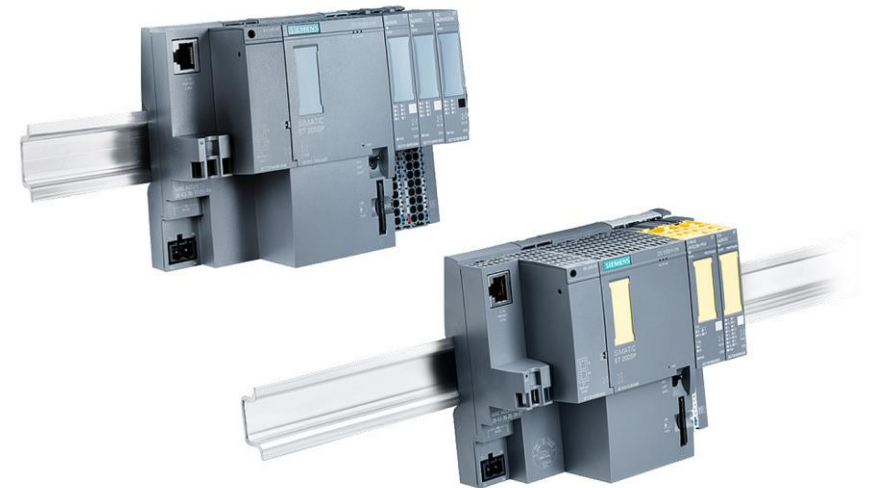
Alarms and conditions / metody

9. Diagnostika

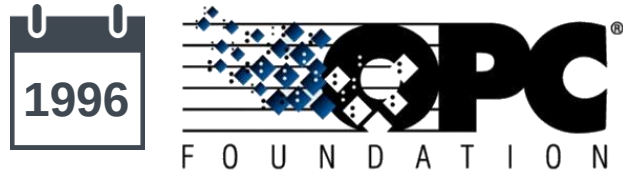
10. OPC UA – off topic

Alarms and Conditions, metody, OPC UA klient, SiOME, WireShark,

11. Rekapitulace



OPC UA protokol



- Založení skupiny OPC Foundation
 - Nyní přes 450 členů
- **O**LE for **P**rocess **C**ontrol
- Postaveno na Microsoft Windows COM/DCOM
- Nebylo kompatibilní s jinými systémy
- Standardizovaný přístup k datům, historickým datům, alarmům a událostem

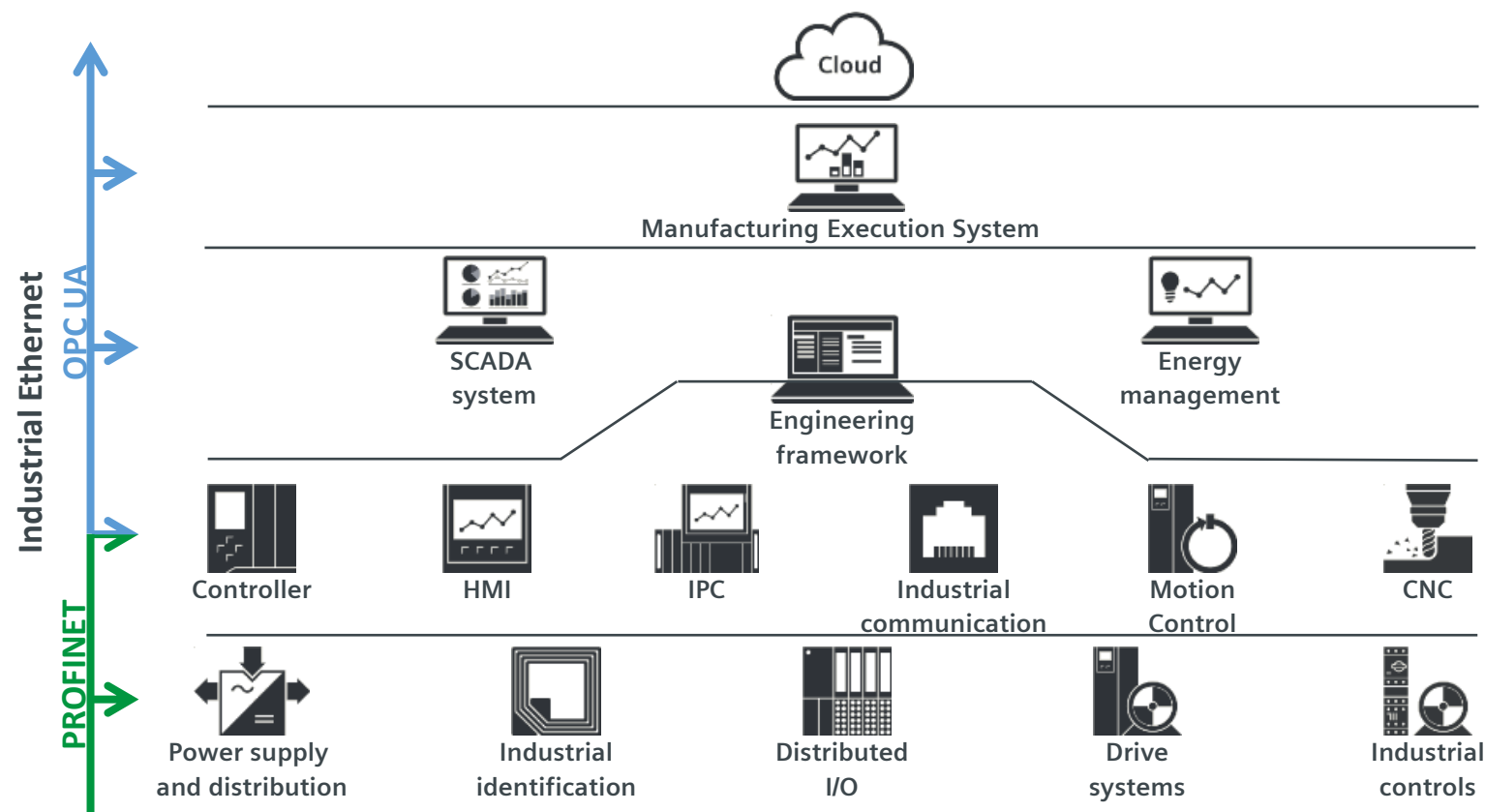
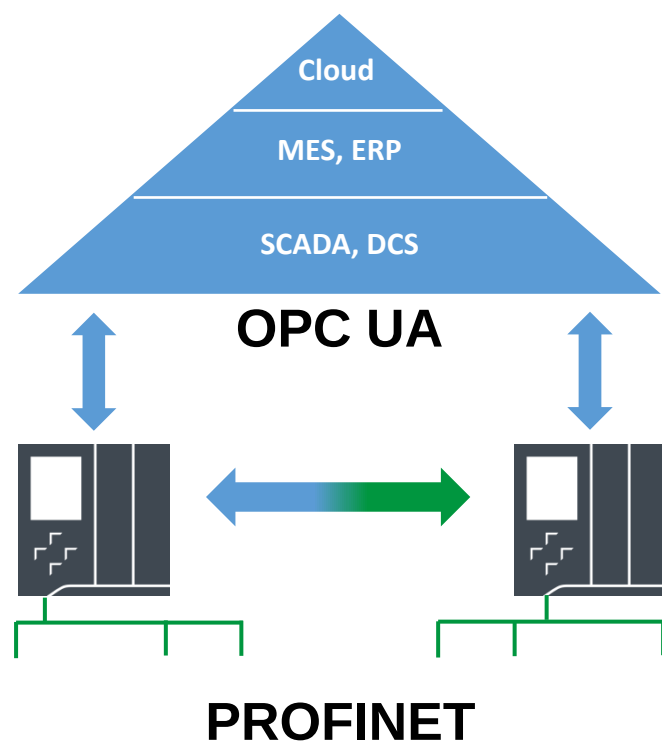


- **O**pen **P**latform **C**ommunications
Unified **A**rchitecture
- **N**ení postaveno na MS Windows COM/DCOM
 - Lze použít na různých platformách
- **R**ozšiřuje OPC standard
 - **K**lient/server či pub/sub
 - **B**ezpečnost, rychlost, různé způsoby čtení
- **O**všem není kompatibilní s OPC standardem
- **N**eustále vyvíjen

- **TCP komunikace**
 - **Model server-klient**
 - Či publisher-subscriber
 - Není real-time
 - **Routing možný**
 - **Lze omezit firewallem**
 - **NAT** (překlad IP adres) **možný**
 - **Port lze měnit** (standardně 4840 u Simatic PLC)
- **Zabezpečená komunikace**
 - **X.509 certifikáty – podpis a šifrování zpráv**
 - Data jsou čitelná pouze pro dvojici server-klient
 - Změna dat při přenosu je detekovatelná a generuje chybové hlášky
 - **Možnost použití i jména a hesla pro uživatelský přístup**
- **Data** (read, write, subscribe), **alarms&conditions, metody** (funkce v PLC)
- **Snadná standardizace**
 - **Definované modely lze implementovat do různých serverů**

OPC UA a Profinet

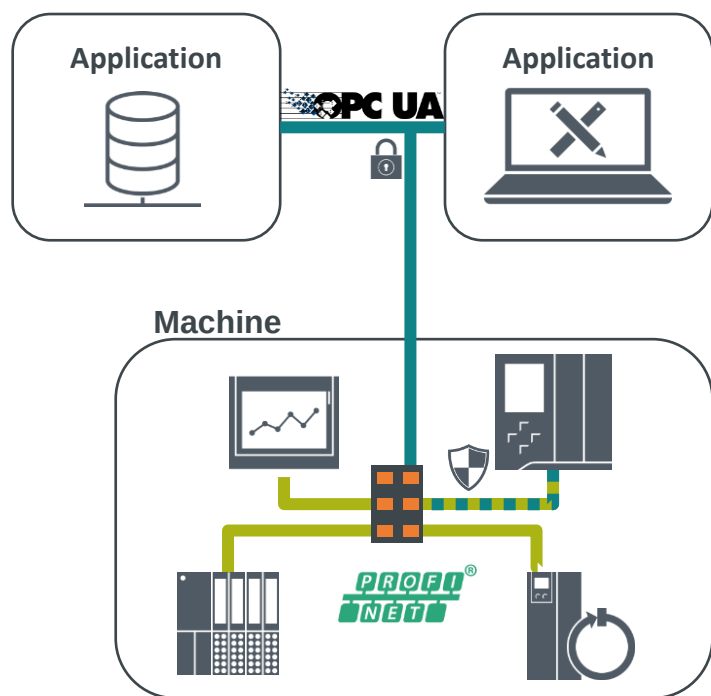
SIEMENS



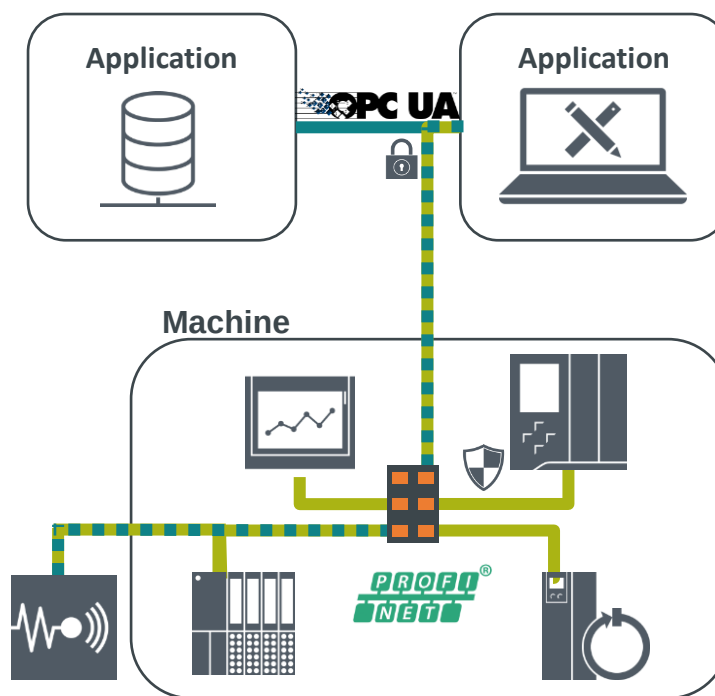
OPC UA a Profinet

SIEMENS

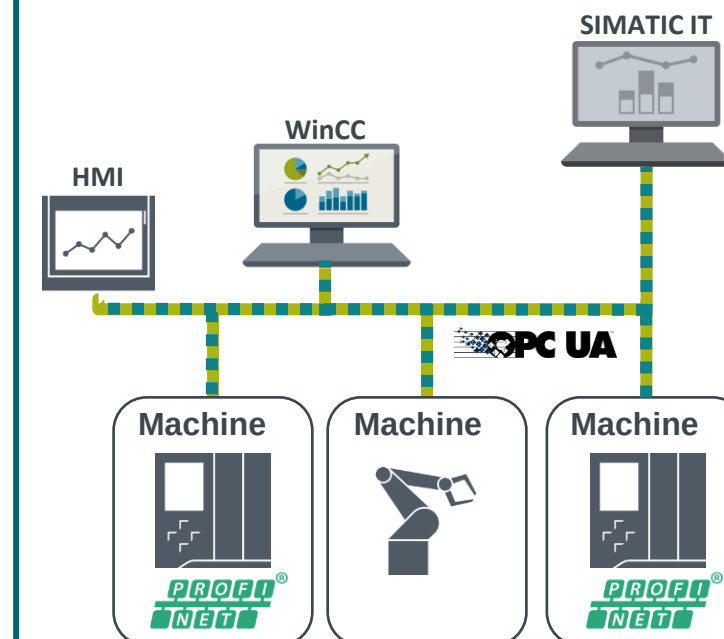
Snadná integrace do existujících systémů

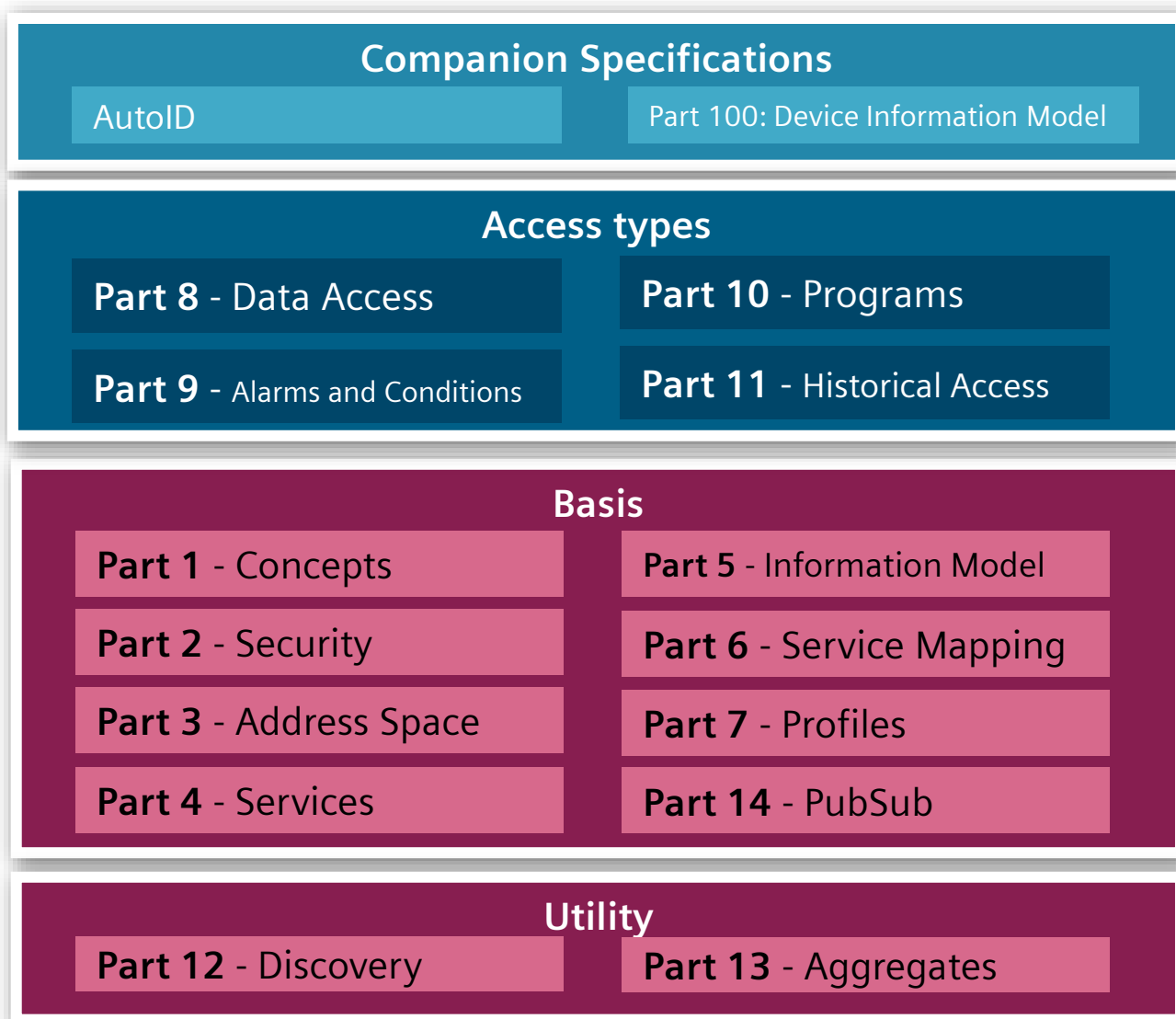


Integrace do Profinet sítě



Integrace do zařízení třetích stran





Part 15 – Safety

Part 15 – StateMachines

Part 20 – FileTransfer

<https://reference.opcfoundation.org/>

Server profile

- Každý OPC UA server i klient musí splňovat standardy - profily
- Profily zajišťují kompatibilitu a konzistentnost
- Profil se skládá z tzv. “Conformance units”
 - Každá taková jednotka definuje funkci, model či službu
- Server profil může definovat schopnost poskytovat alarmy, historická data

The screenshot shows the 'OPC UA Profiles' website. On the left is a sidebar with a tree view of categories: Server Category (Facets, FullFeatured), Client Category (Facets, FullFeatured), Publisher Category, Subscriber Category, Transport Category (Facets), Security Category (Facets), Global Directory Service Category (Facets, FullFeatured), and OPC Companion Standard Category (Facets, FullFeatured). The main content area features the OPC Foundation logo, a welcome message, a link to the 'OPC UA Part 7 Profiles specification', and a terminology section defining Profile, Facet, Conformance Group, and Conformance Unit. It also includes instructions for using the site's features.

OPC UA Profiles

Following are the currently defined profiles, arranged according to their application category.

- Server Category
 - Facets
 - FullFeatured
- Client Category
 - Facets
 - FullFeatured
- Publisher Category
- Subscriber Category
- Transport Category
 - Facets
- Security Category
 - Facets
- Global Directory Service Category
 - Facets
 - FullFeatured
- OPC Companion Standard Category
 - Facets
 - FullFeatured

Welcome to the OPC Foundation Unified Architecture Profile Reporting Visualization Tool. This is the master database and primary source for all profile information and is used to generate the [OPC UA Part 7 Profiles specification](#)

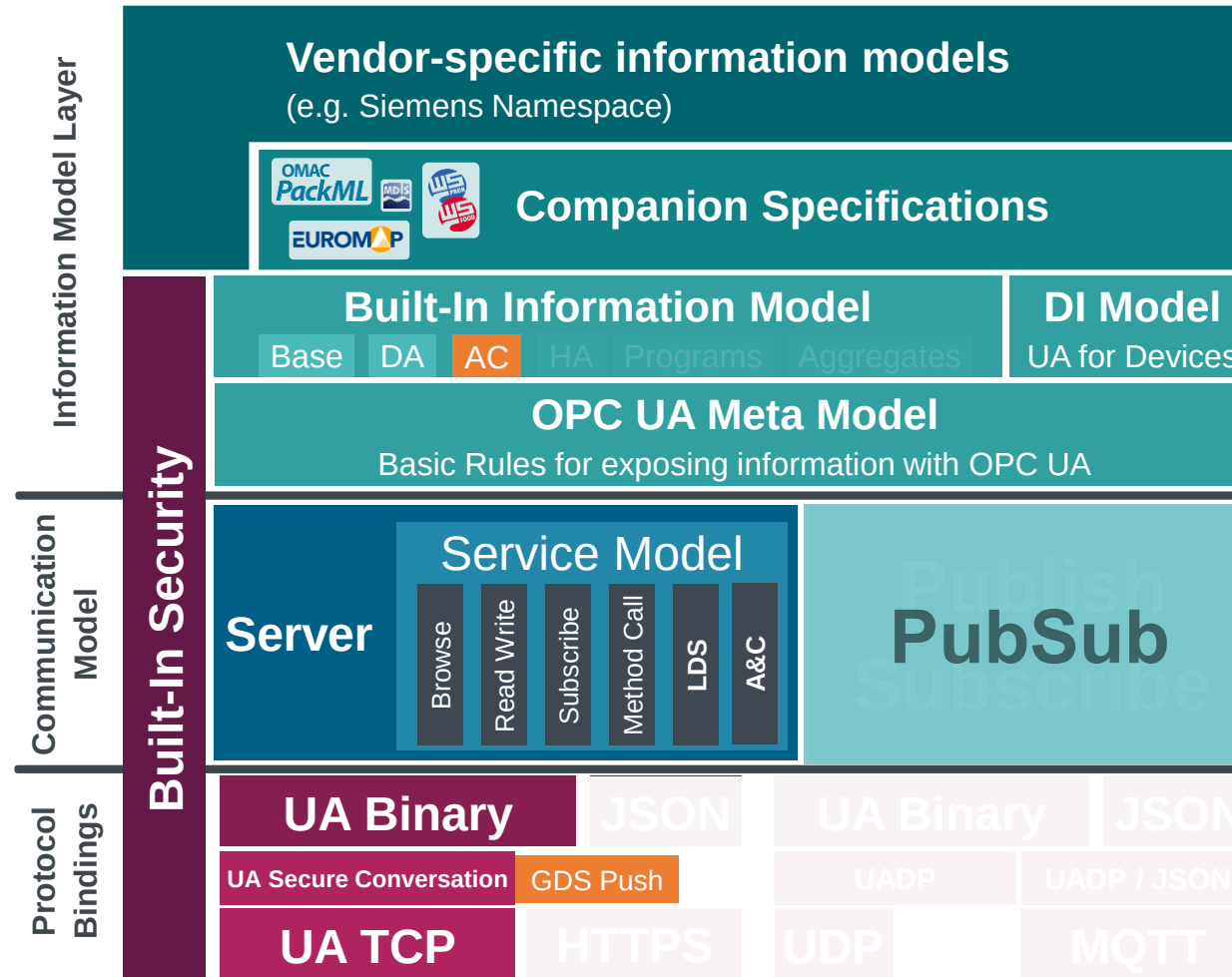
Terminology used in this application:

- **Profile** - a full-featured definition of functionality that must be supported; consumer of other *Profiles, Facets, Conformance Groups, and Conformance Units*.
- **Facet** - a definition of partial functionality; consumer
- **Conformance Group** - a collection of *Conformance Units*
- **Conformance Unit** - specific functionality, e.g. Read an Array type etc.

Please refer to the [OPC Unified Architecture Part 7 Specification](#).

Instructions

- Use the TreeView (left) to select a *Profile* or *Facet*
- The list of *Conformance Units* will appear here
- In the *Conformance Units* page you can filter the list using options at the top of the page.

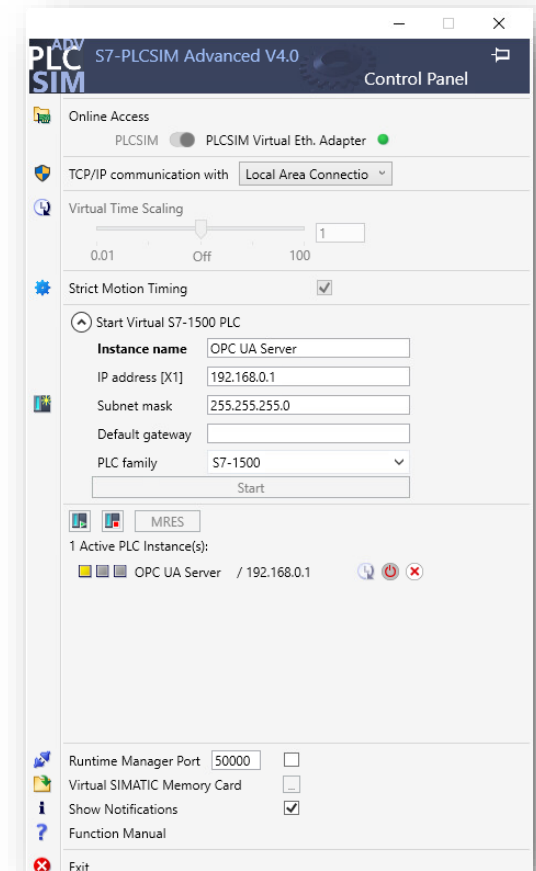


<https://support.industry.siemens.com/cs/start>
→ 109780503

PLCSIM Advanced

SIEMENS

- [Simulátor PLC řady S7-1500 a ET200SP CPU](#)
- Jednoduchá instalace a zprovoznění
- Více instancí PLC v jednom simulátoru
- Rozšířené možnosti komunikace
 - PLCSIM – komunikace v rámci PC
 - Virtual Ethernet Adapter – komunikace i mimo PC pomocí vybraného síťového adaptéru
- Podpora pokročilých funkcí
 - Web server, watch table
 - OPC UA, OUC (secure), HMI komunikace...
 - Škálování času – zrychlení či zpomalení běhu CPU
- Automatická validace programových kódů – API
- Pokročilá simulace IO, pohonů apod. pomocí [SIMIT](#)
- **Není podporován profinet → hlavní rozdíl oproti SW PLC**
- [Trial download](#)
- [Industry mall](#)



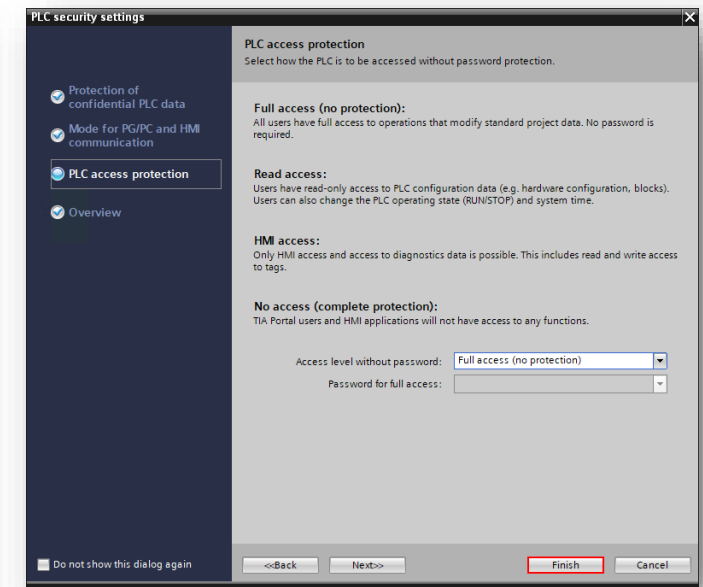
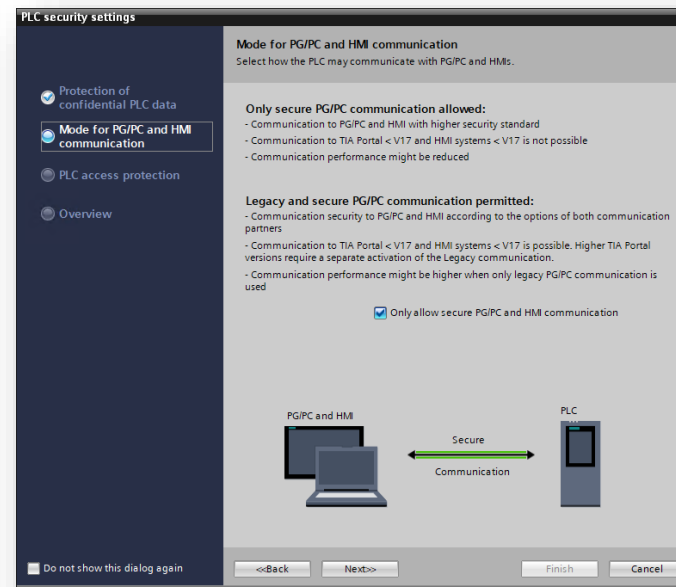
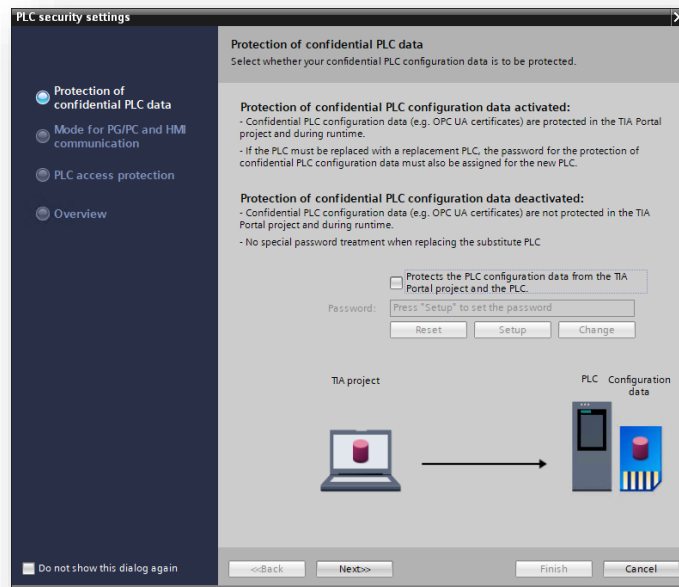
Konfigurace PLC



5 minut

SIEMENS

- Otevřít TIA Portal
- Vytvořit projekt
- Vložit do projektu PLC (S7-1500, FW 2.9)
- Aktivovat licenci (STEP 7 Professional)



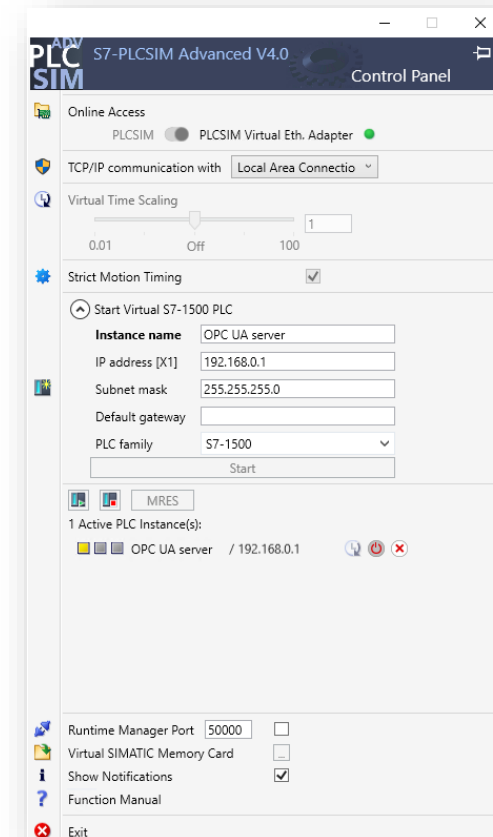
Zapnutí simulátoru PLC



2 minuty

SIEMENS

- Otevřít PLC SIM Advanced V4.0
- Přepnout komunikaci na PLCSIM Virtual Eth. Adapter (ponechat Local Area Connection)
- Start Virtual S7-1500 PLC
 - Vyplnit
 - Instance name (libovolné jméno PLC)
 - IP adresu (192.168.0.1)
 - Masku podsítě (255.255.255.0)
- Start
- Aktivovat licenci (PLC SIM Advanced)



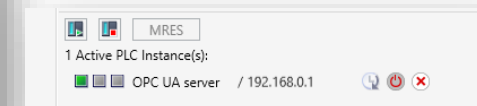
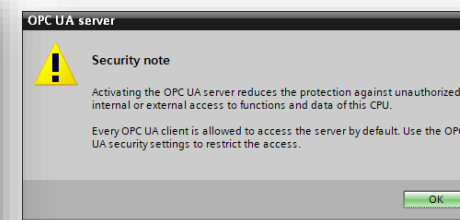
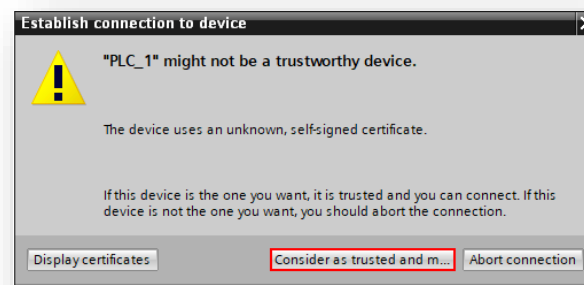
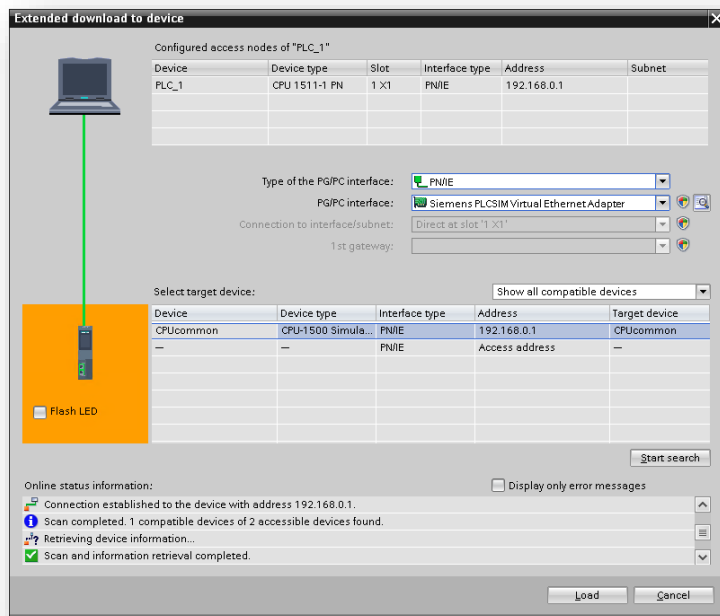
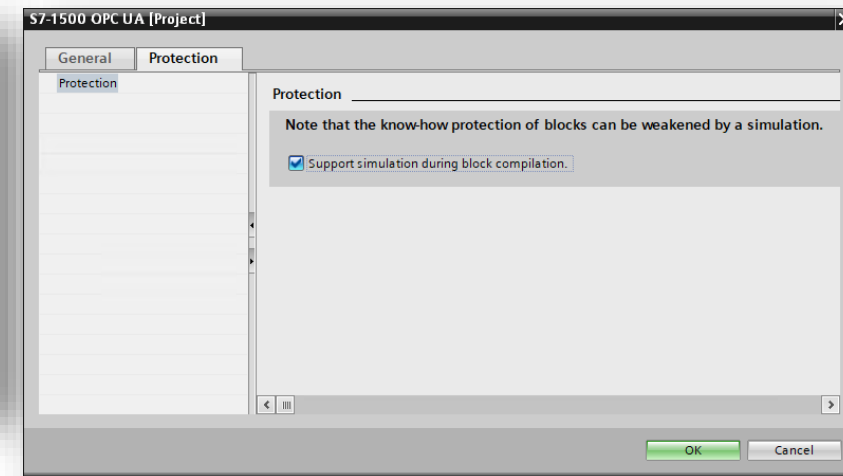
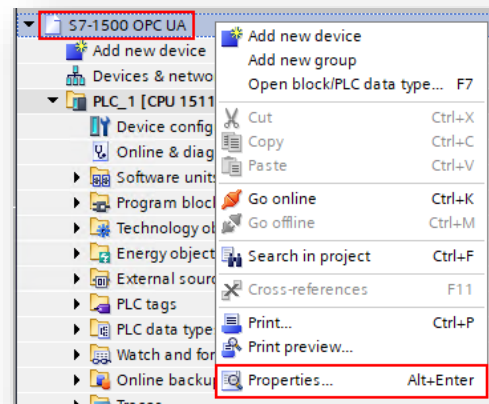
Nahrání PLC do simulátoru



2 minuty

SIEMENS

- Povolit simulaci v projektu
- Nahrát PLC do PLCSIM Advanced
 - Vyhledat PLC
 - Load
 - Přiřadit IP adresu k síťové kartě
 - Přijmout "PLC_1" za důveryhodné
 - Spustit PLC (Start module → RUN)



OPC UA v portfoliu Siemens

Přehled OPC UA v portfoliu Siemens

SIEMENS

Produkt	Server	Client	Licence	Popis
Simatic S7-1200	✓	x	1x basic	Simatic PLC
Simatic S7-1500(S)*	✓	✓	1x S/M/L	Simatic PLC (i software PLC)
Simatic CloudConnect	✓	✓	-	IoT Gateway
Simatic CN 4100	✓	x	-	Komunikační brána (redundantní)
Simatic NET	✓	x	8/64/512	Software pro Windows OS
Comfort panely	✓	✓	-	HMI panel
Unified comfort panely	✓	x	-	HMI panel
WinCC RT Advanced	✓	✓	-	Vizualizace pro PC
WinCC RT Professional	✓	✓	-	SCADA
WinCC V7.5	✓	✓	1x ConnPack	SCADA, ConnPack = connectivity pack option
WinCC OA	✓	✓	?	SCADA, server i client jako option
Industrial Data Bridge	✓	✓	1x IDB	Option pro WinCC (funkční i bez WinCC)

* Přístup k serveru i pomocí CP1543-1

Simatic NET: Softnet / Hardnet

Software pro Windows OS +

Vyčítání dat ze Simatic PLC S7 / S7 optimized +

Publikování vyčtených dat v podobě OPC serveru +

- OPC (COM/DCOM)
- OPC UA

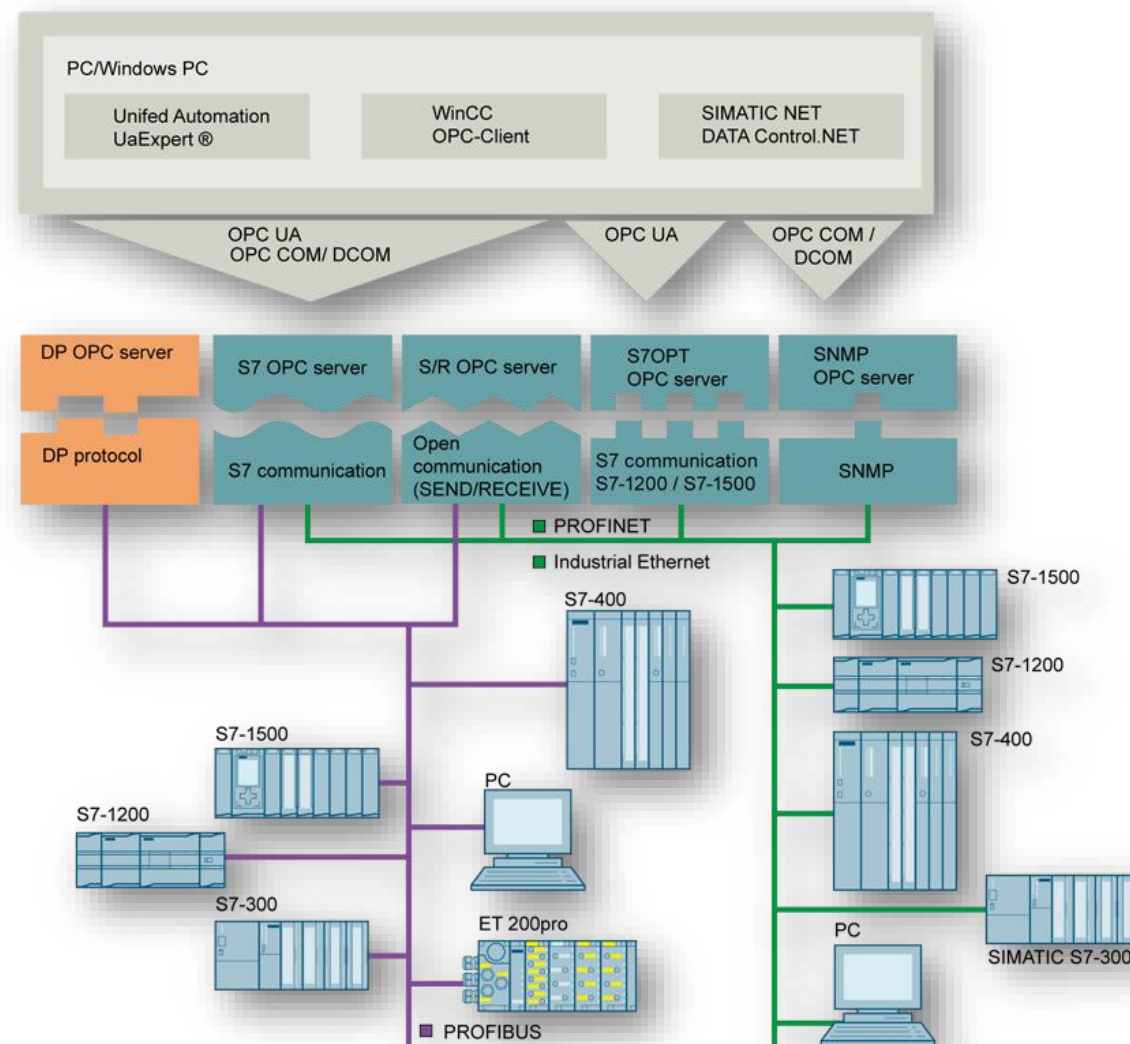
Podpora OPC UA HA (history) +

Podpora Profinet/Industrial Ethernet i Profibus sítí +

Až 207 Simatic PLC +

Konfigurace i v TIA Portalu +

SIEMENS



* Přístup k serveru i pomocí CP1543-1

Simatic CloudConnect 712/716

SIEMENS

Komunikační brána do cloudu



MQTT publisher / subscriber



Komunikace se Simatic PLC
S7-300/400/1200/1500



Data čtená z PLC mohou být
odeslána do cloudu (MQTT)
či publikována v OPC UA
serveru CC71x



Simatic CC716 podporuje i
Profibus a MPI spojení



Připojení až k 7 PLC

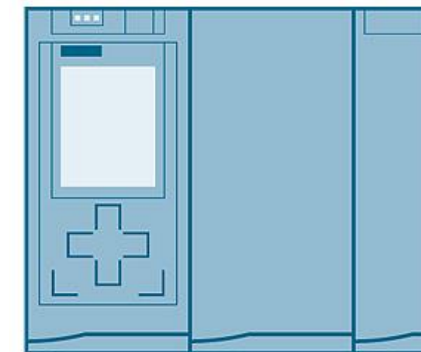
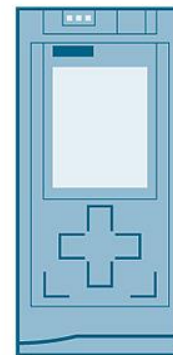
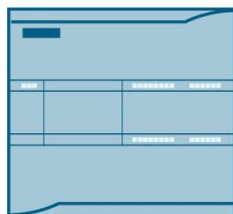


Konfigurace přes web server



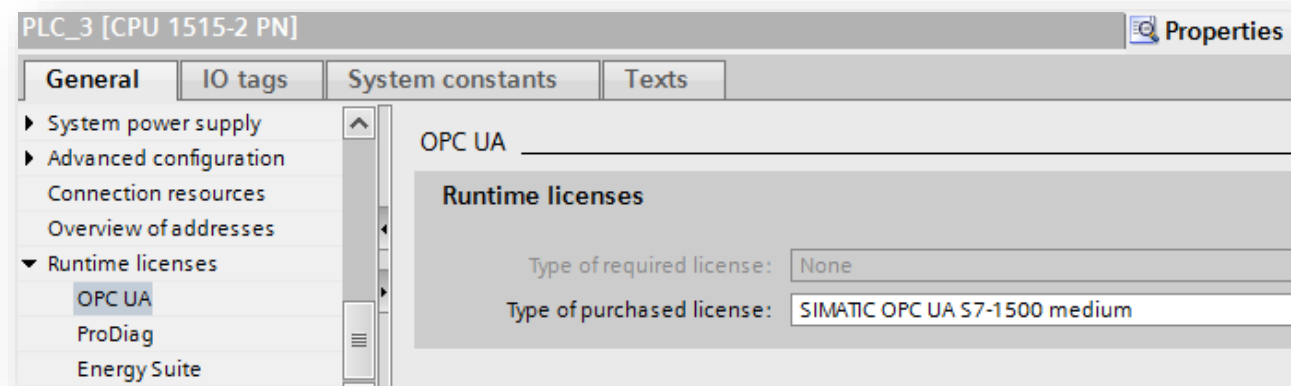
Licencování OPC UA

SIEMENS



	S-1200	1510 ... 1513 CPU	1515 ... 1516 CPU	1517 ... 1518 CPU
Licence	Basic	Small	Medium	Large
Listovní cena	50€	100€	200€	300€

- Licence platí pro server i client
- Součást HW konfigurace



Limity OPC UA serveru

SIEMENS

	S7-1200	CPU 1510...13	CPU 1515/16	CPU 1517/18
No. of sessions, max.	10	32	48	64
No. of accessible variables, max.	1,000	50,000	100,000	200,000
No. of registerable nodes, max.	-	10,000	20,000	50,000
No. of subscriptions per session, max.	50	20	20	20
Sampling interval, min.	100 ms	100 ms	100 ms	10 ms
Publishing interval, min.	200 ms	500 ms	200 ms	10 ms
No. of server methods, max.	20	20	50	100
No. of in/outputs per server method, max.	?	20	20	20
No. of monitored items, recommended.	1000 (max.)	1,000	2,000	10,000
	for 1 s sampling interval and 1 s publishing interval			
No. of server interfaces, max.	2	10	10	10
No. of nodes for server interfaces, max.	2,000	1,000	5,000	30,000
Number of program alarms	-	100	200	400
Number of alarms for system diagnostics	-	50	100	200

Limity OPC UA klienta

SIEMENS

	CPU 1510...13	CPU 1515/16	CPU 1517/18
Number of connection	4	10	40
Number of nodes of the client interfaces	1000	2000	5000
Number of elements for one call of OPC_UA_NodeGetHandleList/OPC_UA_ReadList/OPC_UA_WriteList	300	300	300
OPC_UA_NameSpaceGetIndexList	20	20	20
OPC_UA_MethodGetHandleList	100	100	100
Number of registerable nodes	5000	5000	5000
Number of registerable method calls	100	100	100
Number of inputs/outputs for method calls	20	20	20

- **Kompletní info v produktovém listu technických údajů** (Industry Mall, SIOS)

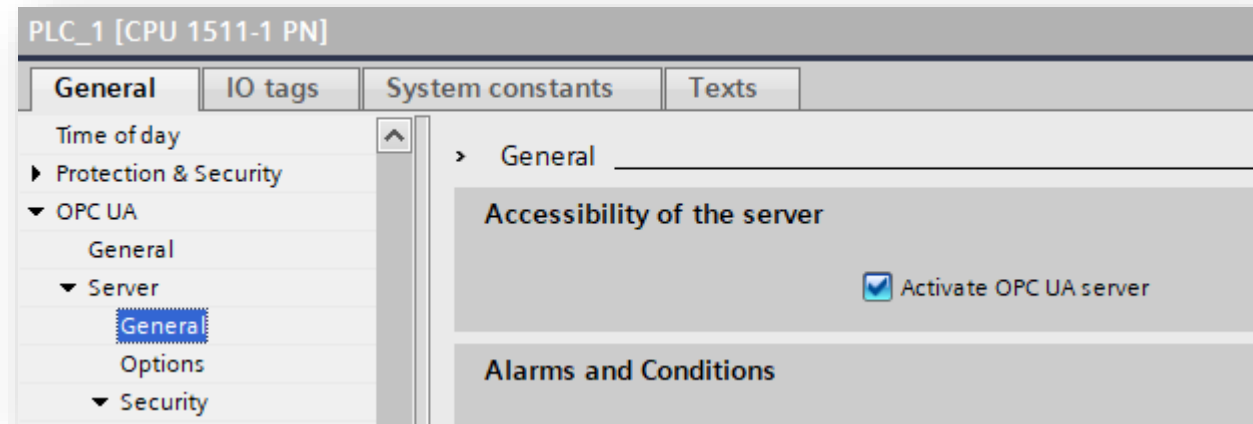
Zapnutí OPC UA serveru



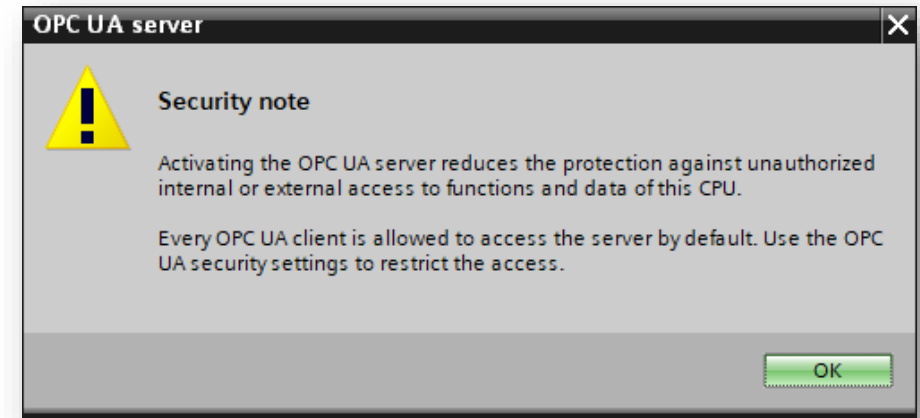
2 minuty

SIEMENS

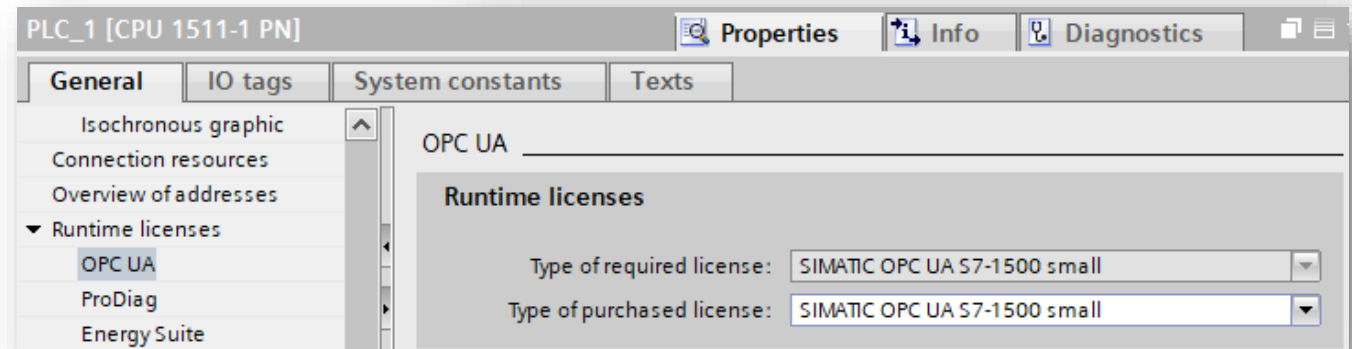
- V HW konfiguraci PLC povolit OPC UA server



- Akceptovat bezpečnostní rizika



- Vložit do PLC požadovanou licenci
- Přehrát HW konfiguraci PLC



Připojení k OPC UA serveru



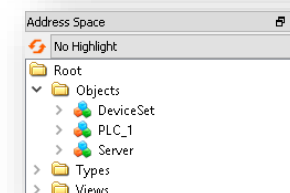
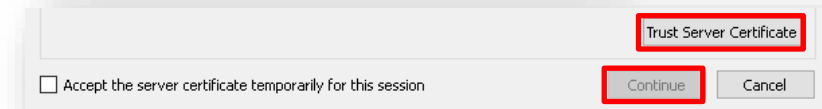
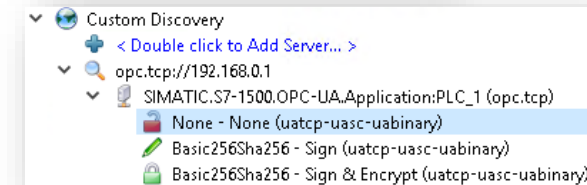
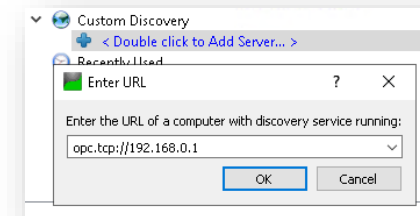
5 minut

SIEMENS



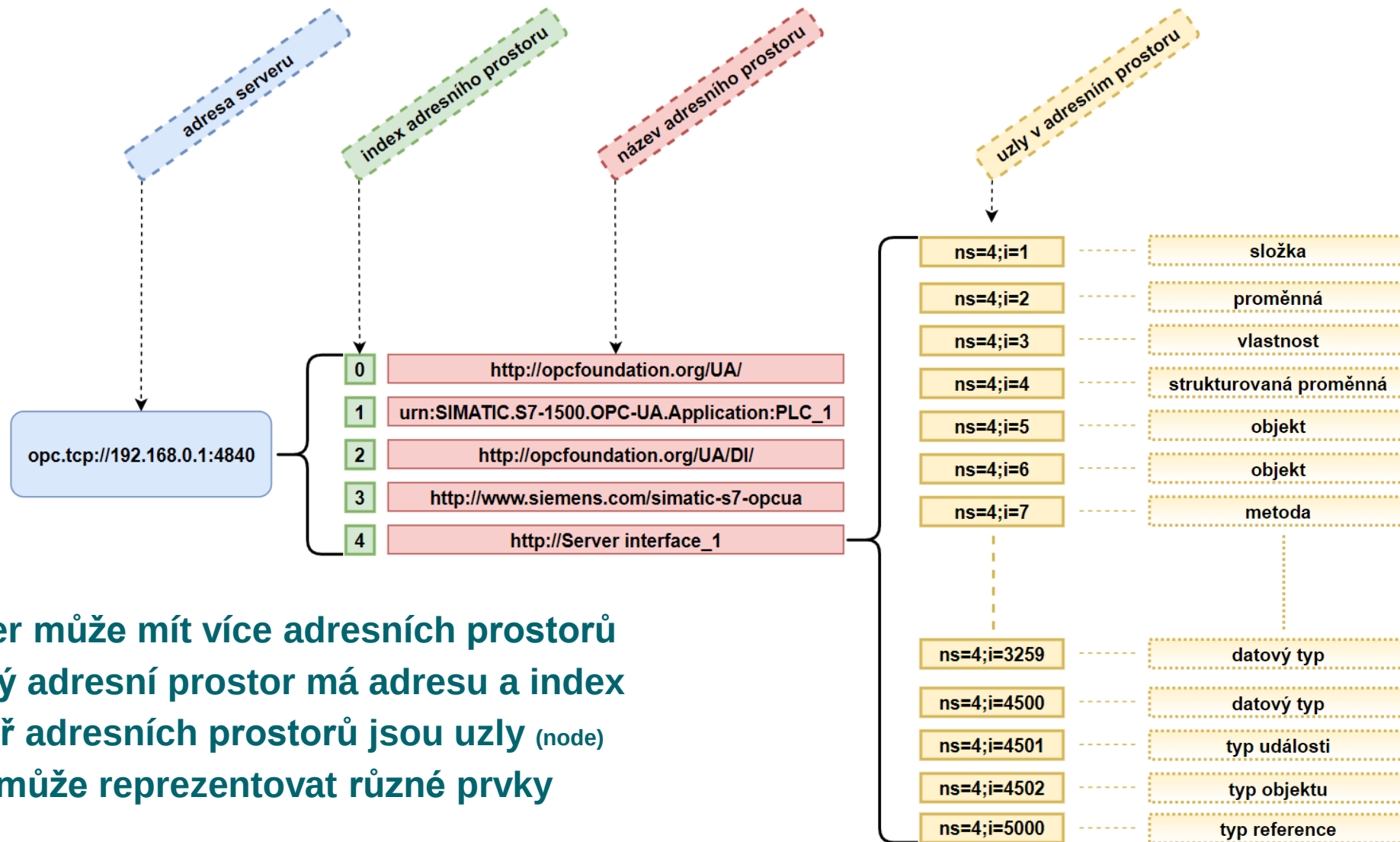
- **UA Expert – univerzální OPC UA klient** (čtení dat, alarmů, diagnostika, archivní data...)
- **Zapnout UA Experta → OK → vygenerovat certifikát pro UA Expert aplikaci**
 - Stačí vložit libovolné jméno organizace, ostatní parametry jsou volitelné
- **Automatický update → OK**
- **Vyhledat server**
- Custom discovery: `opc.tcp://192.168.0.1:4840`
 - Otevřít zadanou adresu
 - Vybrat možnost “None”
 - OK
- **Připojit k serveru**
- UA Expert zobrazí certifikát serveru
 - “Trust Server Certificate”
 - “Continue”

→ Klient připojen k serveru → je vidět adresní prostor



Adresní prostor

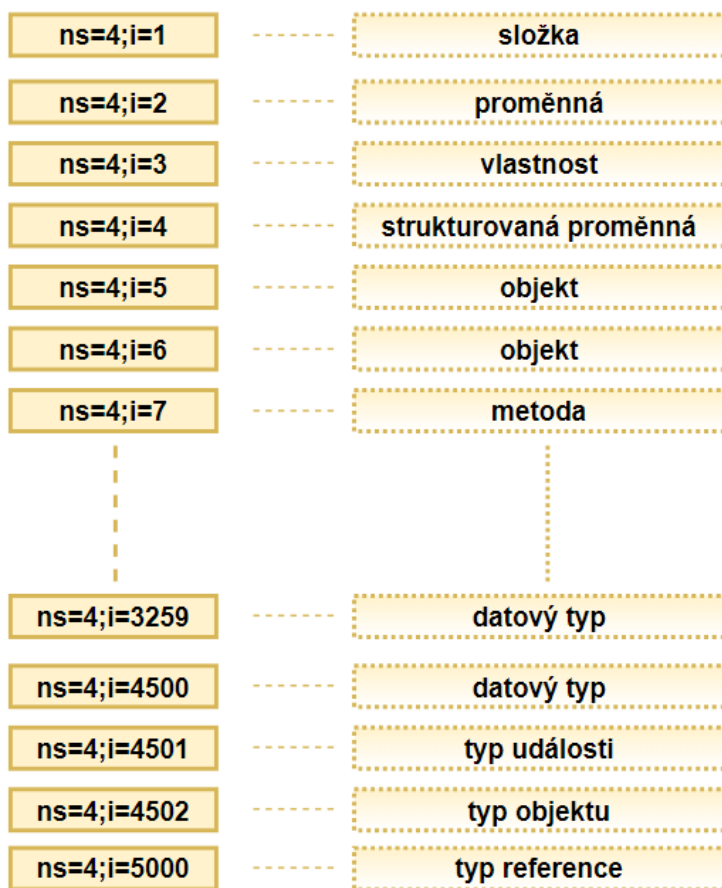
Koncept adresního prostoru



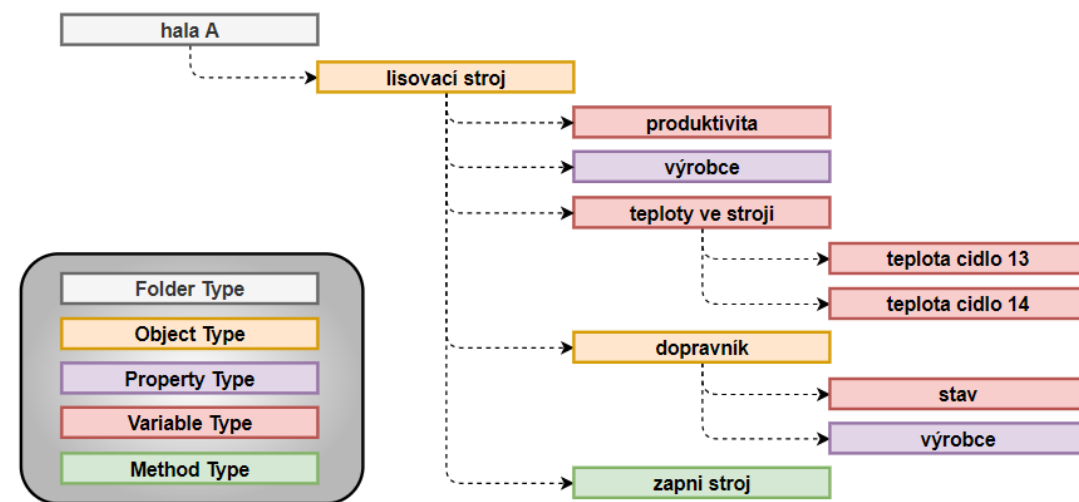
- Server může mít více adresních prostorů
- Každý adresní prostor má adresu a index
- Uvnitř adresních prostorů jsou uzly (node)
- Uzel může reprezentovat různé prvky

Koncept adresního prostoru

SIEMENS

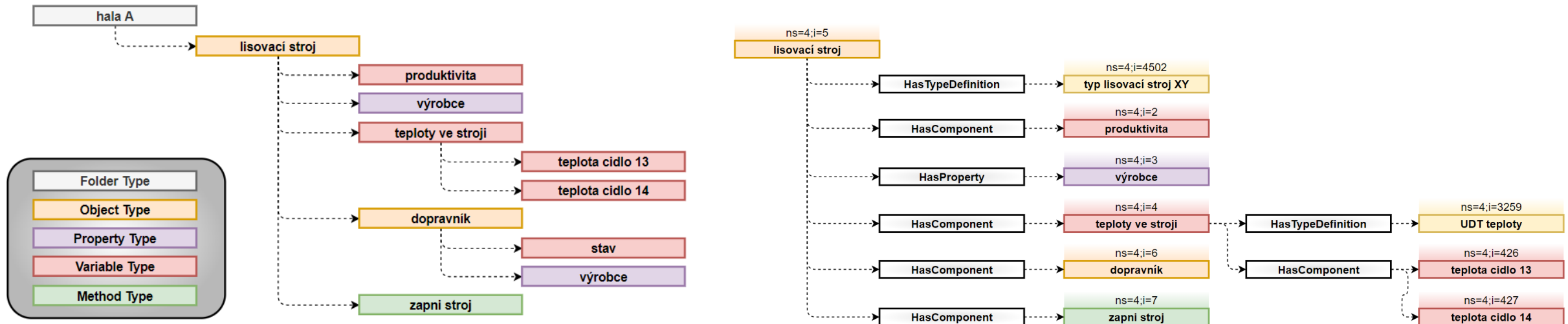


- Uzly jsou mezi sebou provázané



Koncept adresního prostoru

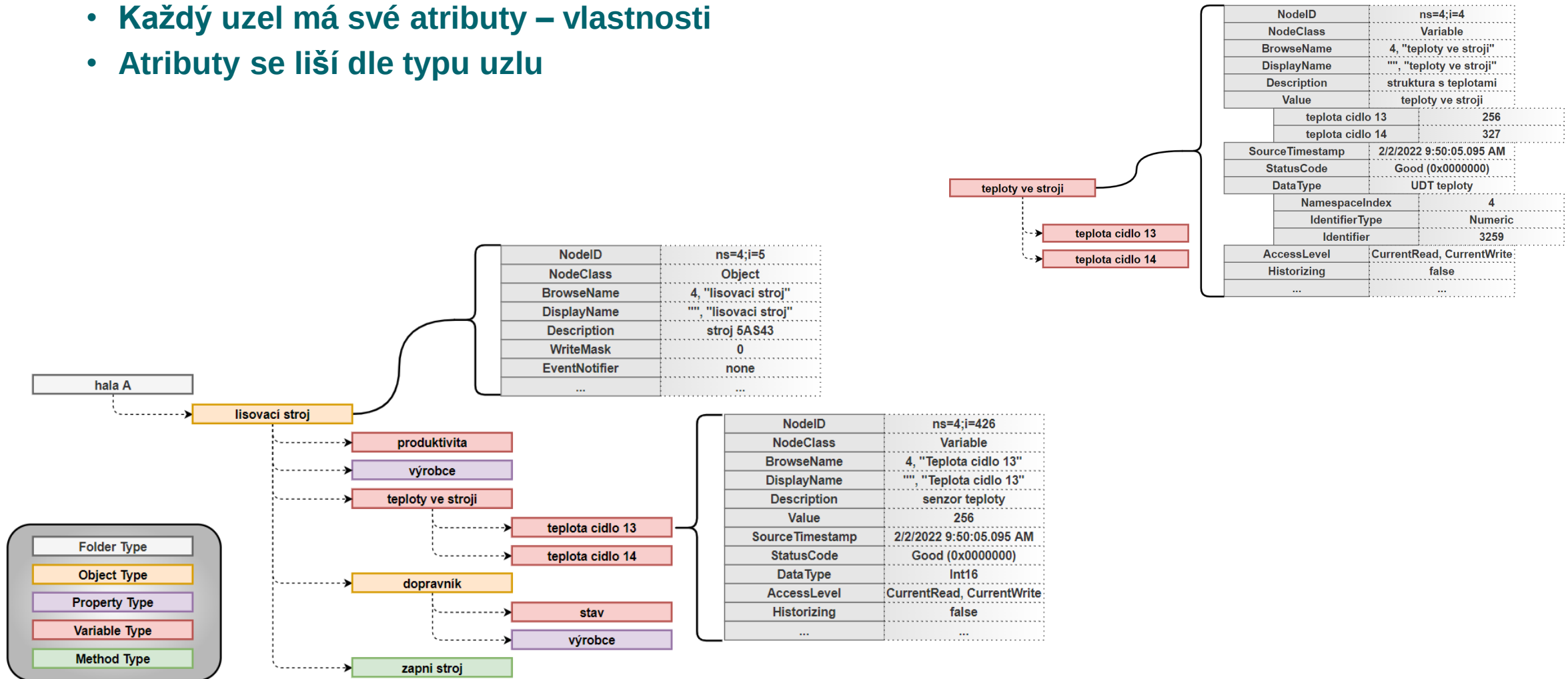
- Jednotlivé prvky jsou mezi sebou vázané referencemi
- Reference umožňují strukturalizaci adresních prostorů
- Reference/vazba může být různého typu
 - HasComponent – daný prvek má nějakou komponentu, která s ním souvisí
 - Organizes - daný prvek má nějakou komponentu, kterou pouze zahrnuje a nesouvisí s ním
 - HasProperty – má vlastnost
 - HasObject – má jiný prvek
 - HasTypeDefinition – má definici svého typu



Koncept adresního prostoru

SIEMENS

- Každý uzel má své atributy – vlastnosti
- Atributy se liší dle typu uzlu



- **Každý server může mít více adresních prostorů** (namespaces)

- **S7-1500 má vždy alespoň tři:**

- ns=0: adresní prostor obsahující informace o serveru (stav, vlastnosti, dovednosti)
 - ns=1: diagnostické informace k jednotlivým spojením s klienty
 - ns=2: popisuje diagnostické možnosti
 - ns=3: Standard SIMATIC interface (automaticky publikuje datové bloky a tagy)
 - ns=4: uživatelský adresní prostor (vlastní navržený adresní prostor)

- **Objektový model**

- **Objekt** (object) může mít **proměnné** (variable), **metody** (method), **vlastnosti** (property) či **další vnořené objekty**
Objekt “lisovací stroj” má proměnnou “produktivita”, metodu “zapni stroj”, vlastnost “výrobce” a objekt “dopravník”
Objekt “dopravník” má proměnné “stav” a vlastnost “výrobce”

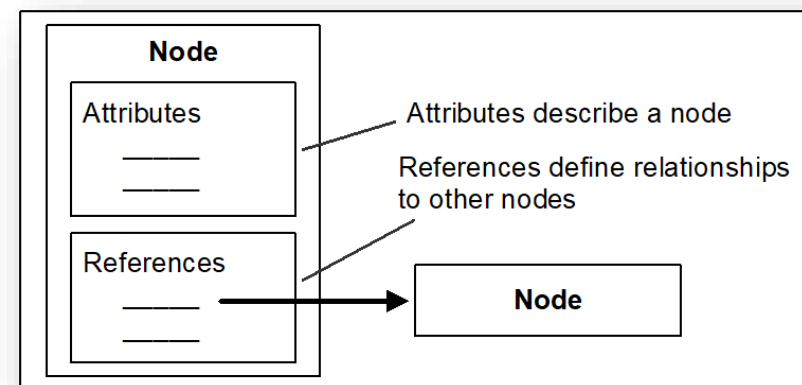
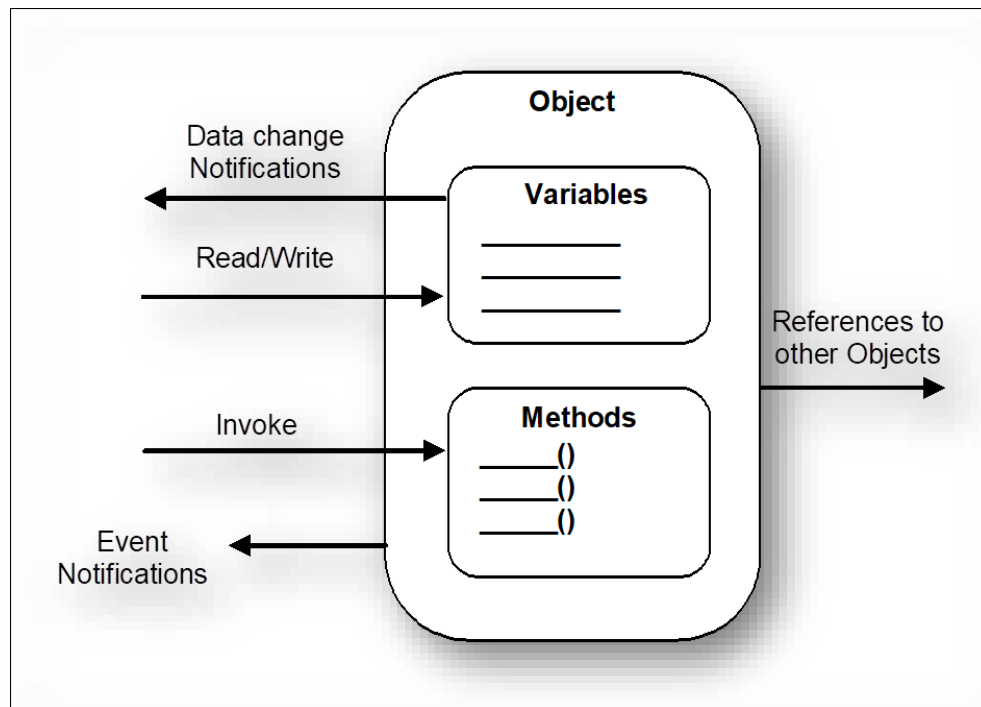
- **Objekty a jejich komponenty v serveru reprezentují uzly** (node)

- **Každý uzel má svůj identifikátor v daném adresním prostoru** (integer či string nejčastěji)
 - **Každý uzel má svoje parametry** (attributes), které ho popisují
např.: typ: objekt/proměnná/metoda, datový typ: bool/int/string,
Objekt “lisovací stroj” je reprezentován uzlem “5”, vlastnost “výrobce” uzlem “3”, “produktivita” uzlem “2” a metoda “zapni stroj” uzlem “7”

- **Jednotlivé uzly se mezi sebou váží pomocí referencí**

- **Reference jsou různého typu**

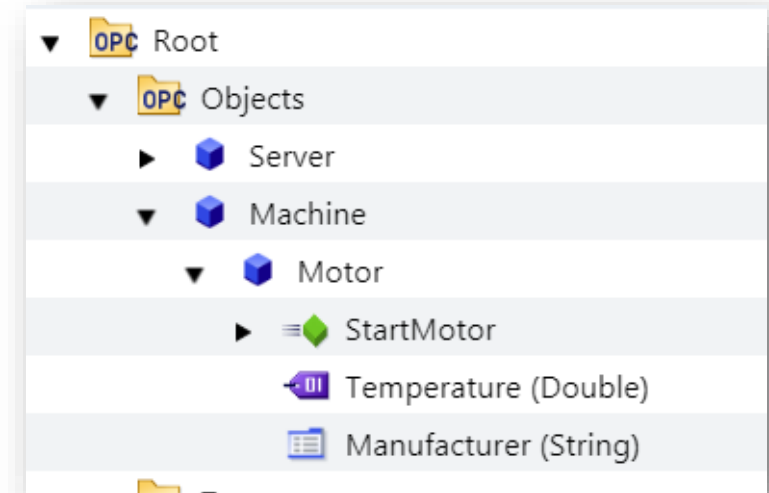
- Objekt “lisovací stroj” má referenci typu “HasComponent” na proměnnou “produktivita”, další referenci tohoto typu na metodu “zapni stroj”
 - Objekt “lisovací stroj” má referenci “HasProperty” na “výrobce”
 - Objekt “Hala A” má referenci “Organizes” na vnořený objekt “lisovací stroj”



Typy a instance

- **Type je označení pro prototyp** (knihovna)
 - **Variable type – definuje typ proměnné**
BaseDataVariableType (bool, int, string...), IEC_TIMER, PD_STW1, TADDR_Param atd...
 - **Object type**
NamespacesType – objekt obsahující popis adresních prostorů serveru
FolderType – organizační složka
ServerCapabilitiesType – objekt obsahující popis schopností serveru
 - **Data type – definuje datový typ proměnné (její atribut)**
 - **Reference type**
- **Instance typů dědí jejich vlastnosti**
 - Např. proměnná typu **SYS_SDT_521** (cílová adresa pro OUC) **bude vždy obsahovat pole ADDR se čtyřmi byty adresy**
 - Objekt typu IEC_TIMER vždy bude obsahovat proměnné ET, IN, PT a Q
- **Typy jsou čitelné ze serveru**

- Objekt “Machine” reprezentuje stroj
- Objekt “Motor” reprezentuje zařízení ve stroji
- Metoda “StartMotor” dává přístup k funkci v PLC
- Proměnná “Temperature” poskytuje dynamickou hodnotu
- Vlastnost “Manufacturer” poskytuje statickou informaci



- Reference objektu “Motor”
 - **HasProperty** → **Manufacturer**
Motor má vlastnost popisující výrobce
 - **HasComponent** → **StartMotor**
Motor má metodu pro start motoru
 - **HasComponent** → **Temperature**
Motor má proměnnou udávající teplotu

References				
Type Defined Placeholder				
Hierarchical References				
Forward	ReferenceType	NodeClass	Name	TypeDefinition
true	HasProperty	Variable	Manufacturer	PropertyType
true	HasComponent	Method	StartMotor	
true	HasComponent	Variable	Temperature	BaseDataVariableType

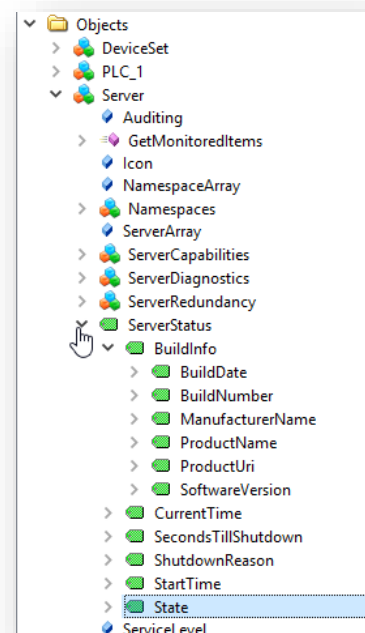
- Každý uzel (objekt, proměnná, vlastnost, metoda) má vlastní unikátní identifikátor
- Identifikátor (ID) je složen z adresního prostoru, typu adresace a adresy
- Adresní prostor (NameSpace) lze identifikovat stringem nebo číslem (index)
ns=http://siemens.com/simatic-s7-opc-ua
ns=3
- Typ adresace je většinou číselný (i) nebo textový (s)

ns= http://siemens.com/simatic-s7-opc-ua;i=2384

ns=0;i=2259

ns=3;s="S210_Data"."Data_struct"."Position"
(Position je proměnná ve struktuře Data_struct v DB S210_data)

- Pokud to klient dovolí, použijte textovou adresaci adresního prostoru
 - Namespace index se může změnit po přehrání PLC



Attribute	Value
▼ NodeId	i=2259 [Server_ServerStatus_State]
NamespaceIndex	0
IdentifierType	Numeric
Identifier	2259 [Server_ServerStatus_State]
NodeClass	Variable
BrowseName	0, "State"
DisplayName	"", "State"
Description	BadAttributeInvalid (0x80350000)
WriteMask	0
UserWriteMask	0
RolePermissions	BadAttributeInvalid (0x80350000)
UserRolePermissions	BadAttributeInvalid (0x80350000)
AccessRestrictions	BadAttributeInvalid (0x80350000)
▼ Value	
SourceTimestamp	1/5/2022 9:34:43.856 AM
SourcePicoSeconds	0
ServerTimestamp	1/5/2022 9:34:43.856 AM
ServerPicoSeconds	0
StatusCode	Good (0x00000000)
Value	0 (Running)
▼ DataType	ServerState
NamespaceIndex	0
IdentifierType	Numeric
Identifier	852 [ServerState]
ValueRank	-1 (Scalar)
ArrayDimensions	BadAttributeInvalid (0x80350000)
AccessLevel	CurrentRead
UserAccessLevel	CurrentRead
AccessLevelEx	BadAttributeInvalid (0x80350000)
MinimumSamplingInterval	50
Historizing	false

Zobrazení hodnot

Připojené servery

Vybraný objekt

Průzkumník adresních
prostorů

log

The screenshot displays the UaExpert software interface, which is a client for the OPC Unified Architecture (Ua). The main window is titled "Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*". It features a menu bar (File, View, Server, Document, Settings, Help) and a toolbar with various icons for file operations, server management, and data access.

The interface is divided into several panes:

- Project Pane:** Shows the project structure, including "Servers" and "Documents". The "Servers" pane lists the connected servers, with "SIMATIC.S7-1500.OPC-UA.Application:PLC_1" selected.
- Address Space Pane:** Displays the hierarchical structure of the address space. The "ServerCapabilities" object is selected under the "ServerArray" node.
- Data Access View:** A table showing the data access results. It includes columns for "#", "Server", "Node Id", "Display Name", "Value", "Datatype", and "Source". The table lists various properties of the "ServerCapabilities" object, such as "MaxArrayLength", "MaxBrowseContinuationPoints", "MaxHistoryContinuationPoints", etc.
- Attributes Pane:** Provides a detailed view of the selected object's attributes. It shows the "Node" attribute with a value of "i=2268 [Server_ServerCapabilities]" and lists other attributes like "NamespaceIndex", "IdentifierType", "Identifier", "NodeClass", "BrowseName", "DisplayName", "Description", "WriteMask", "UserWriteMask", "RolePermissions", "UserRolePermissions", "AccessRestrictions", and "EventNotifier".
- References Pane:** Shows the references between the selected object and other objects in the address space. It lists the "Reference" and "Target DisplayName" for each relationship, such as "HasComponent", "HasProperty", and "HasReference".
- Log Pane:** Displays the system log, showing timestamps, sources, servers, and messages. The log indicates successful data access operations.

#	Server	Node Id	Display Name	Value	Datatype	Source
1	SIMATIC.S7...	NS0[Numeric]2271	LocalIdArray	{}	String	8:01
2	SIMATIC.S7...	NS0[Numeric]11702	MaxArrayLength	131072	UInt32	8:01
3	SIMATIC.S7...	NS0[Numeric]2735	MaxBrowseContinuationPoints	5	UInt16	8:01
4	SIMATIC.S7...	NS0[Numeric]12911	MaxByteStringLength	131072	UInt32	8:01
5	SIMATIC.S7...	NS0[Numeric]2737	MaxHistoryContinuationPoints	5	UInt16	8:01
6	SIMATIC.S7...	NS0[Numeric]6387	MaxInactiveLockTime		Null	8:01
7	SIMATIC.S7...	NS0[Numeric]2736	MaxQueryContinuationPoints	5	UInt16	8:01
8	SIMATIC.S7...	NS0[Numeric]11703	MaxStringLength	16382	UInt32	8:01
9	SIMATIC.S7...	NS0[Numeric]2272	MinSupportedSampleRate	100	Double	8:01
10	SIMATIC.S7...	NS0[Numeric]2269	ServerProfileArray	{'http://opcf...	String	8:01
11	SIMATIC.S7...	NS0[Numeric]3704	SoftwareCertificates		Null	8:01
12	SIMATIC.S7...	NS0[Numeric]11714	MaxMonitoredItemsPerCall	1000	UInt32	8:01
13	SIMATIC.S7...	NS0[Numeric]11710	MaxNodesPerBrowse	1000	UInt32	8:01
14	SIMATIC.S7...	NS0[Numeric]11709	MaxNodesPerMethodCall	1	UInt32	8:01
15	SIMATIC.S7...	NS0[Numeric]11705	MaxNodesPerRead	1000	UInt32	8:01
16	SIMATIC.S7...	NS0[Numeric]11711	MaxNodesPerRegisterNodes	1000	UInt32	8:01
17	SIMATIC.S7...	NS0[Numeric]11712	MaxNodesPerTranslateBrowsePathsToNodeIds	1000	UInt32	8:01
18	SIMATIC.S7...	NS0[Numeric]11707	MaxNodesPerWrite	1000	UInt32	8:01
19	SIMATIC.S7...	NS0[Numeric]11509	NamingRule		Null	8:01
20	SIMATIC.S7...	NS0[Numeric]113	NamingRule		Null	8:01
21	SIMATIC.S7...	NS0[Numeric]11511	NamingRule		Null	8:01
22	SIMATIC.S7...	NS0[Numeric]112	NamingRule		Null	8:01
23	SIMATIC.S7...	NS0[Numeric]114	NamingRule		Null	8:01

Attribute	Value
Node	i=2268 [Server_ServerCapabilities]
NamespaceIndex	0
IdentifierType	Numeric
Identifier	2268 [Server_ServerCapabilities]
NodeClass	Object
BrowseName	0, "ServerCapabilities"
DisplayName	0, "ServerCapabilities"
Description	BadAttributeIdInvalid (0x80350000)
WriteMask	0
UserWriteMask	0
RolePermissions	BadAttributeIdInvalid (0x80350000)
UserRolePermissions	BadAttributeIdInvalid (0x80350000)
AccessRestrictions	BadAttributeIdInvalid (0x80350000)
EventNotifier	None

Reference	Target DisplayName
HasComponent	AggregateFunctions
HasProperty	LocalIdArray
HasProperty	MaxArrayLength
HasProperty	MaxBrowseContinuationPoints
HasProperty	MaxByteStringLength
HasProperty	MaxHistoryContinuationPoints
HasProperty	MaxQueryContinuationPoints
HasProperty	MaxStringLength
HasProperty	MinSupportedSampleRate
HasComponent	ModellingRules
HasComponent	OperationLimits

Timestamp	Source	Server	Message
1/5/2022 8:02:1...	Reference Plugin	SIMATIC.S7-150...	Browse succeeded.
1/5/2022 8:02:1...	Attribute Plugin	SIMATIC.S7-150...	Read attributes of node 'NS0[Numeric]11715' succeeded [ret = Good].
1/5/2022 8:02:1...	Reference Plugin	SIMATIC.S7-150...	Browse succeeded.

Přehled vlastností
(atributů)

Reference objektu



1. Jaký je identifikátor uzlu kmenové složky “Root”?
2. Jaké reference má objekt “Objects”? (typ reference a cílový prvek)
3. Jaké reference má objekt “DeviceSet”? (typ reference a cílový prvek)
4. Jaký je rozdíl mezi objektem “PLC_1” v Objects a v DeviceSet?
5. Jaký typ reference má objekt “Server” na “NamespaceArray” a “ServerStatus”?
6. Jaké reference má vlastnost “NamespaceArray”?
7. Jaký datový typ má vlastnost “NamespaceArray” a co vlastnost popisuje?
8. Kam odkazuje reference “HasTypeDefinition” u proměnné “ServerStatus”?
9. Jaký datový typ má proměnná “ServerStatus”?
10. Jaké OPC UA profily podporuje server v S7-1500?
11. Jaký je operační stav PLC? Integer

Přístup k datům

- **Server interface je rozhraní, které poskytuje OPC UA data**
- **Interface má svůj adresní prostor (namespace)**
- **Každý interface jinak využívá paměť PLC a je jinak rychlý**
- **V PLC lze zvolit, která data mají být přístupná v OPC UA několika způsoby**

1) Standard Simatic interface

- Automaticky publikuje všechna data (DB, tagy) v OPC UA serveru
- U jednotlivých DB a proměnných lze OPC UA přístup vypnout/omezit na čtení

2) User defined server interface

- Uživatelsky definované rozhraní
- Pouze vybraná data jsou publikována
- Lze vytvořit v TIA Portal

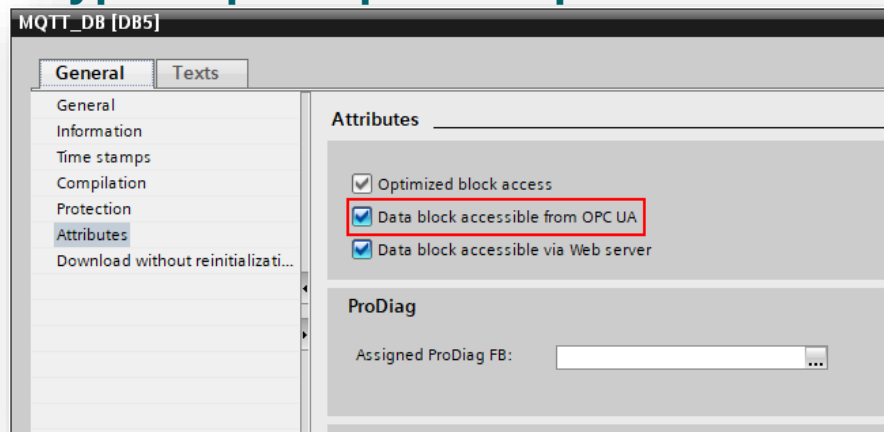
3) Companion Specification

- Standardní rozhraní, které lze importovat do TIA Portalu (OMAC, PackML...)

Server interface

SIEMENS

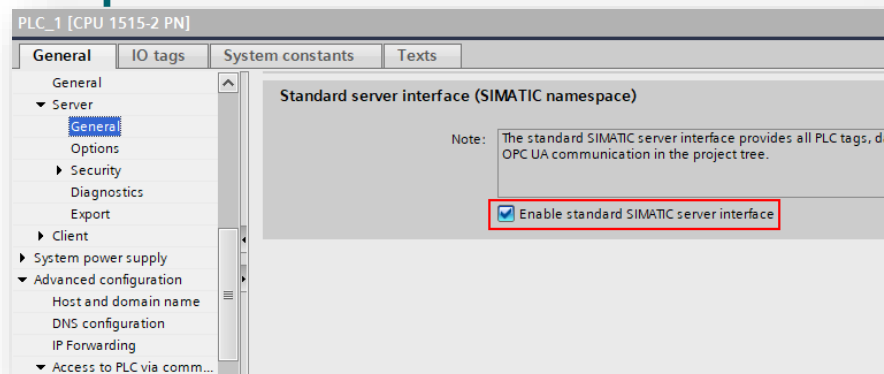
Vypnutí přístupu k DB přes OPC UA



Vypnutí přístupu k proměnným přes OPC UA

	Name	Data type	Offset	Start value	Retain	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API
1	Static					☐	☐
2	Velocity	Int	0.0	0	☐	☒	☒
3	Position	Int	2.0	0	☐	☒	☒
4	Torque	Int	4.0	0	☐	☒	☒
5	InOperation	Bool	6.0	false	☐	☒	☒

Zapnutí Simatic rozhraní



Vytvoření vlastního rozhraní OPC UA v TIA Portalu

OPC UA server interface				OPC UA elements	
Browse name	Node type	Access level	Local data	Project data	Data type
1 S210	Interface	---		1 Software units	
2 S210_Data	Object	---		2 Program blocks	
3 Velocity	INT	RD/WR	"S210_Data"."Velocity"	3 Date and time	
4 Position	INT	RD/WR	"S210_Data"."Position"	4 LS/NMP	
5 Torque	INT	RD/WR	"S210_Data"."Torque"	5 MQTT	
6 InOperation	BOOL	RD/WR	"S210_Data"."InOperation"	6 NTP	
7 Data_struct	"S210_Data"."Data_struct"	RD/WR	"S210_Data"."Data_struct"	7 OPC_UA_Client	
8 Record_error	BOOL	RD/WR	"S210_Data"."Record_error"	8 OUC k 57-300	
9 IDB_trigger	INT	RD/WR	"S210_Data"."IDB_trigger"	9 OUC testy	
10 <Add new>				10 Profi Energy	
11 <Add new>				11 Profinet diagnostics	
				12 Runtime Info	
				13 S210	
				14 S210_AutoRun_DB [DB10]	S210_AutoRun
				15 S210_Control_DB [DB3]	S210_Control
				16 S210_Data [DB2]	S210_Data
				17 Velocity	Int
				18 Position	Int
				19 Torque	Int
				20 InOperation	Bool
				21 Data_struct	Struct
				22 Record_error	Bool
				23 IDB_trigger	Int
				24 ModuleState	Struct
				25 SMS	
				26 SQL	
				27 Web server	
				28 Technology objects	
				29 PLC tags	

- **Standard Simatic Interface**

- Publikuje všechny vybrané DB a tagy v PLC
- Výkonově náročné pro CPU
- Stringová adresace proměnných (nelze měnit)



- **Used defined Server Interface**

- Vlastní rozhraní pro data, do kterého se mapují proměnné z CPU
- Jednoduché, výkonově nenáročné a efektivní
- Číselná adresace proměnných (nelze měnit)



- **Companion specification**

- Vlastní rozhraní pro data
- Definice se provádí v programu SiOME
- Vyžaduje pokročilé znalosti OPC UA protokolu
- Libovolná konfigurace parametrů proměnných

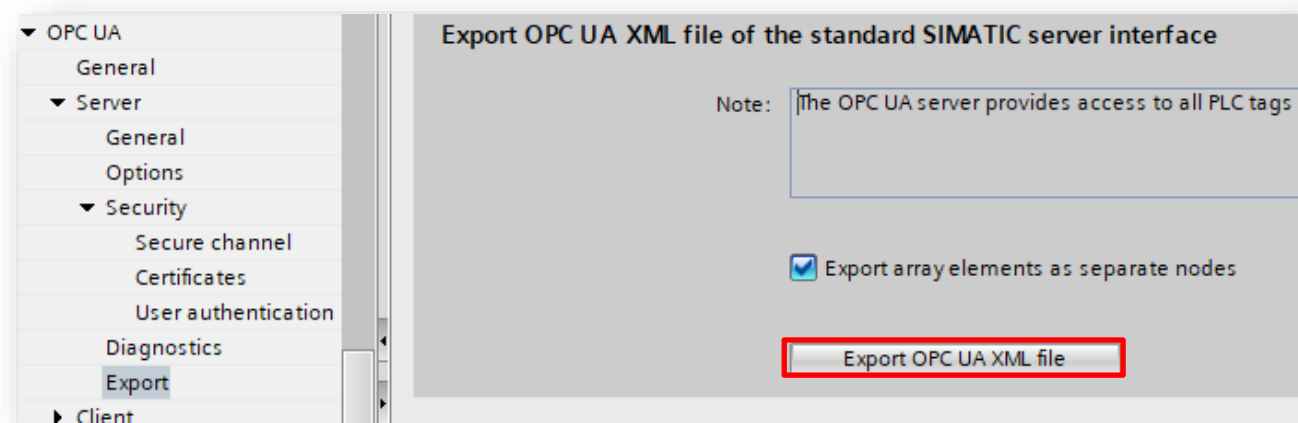


- **Namespace reference**

- Referenční rozhraní (definice typů) pro data (nelze mapovat k proměnným CPU)

Export OPC UA rozhraní - XML

- **Standard Simatic Interface**



- **User Defined Interface**

OPC UA server interface					
	Browse name	Node type	Access level		Local data
1	▼ S210	Interface	---		
2	■ ▼ S210_Data	Object	---		
3	■ Velocity	INT	RD/WR		☐ "S210_Data"."Velocity"
4	■ Position	INT	RD/WR		☐ "S210_Data"."Position"
5	■ Torque	INT	RD/WR		☐ "S210_Data"."Torque"
6	■ InOperation	BOOL	RD/WR		☐ "S210_Data"."InOperation"

Vlastní OPC UA rozhraní

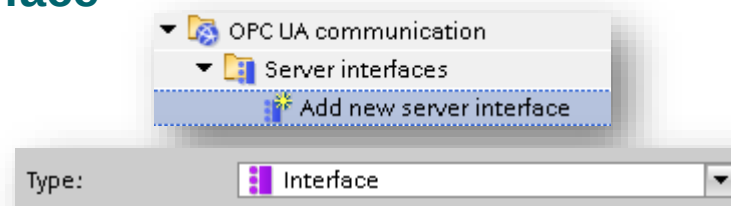


10 minut

SIEMENS

- Vytvořte dva datové bloky
 - DB1 bude obsahovat 500x integer (INT_0, INT_1, INT_2 .. INT_499)
 - DB2 bude obsahovat 1x pole (Array [0 .. 499] of Int) a 1x strukturu (INT_0, INT_1, INT_2 .. INT_499)

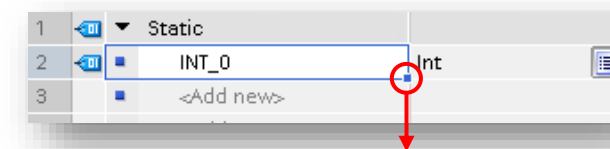
- Vytvořte nový OPC UA server interface



- V pravém okně otevřete DB2

- Myší přetáhněte pole a strukturu do řádku "Add new" v levém okně
- Myší přetáhněte i celé DB1

- Přehrajte PLC



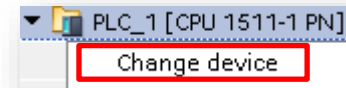
OPC UA server interface				OPC UA elements	
	Browse name	Node type	Access level	Project data	Data type
1	▼ Server interface_1	Interface	---	1 Software units	
2	▶ Array	ARRAY[0..499] of INT	RD/WR	2 Program blocks	
3	▶ Struct	"DB_Struct"."Struct"	RD/WR	3 DB_INT [DB1]	DB_INT
4	▶ DB_INT	Object	---	4 DB_Struct [DB2]	DB_Struct
5	<Add new>			5 ▶ Array	Array[0..499] of Int
				6 ▶ Struct	Struct
				7 Technology objects	
				8 ▶ PLC tags	



- Chyba kompilace? CPU nižší než 1515 mají limit 1000 proměnných na server interface

	S7-1200	CPU 1510...13	CPU 1515/16	CPU 1517/18
No. of nodes for server interfaces, max.	2,000	1,000	5,000	30,000

- Změňte PLC na S7-1515 (FW2.9) nebo vyšší
- Zkompilujte a přehrajte PLC
- Otevřete UA Expert, znovu načtete adresní prostor

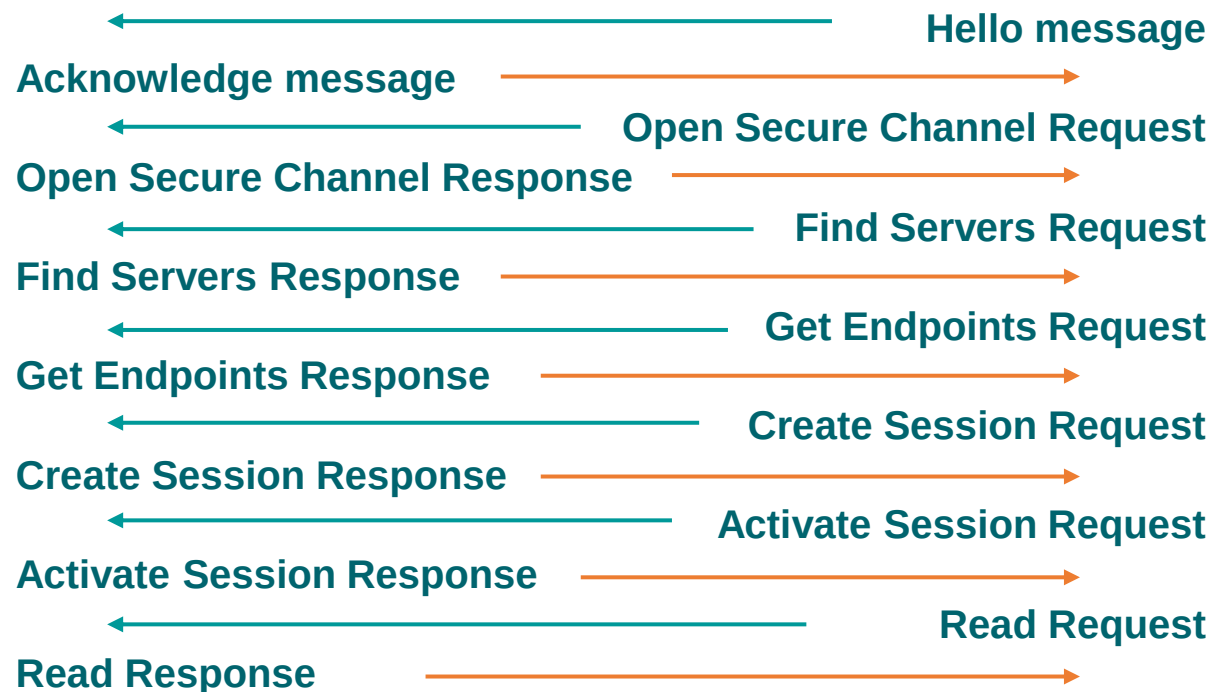
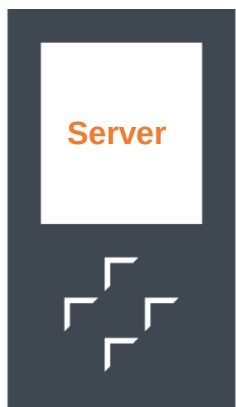


- Co vše se v OPC UA serveru objevilo navíc?
- Jaký identifikátor má proměnná pole?
- Kolik různých identifikátorů má proměnná pole?
- Jaký identifikátor má nově vytvořené rozhraní?
- Jaký datový typ má struktura z DB2 v OPC UA?
- Kde je tento datový typ definovaný?
- Co vše lze definovat u proměnných a OPC UA rozhraní v TIA? adresaci, jméno...

Komunikační relace

Připojení k serveru

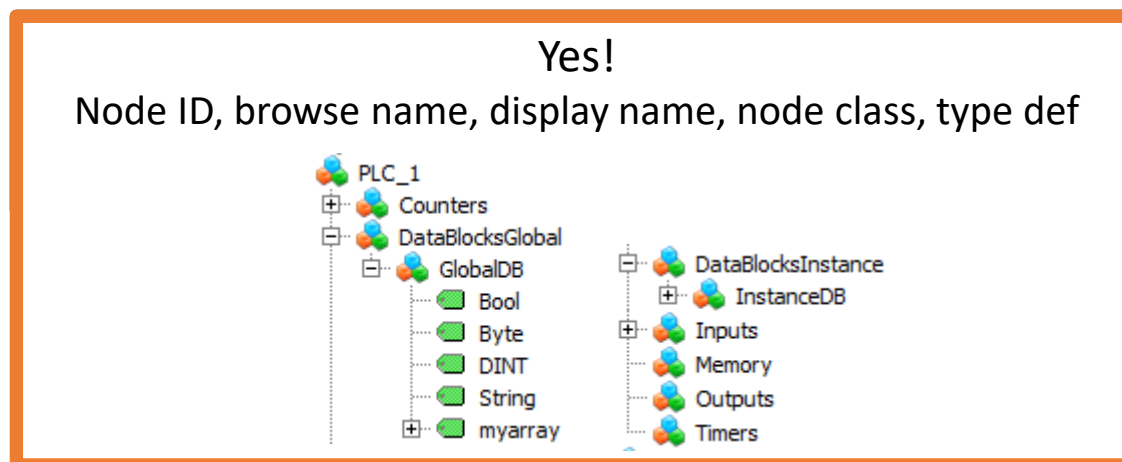
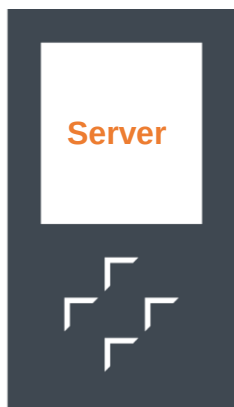
SIEMENS



Yes, I am!
Server state = running

Procházení serveru - browse

SIEMENS

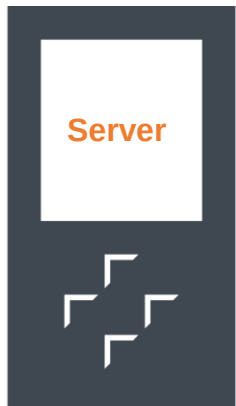


Způsoby čtení dat

- **Read – jednorázové přečtení hodnoty**
- **Registered Read – opakované čtení hodnoty**
 - Server si vytvoří nový číselný identifikátor čtené proměnné
 - Rychlejší metoda čtení
 - Vždy na žádost klienta
- **Subscription – monitorování změn hodnoty**
 - Klient požádá o sledování proměnné
 - Při změně hodnoty si server změnu zapíše a periodicky odešle klientovi
 - Nejlepší možnost pro kontinuální čtení dat
 - Sampling interval → perioda kontroly změn
 - Publishing interval → perioda odeslání dat
 - Pokud se hodnota změní vícekrát, je možné jich odeslat víc najednou s časovou značkou
- **Analogie ke čtení dat: write / registered write**

Čtení dat - read

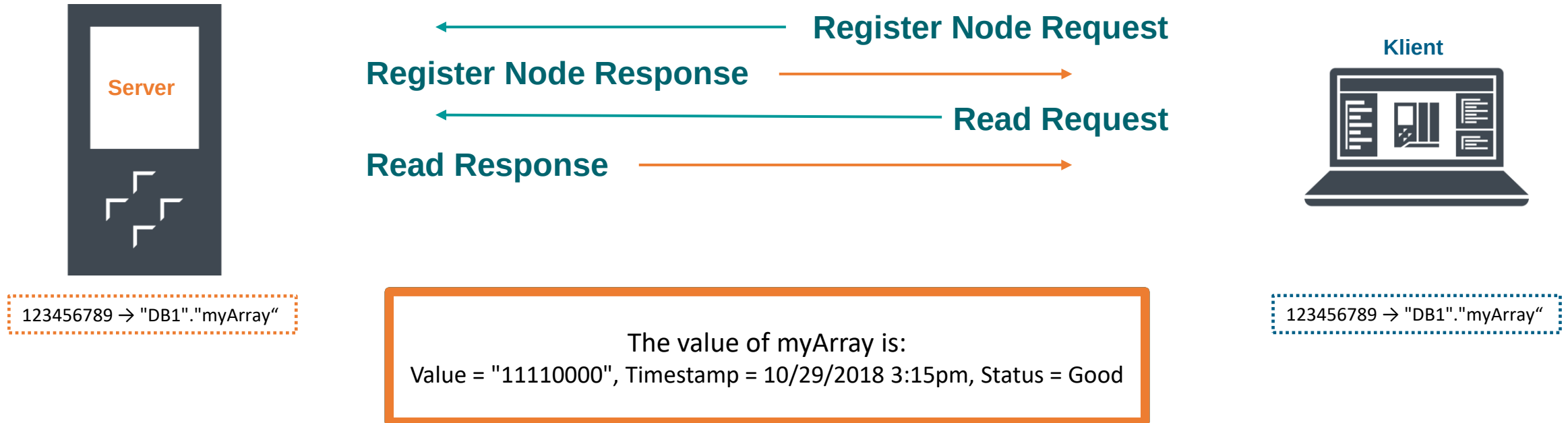
SIEMENS



Value = "11110000", Timestamp = 10/29/2018 3:15pm, Status = Good

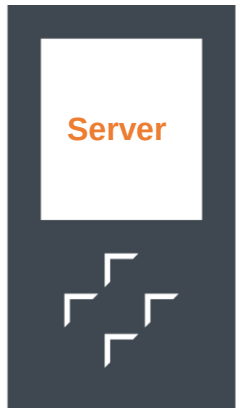
Čtení dat – registered read

SIEMENS

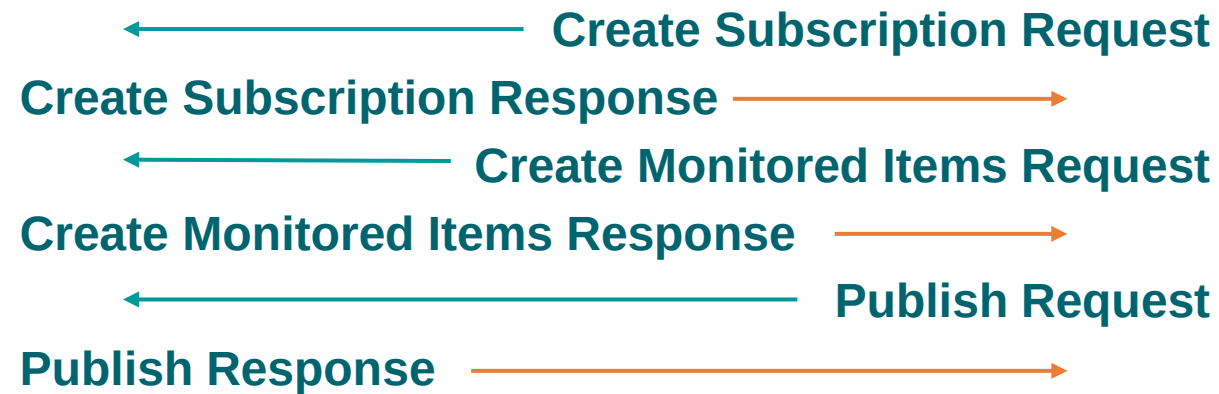


Čtení dat – subscription

SIEMENS



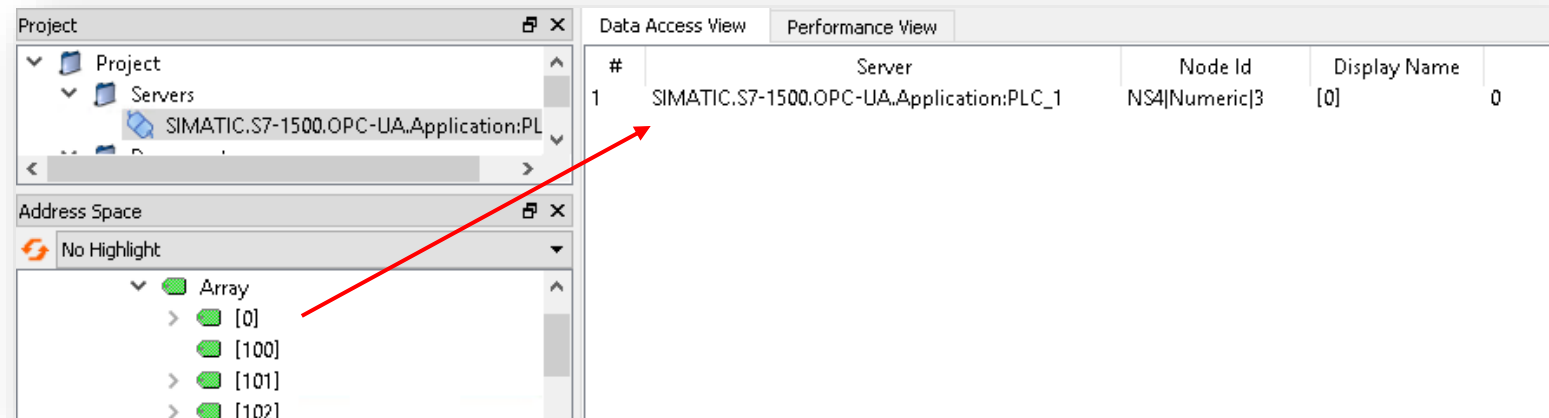
"DB1"."myArray" = 3



Requesting online values!



- V UA Expertovi si vyberte proměnnou a myší přetáhněte do prostředního okna

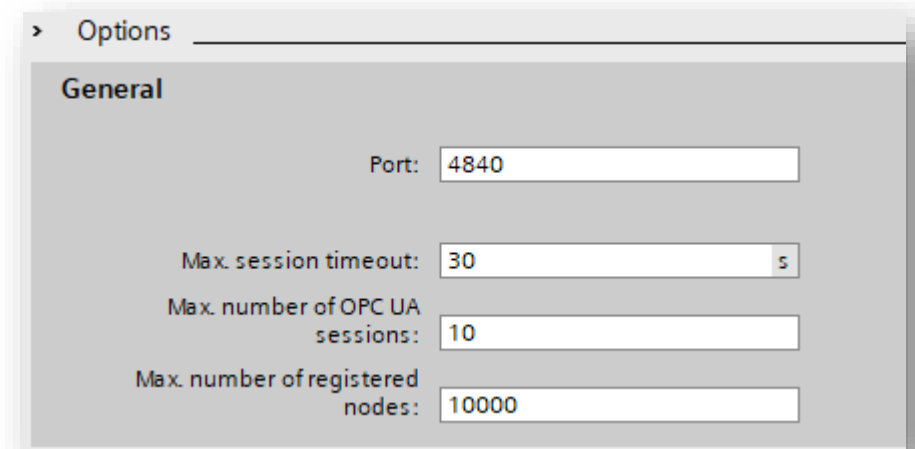
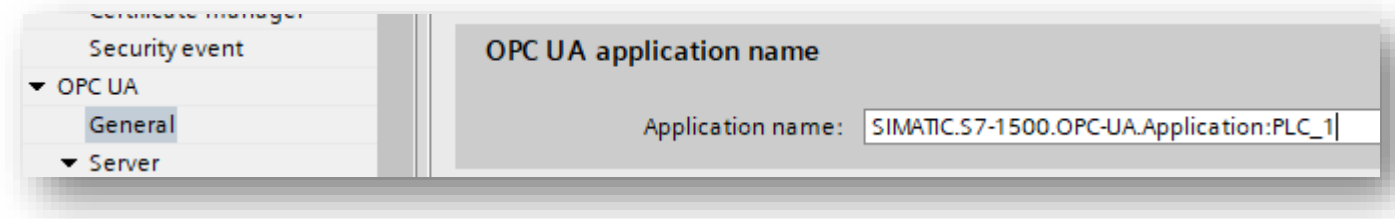


- 1) Jakou vzorkovací periodu požadoval klient a jaká byla nastavena? → log
- 2) Bude server odesílat více hodnot, pokud se během jednoho komunikačního cyklu hodnota změní vícekrát?
- 3) Odešle se první zaznamenaná hodnota nebo poslední?
- 4) Změňte publishing interval ("Subscription settings...") na 10000ms a zkontrolujte v logu.
- 5) Změňte sampling interval ("Monitored Item Settings...") na 3000ms a zkontrolujte v logu.
- 6) Změňte sampling interval ("Monitored Item Settings...") na 3001ms a zkontrolujte v logu.
- 7) Zapište do sloupce "Value" číselnou hodnotu. Co udělá klient? Jakou "instrukci" použije

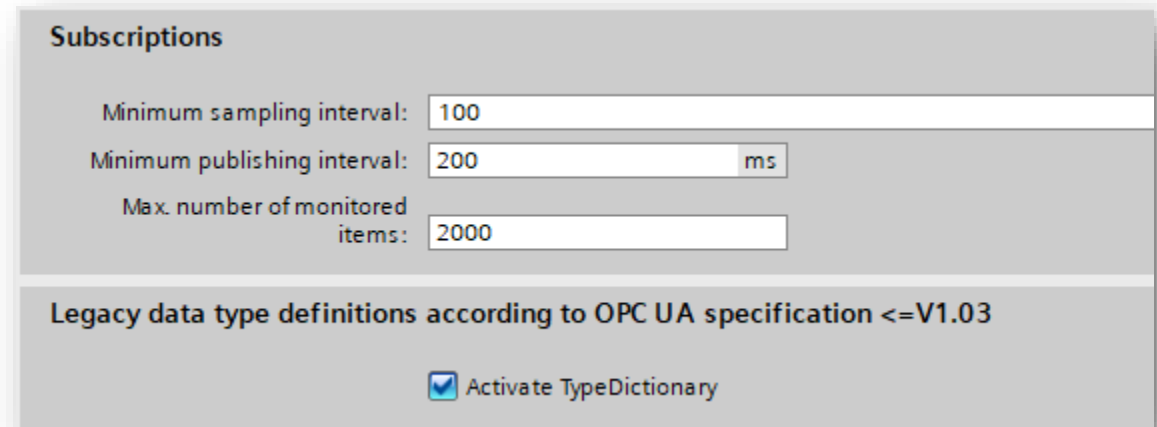
Parametry serveru

OPC UA server - options

- **Application Name:** jméno aplikace
- **Port:** přístupový TCP port
- **Max. session timeout:** doba bez výměny dat, po kterou server udržuje spojení s klientem
- **Max. number of OPC UA sessions:** maximální počet spojení k serveru (klientů)
- **Max. number of registered nodes:** maximální počet proměnných pro registrované čtení (registered read)
 - Proměnné nad tento limit jsou čteny klasicky (read)



- **Minimum sampling interval: minimální vzorkovací perioda**
 - Při monitorování proměnné je změna hodnoty identifikována nejrychleji s touto periodou
- **Minimum publishing interval: minimální interval pro odesílání dat**
 - Změna hodnoty je do klienta odeslána nejrychleji s touto periodou
 - Pokud je zaznamenáno více změn, jsou zapsány do řady a odeslány najednou
- **Max. number of monitored items: maximální počet sledovaných proměnných**
 - Platí pro všechny klienty dohromady
- **Activate TypeDictionary**
 - Vygeneruje popis strukturovaných datových typů použitých v OPC UA serveru pro klienty se starší verzí standardu



The screenshot shows a configuration window titled "Subscriptions". It contains three input fields: "Minimum sampling interval" with a value of 100, "Minimum publishing interval" with a value of 200 and a unit dropdown set to "ms", and "Max. number of monitored items" with a value of 2000. Below these fields is a section titled "Legacy data type definitions according to OPC UA specification <=V1.03" which includes a checked checkbox labeled "Activate TypeDictionary".

Parameter	Value
Minimum sampling interval	100
Minimum publishing interval	200 ms
Max. number of monitored items	2000

Legacy data type definitions according to OPC UA specification <=V1.03

☒ Activate TypeDictionary

Restart OPC UA serveru při přehrání PLC

SIEMENS

- Změna FB, FC, OB, komentářů



- Přidání nových DB nepřístupných v OPC UA



- Přidání nových DB přístupných v OPC UA



- **Změna současných DB**
včetně DB nepřístupných z OPC UA



- **Odstranění současných DB**
včetně DB nepřístupných z OPC UA



- restart neproběhne



- restart proběhne

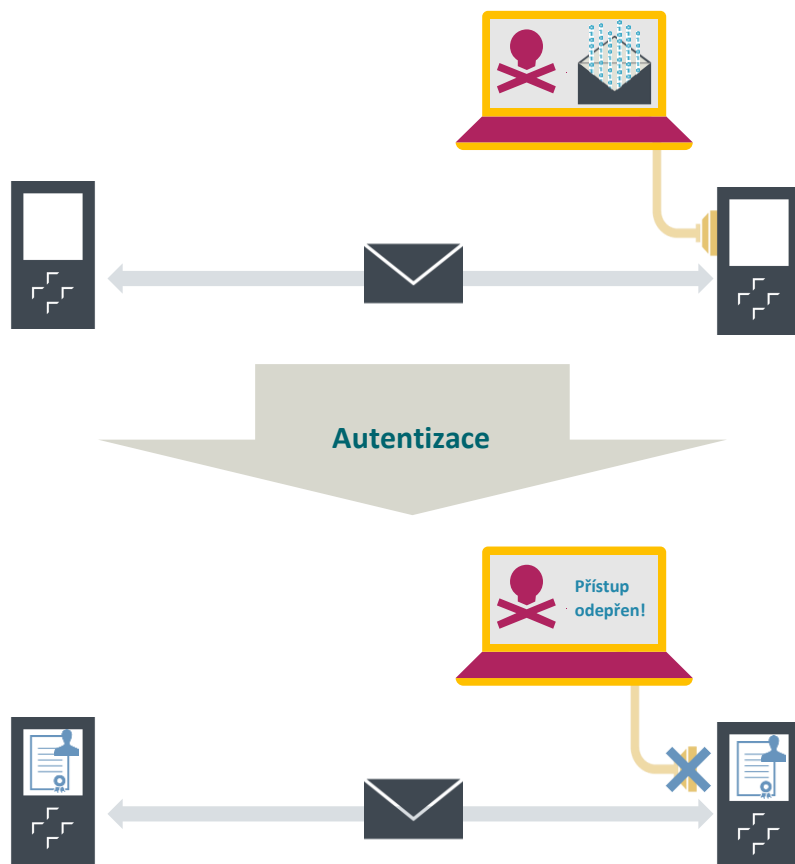
Bezpečnost

- Komunikace mezi serverem a klientem je zabezpečena certifikátem (aplikační certifikát)
- Certifikát slouží k podpisu a šifrování
 - Je tedy zajištěna identita obou komunikačních partnerů
 - A data nejsou čitelná (editovatelná) pro nikoho jiného
- Profily u S7-1200 a S7-1500
 - **No security → používat pouze pro testy a uvedení do provozu**
 - Basic128Rsa15 – Sign
 - Basic128Rsa15 – Sign & Encrypt
 - Basic256 – Sign
 - Basic256 – Sign & Encrypt
 - **Basic256Sha256 – Sign → nešifruje data, jsou čitelná pro každého**
 - Basic256Sha256 – Sign & Encrypt → **jediné dostatečné zabezpečení**
- Bezpečnost na úkor rychlosti (?)
- Přístup může být omezen i uživatelským jménem a heslem

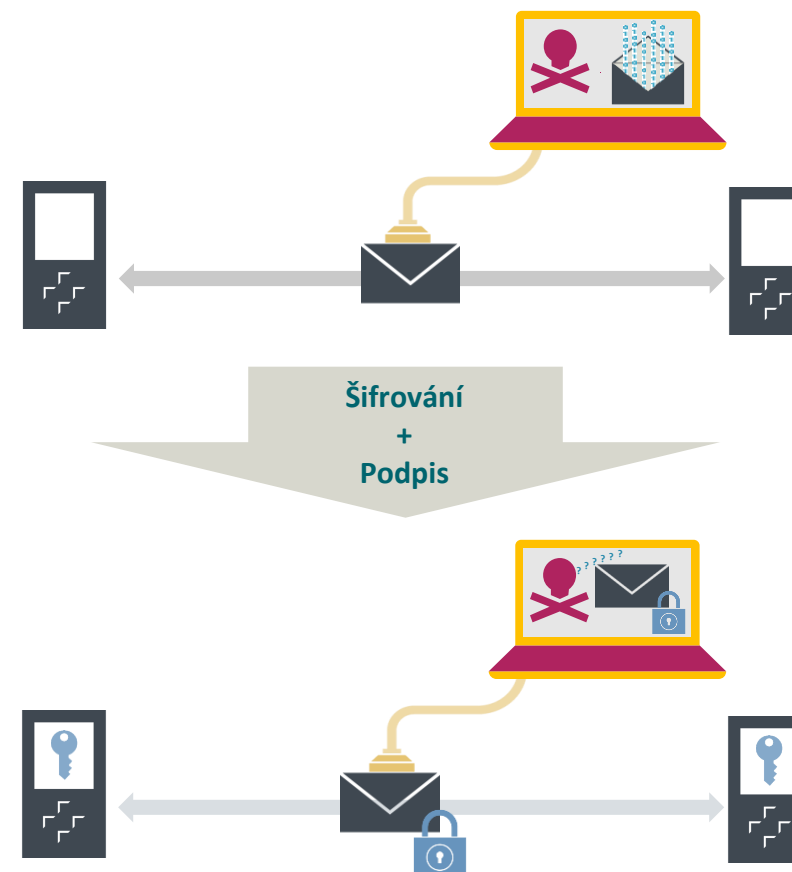


dnes již neposkytují dostatečné zabezpečení

Kdokoliv se může připojit k PLC



Data mohou být přečtena a změněna

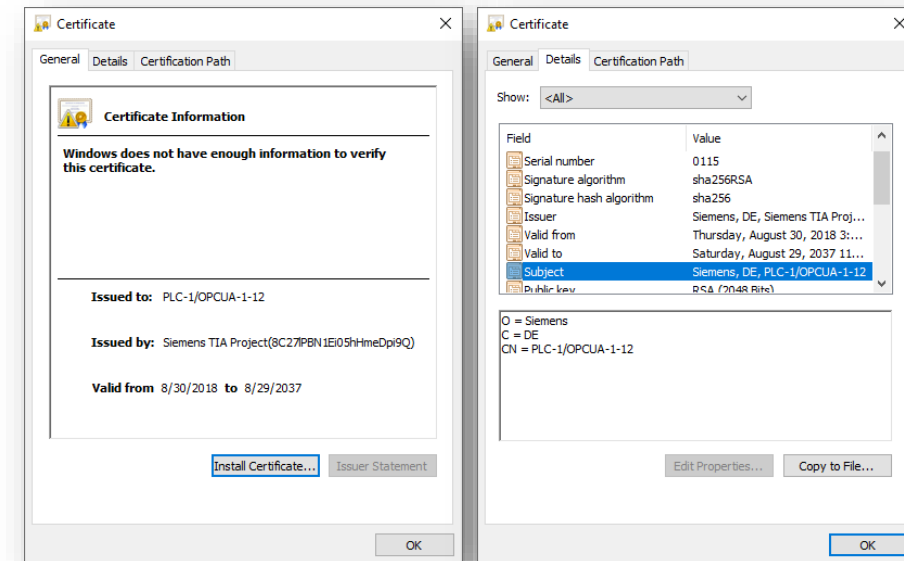


Bezpečnost - certifikáty

- ITU X.509 standard
- Certifikát musí mít každý účastník komunikace

Certifikát obsahuje verzi, sériové číslo, šifrovací a hashovací algoritmus, vydavatele, certifikační autoritu, časový rozsah platnosti, subjekt, kterému certifikát patří, veřejný klíč a jeho parametry

- Při zahájení komunikaci si obě strany vymění certifikáty
- Komunikace může být zahájena, jen pokud si obě strany důvěřují (certifikátům partnera)
- Certifikát může být podepsaný sebou (self signed) nebo certifikační autoritou (CA signed)
 - V tomto případě může být komunikace zahájena i když druhá strana důvěřuje dané autoritě
 - Certifikační autoritou může být i TIA Portal
- Certifikáty OPC UA serveru lze vytvořit i v TIA Portalu nebo je možné je importovat
- Správa OPC UA certifikátů je možná z TIA Portalu nebo z OPC UA klienta (GDS Push)
- Certifikáty podepsané autoritou, které již nejsou důvěryhodné musí být zapsány na Certificate revocation list



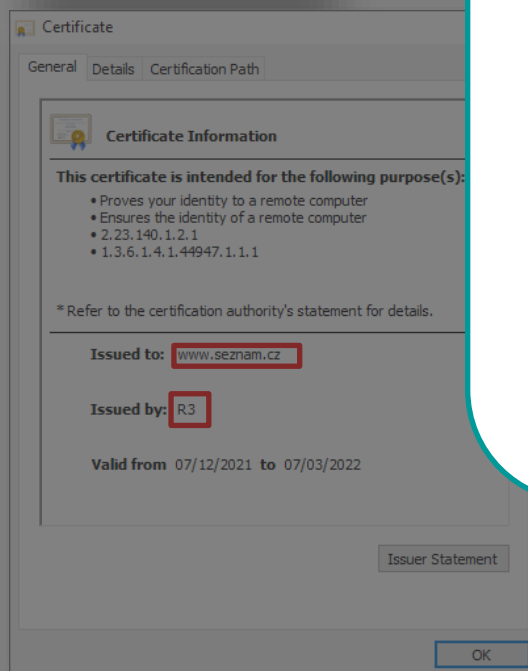
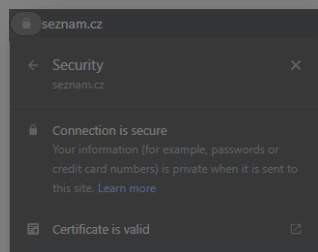
- Příklad: seznam.cz

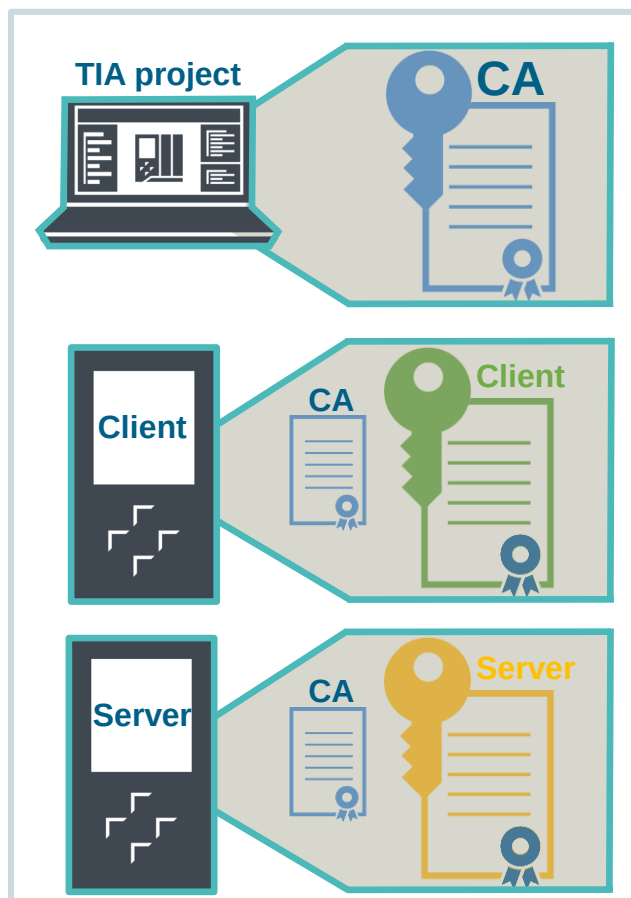
TLS – transport layer security (1999)
dříve ssl – secure sockets layer (1995)

Bezpečnostní prvek používaný ve většině moderních komunikacích

- Webové stránky
- Internetové platby

OD TIA V17 je implementován pro PG/PC a HMI komunikaci s PLC!

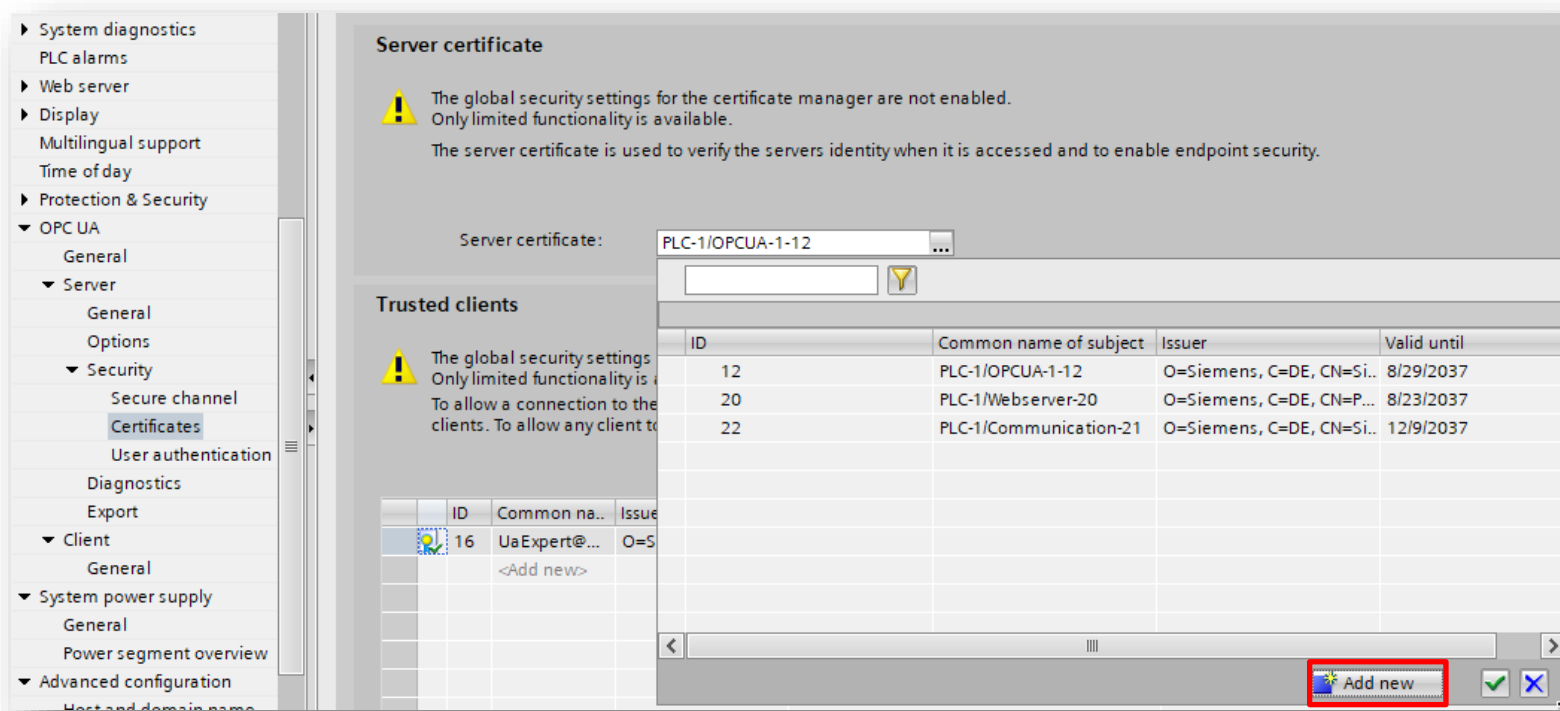




V TIA Portalu lze generovat certifikáty pro OPC UA server, klient, CA i jiné služby (web server, OUC, VPN...)

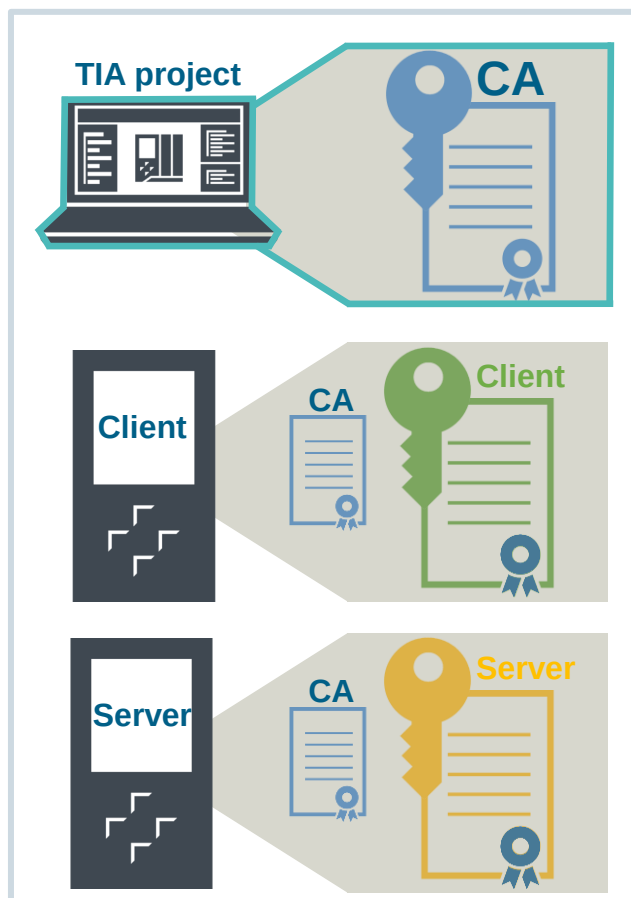
Certifikáty lze generovat v HW konfiguraci – např. pro OPC UA server

Po zapnutí OPC UA se certifikát vygeneruje automaticky

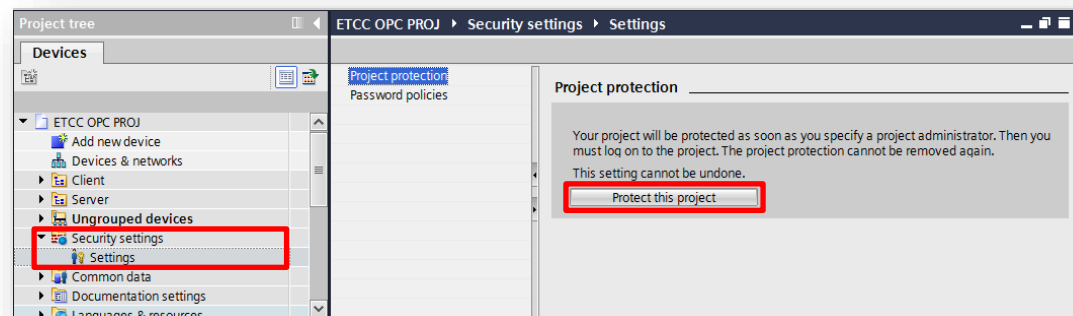


TIA Portal jako certifikační autorita

SIEMENS

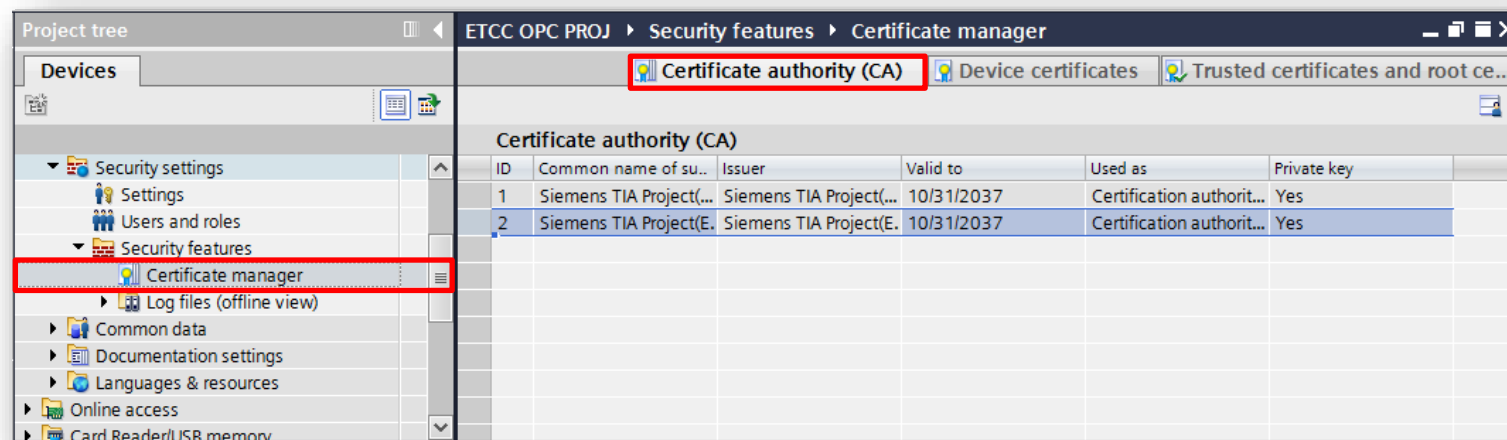


TIA Portal poskytuje certifikační autoritu pro podpis certifikátů zařízení



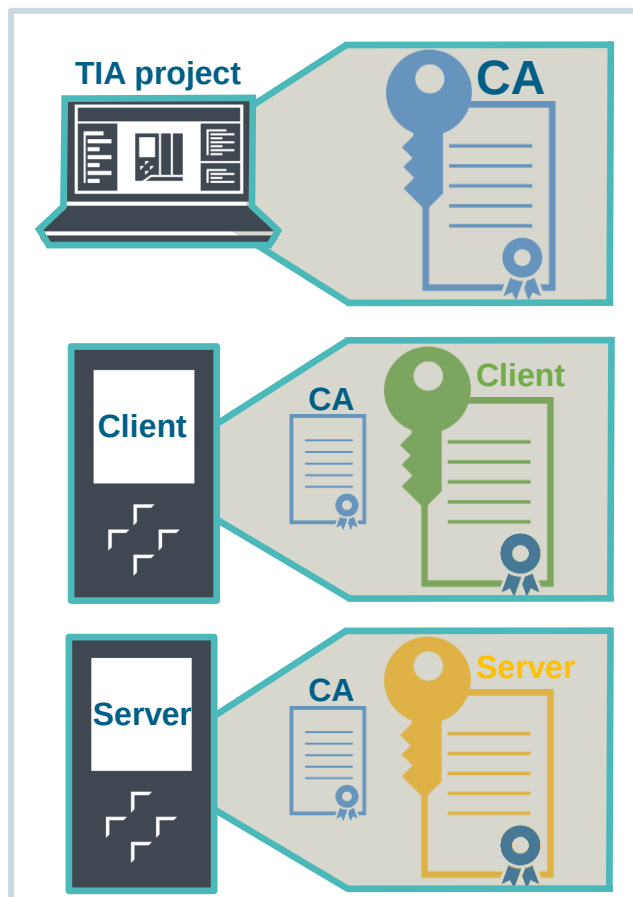
Projekt je nutno chránit heslem, aby certifikáty byly bezpečně uloženy

Ochrana projektu heslem aktivuje globální správu certifikátů:



Generování certifikátů v TIA Portalu

SIEMENS



Zde se spravují certifikáty zařízení v TIA projektu i důveryhodných komunikačních partnerů (OPC UA, VPN, HTTPS...)

06.05.2022

Certifikáty lze generovat v global certificate manageru – pro různé účely

ID	Common name of subject	Serial number	Issuer	Serial number issuer	Valid to	Used as
5	SCALANCE M876-4(v3CpUFxId...	03	O = Siemens, C = DE, CN = Sie...	00	Thursday, March 19, ...	SSL certificate of mo...
12	PLC-1/OPCUA-1-12	0115	O = Siemens, C = DE, CN = Sie...	00	Saturday, August 29, ...	Certificate (Digital Si...
20	PLC-1/Webserver-20	19	O = Siemens, C = DE, CN = PLC...	00	Sunday, August 23, ...	SSL certificate of mo...
22	PLC-1/Communication-21	537064E...	O = Siemens, C = DE, CN = Sie...	340F0770FEA65EB7	Wednesday, Decemb...	SSL certificate of mo...

Buttons: Create, Import

Typ podpisu (vlastní / certifikační autority)

Certifikát certifikační autority

Název subjektu

Šifrovací algoritmus (RSA / EC)

Délka klíče

Hash algoritmus

Platnost certifikátu (Pozor na čas v PLC!)

Použití certifikátu (web server, OPC UA, VPN...)

Adresy subjektu (IP, jméno, email, URI)

Create certificate

Certificate authority (CA)

Select how the new certificate will be signed:

- ☐ Self signed
- ☒ Signed by certification authority

CA name: Siemens TIA Project - DemoRack-V17 [Select]

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1-OPCUA-Server

Encryption method: RSA

Encryption parameter: 2048

Hash algorithm: sha256

Valid from: January 13, 2022 10:24:04 AM

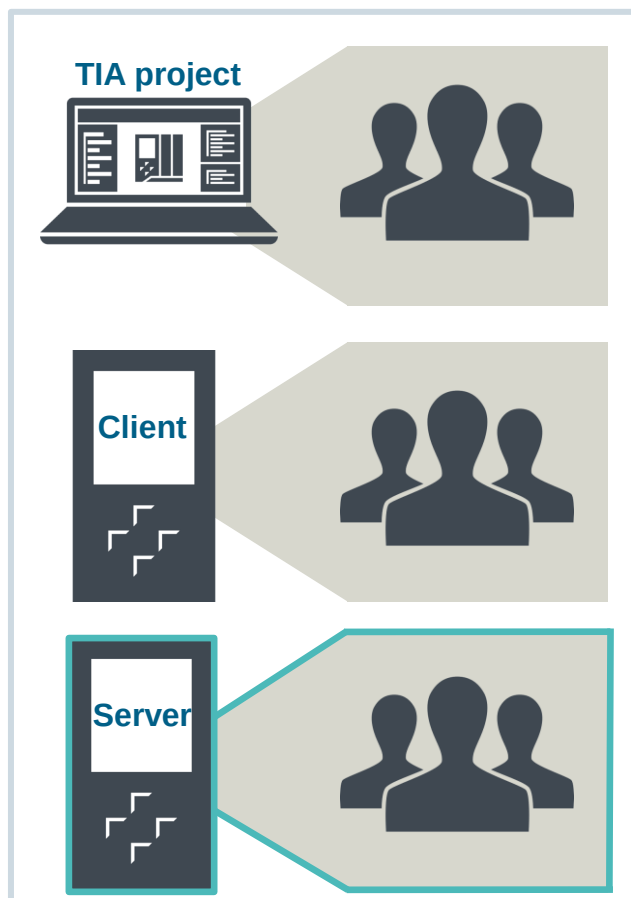
Valid until: January 13, 2037 01:00:00 AM

Usage: OpcUa Server

Subject Alternative Name (SAN):

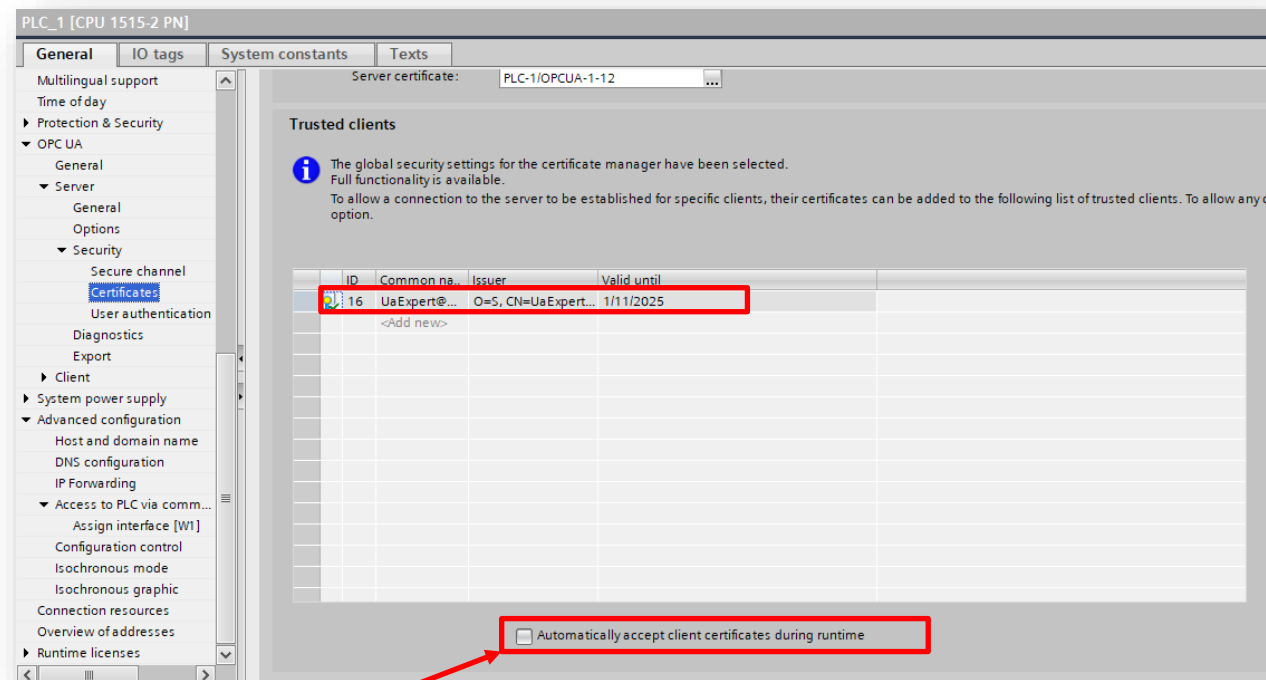
Type	Value
IP	192.168.0.1
<Add new>	

OK Cancel



TIA Portal poskytuje globální správu certifikátů

Vložení certifikátů důvěryhodných klientů:



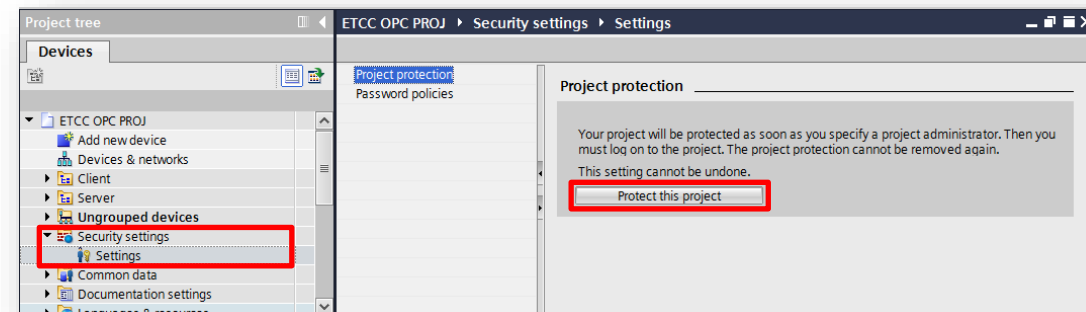
Tímto se akceptují certifikáty všech klientů – nebezpečné!

**Postup:**

- 1) Zabezpečit projekt jménem a heslem
- 2) Vygenerovat certifikát OPC UA serveru podepsaný certifikační autoritou
- 3) V PLC povolit použití Certificate manageru
- 4) Vložit do PLC vygenerovaný certifikát pro OPC UA server
- 5) Vložit do Certificate manageru certifikát UA Experta
- 6) Certifikát UA Experta vložit do důvěryhodných klientů OPC UA serveru
- 7) Vypnout automatické akceptování klientských certifikátů
- 8) Exportovat certifikát certifikační authority a certificate revocation list
- 9) Vložit certifikát certifikační authority do UA Experta
- 10) Přehrát HW konfiguraci PLC
- 11) Připojit se klientem přes zabezpečený kanál z UA Experta



- Otevřete security settings a zabezpečte projekt jménem a heslem



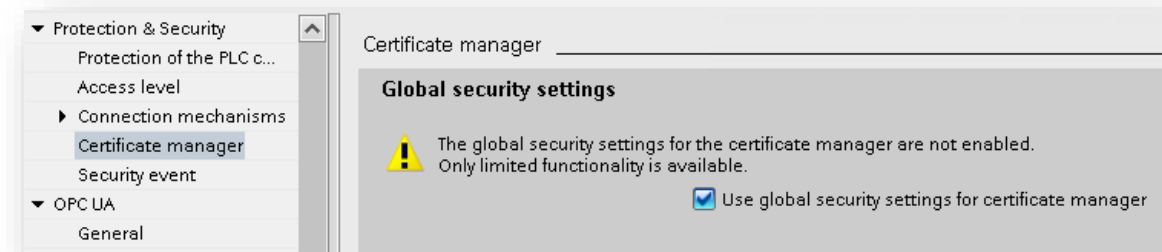
- Otevřete Certificate manager → Device certificates
- Vygenerujte OPC UA server certifikát pro PLC
 - Začněte od konce → nastavte “Usage”
 - Podepište certifikát certifikační autoritou TIA
 - Zvolte libovolné jméno subjektu
 - Šifrovací a hashovací parametry ponechte
 - Zkontrolujte platnost certifikátu
 - Vložte IP adresu PLC

Device certificates

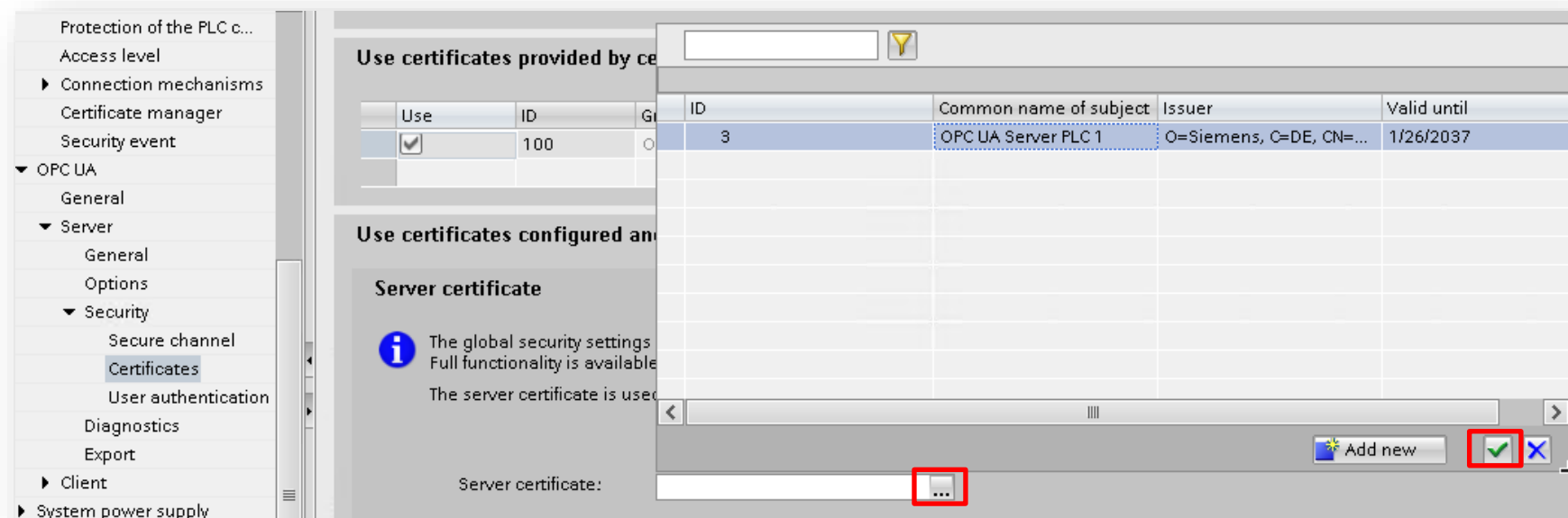
ID	Common name of subject	Serial number	Issuer	Serial number issuer	Valid to	Used as	Private key	Signature algorithm	Responsibility
3	OPC UA Server PLC 1	041C5C42BC6486F0	O = Siemens, C = DE, CN = Siemens TIA Project - OPC UA workshop	7EBD6F9D96323BEA	Monday, January 26, 2037	Certificate (Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign)	Yes	RSA-SHA256	User



- V HW konfiguraci povolte použití Certificate manageru

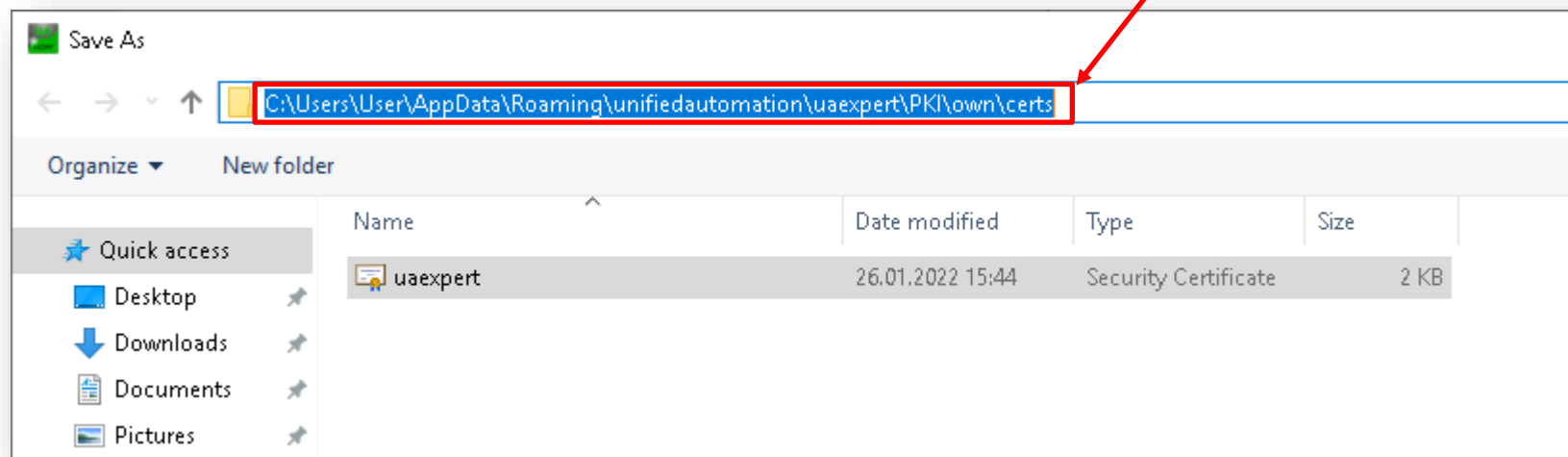
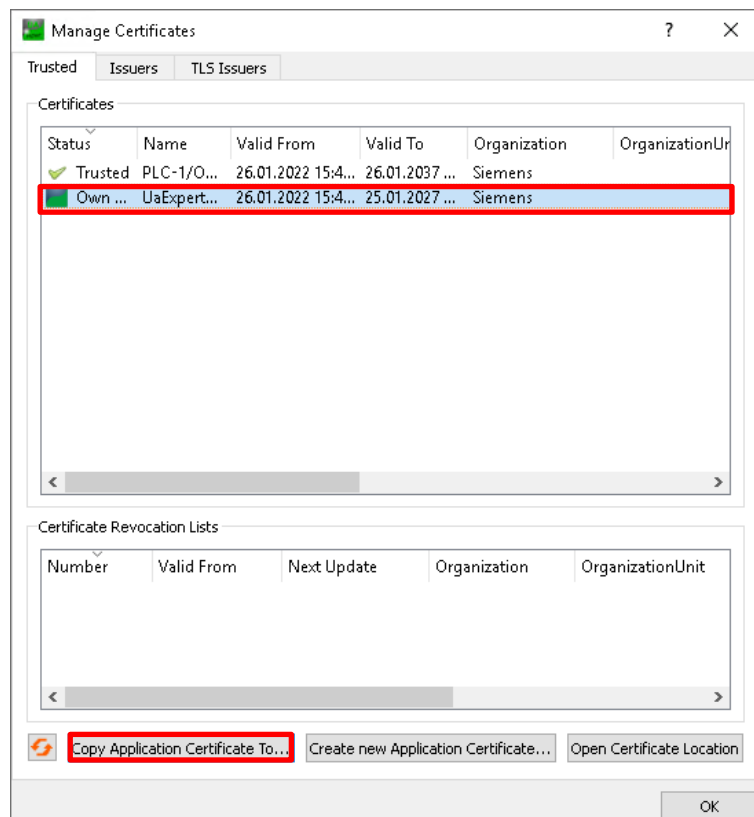
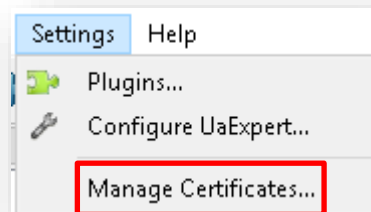


- V nastavení OPC UA serveru vložte nově vygenerovaný certifikát



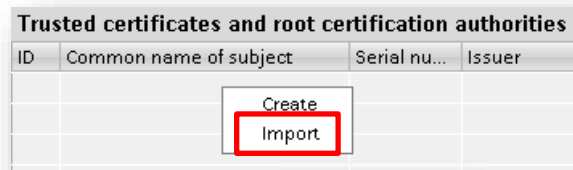


- Otevřete UA Expert
- Otevřete správce certifikátů
- Zkopírujte cestu k certifikátu

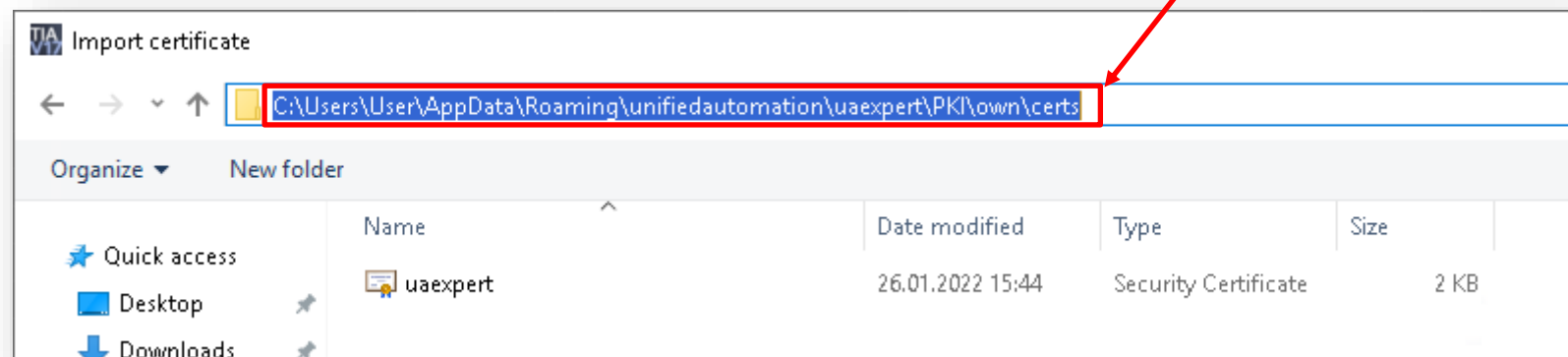




- Otevřete Certificate manager v TIA → Trusted certificates and root certification authorities
- Importujte certifikát UA Experta



- Vložte cestu ke složce s certifikátem
- Vyberte certifikát → Open



Trusted certificates and root certification authorities							
ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signa...
4	UaExpert@TIA-V17	61F15E3E	CN = UaExpert@TIA-V17, O = S...	Monday, January 25, ...	Certificate (Digital Si...	No	RSA-S...



- Vložte certifikát UA Experta mezi důveryhodné klienty v HW konfiguraci PLC
- Vypněte automatické akceptování klientských certifikátů

Trusted clients

i The global security settings for the certificate manager have been selected. Full functionality is available.
To allow a connection to the server to be established for specific clients, their certificates can be added to the following list of trusted clients. To allow any

ID	Common name of subject	Issuer	Valid until
1	Siemens TIA Project - OP...	O=Siemens, C=DE, CN=...	1/26/2037
2	Siemens TIA Project - OP...	O=Siemens, C=DE, CN=...	1/26/2037
3	OPC UA Server PLC 1	O=Siemens, C=DE, CN=...	1/26/2037
4	UaExpert@TIA-V17	O=Siemens, CN=UaExpe...	1/25/2027

☐ Automatically accept client certificates during runtime



- Otevřete Certificate manager → Certificate authority (CA)
- Exportujte Certifikát autority (ten, kterým jste podepsali certifikát serveru)
- Neexportujte privátní klíč!

Certificate authority (CA)		
ID	Common name of subject	Serial number
1	Siemens TIA Project - OPC UA workshop	02E04E
2	Siemens TIA Project - OPC UA workshop	06F
		Export Assign Show

Export certificate

☐ Include certificate chain (in the export)

☐ Include private key (in the export)

Encryption for private key: None

Enter a password for the private key. If you do not enter a password, the project name will be used as the password.

Password: Very weak

Confirm password:

Export Cancel

- Exportujte Certificate revocation list

Certificate authority (CA)		
ID	Common name of subject	Serial number
1	Siemens TIA Project - OPC UA workshop	02E04E
2	Siemens TIA Project - OPC UA workshop	06F
		Export Assign Show

File name: Siemens TIA Project - OPC UA workshop_X.509 Certificate_1

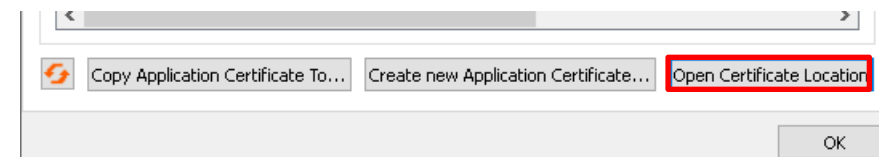
Save as type: Certificate - Certificate revocation list, DER coded (unencrypted) (*.crl)

Save in: de Folders

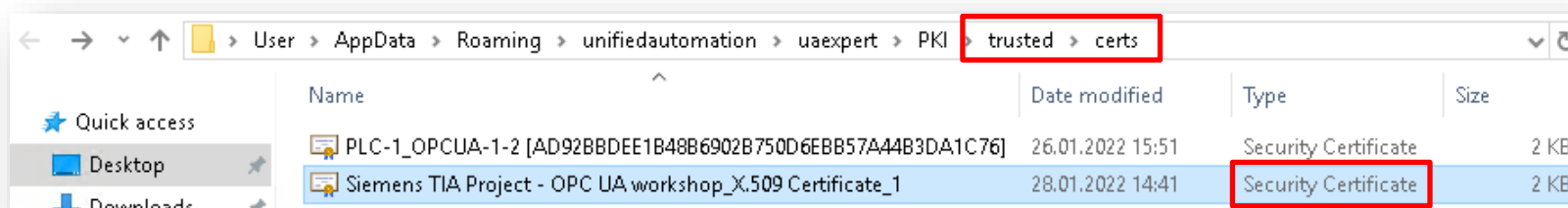
Certificate - DER coded (unencrypted) (*.der)
 Certificate - DER coded (unencrypted) (*.cer)
 Certificate - PEM coded (*.crt)
 Certificate - PEM coded (*.pem)
 Certificate - Certificate revocation list, DER coded (unencrypted) (*.crl)
 PKCS12 archive - certificate and private key (*.p12)
 PKCS12 chain archive - certificate and private key (*.p12)



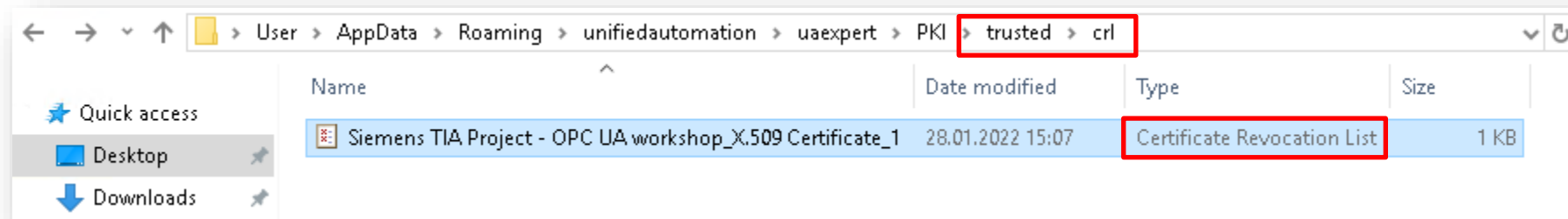
- Otevřete správce certifikátů v UA Expertovi
- Otevřete složku s důveryhodnými certifikáty



- Do této složky zkopírujte exportovaný certifikát certifikační authority (.der)



- Do složky s certificate revocation listy zkopírujte exportovaný certificate revocation list (.crl)



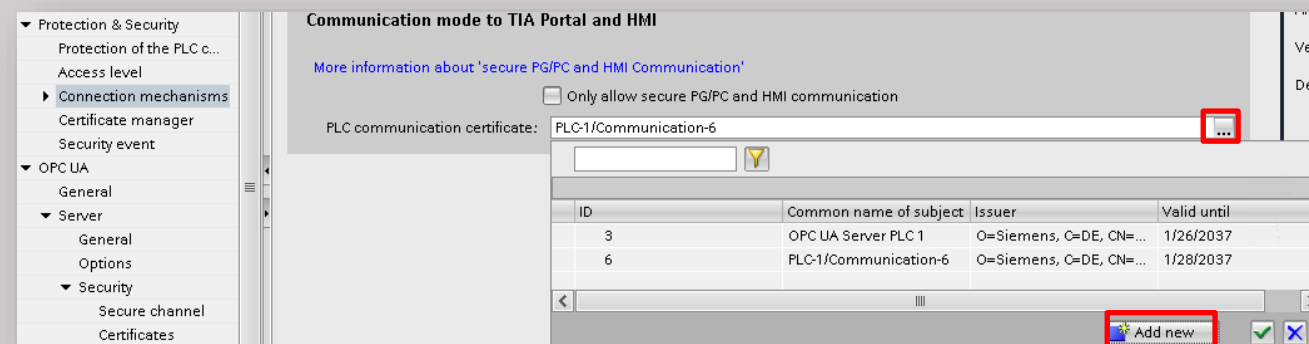


- Přehrajte HW konfiguraci PLC

Chyba při kompilaci: z důvodu zapnutí certificate manageru v PLC je nutno vytvořit certifikát pro TLS komunikaci s PLC

!!!! Toto nesouvisí s tématem OPC UA !!!!

- TLS komunikace s PLC je novinka v TIA Portalu V17
- Díky tomu je komunikace mezi TIA/HMI a PLC šifrovaná
- Je nutno vygenerovat certifikát – v HW konfiguraci
- “Add New” → “OK”



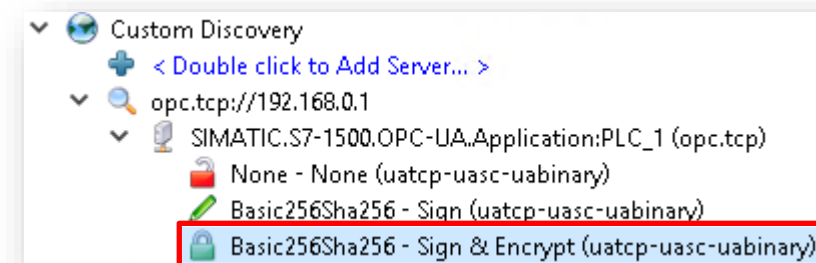
- Připojte se k OPC UA serveru z UA Experta přes zabezpečený kanál



- Klient by neměl požadovat žádné bezpečnostní kontroly

- Protože má CA certifikát i CRL

- Spojení server-klient je nyní bezpečné



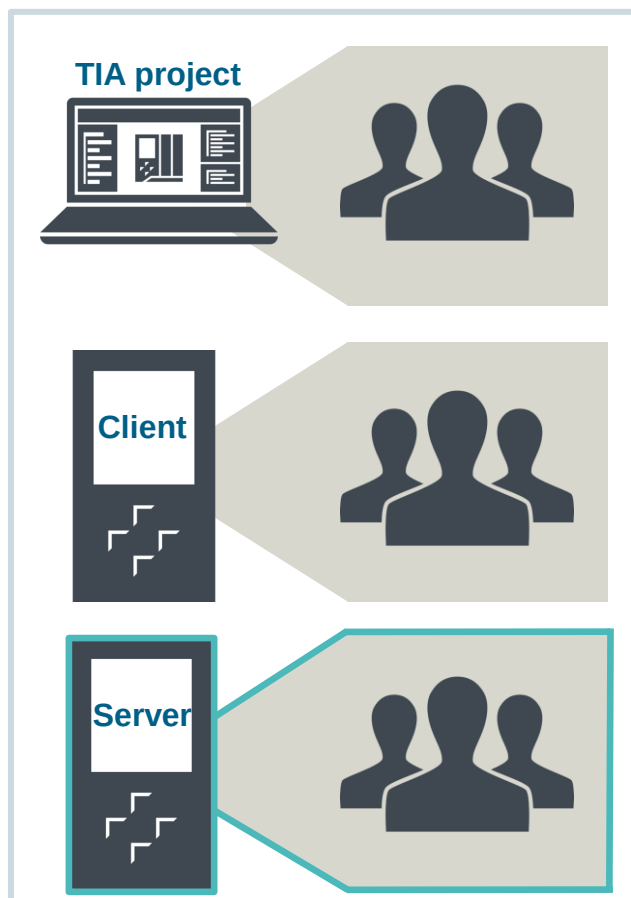
Zabezpečené připojení k serveru

Shrnutí

- 1) Vytvoření certifikátu pro OPC UA server v PLC – podepsaný autoritou
- 2) Vložení klientského certifikátu mezi důvěryhodné v HW konfiguraci PLC
- 3) Vložení certifikátu CA a CRL do klienta

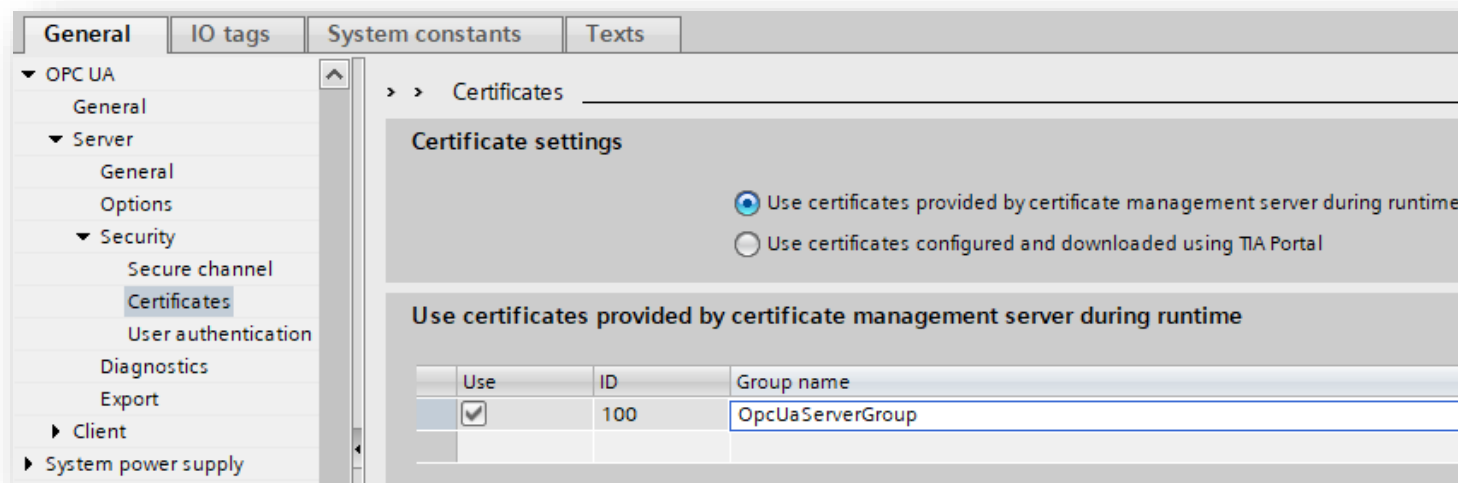
Klient se připojí k serveru a navzájem si vymění certifikáty

- **server má certifikát klienta v HW konfiguraci**
- **klient důvěřuje CA, která serveru podepsala certifikát**
- **zabezpečená komunikace může začít**
- **nikdo kromě serveru, klienta a vlastníka TIA projektu komunikaci nerozluští**
- **nikdo jiný také nezmění odesílaná data, aniž by si toho server či klient nevšiml**

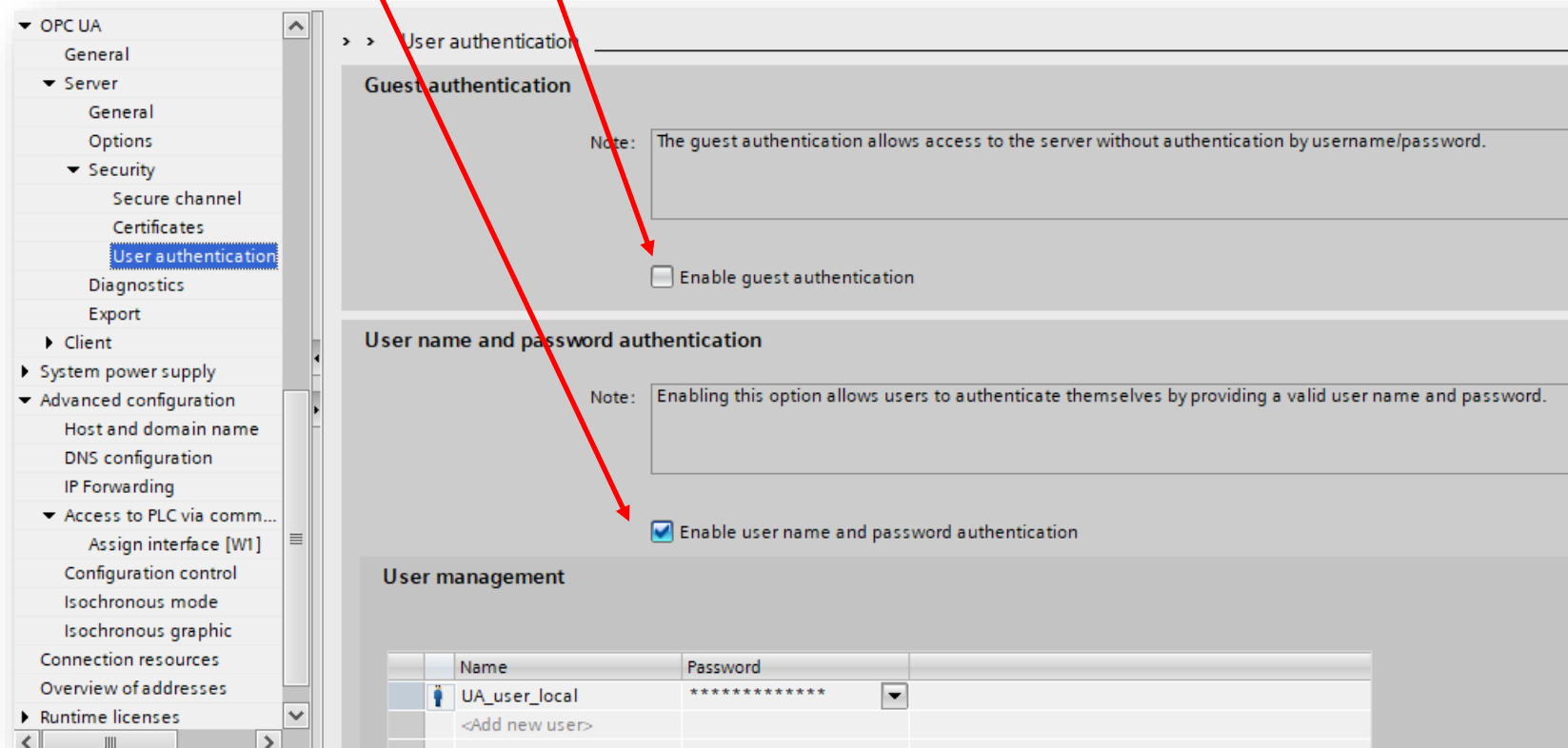


TIA Portal poskytuje globální správu certifikátů

- **Certifikáty lze spravovat i OPC UA klientem**
 - Certifikát serveru i důveryhodných klientů
 - Také nedůveryhodných klientů – již nebezpečné certifikáty
- **Není nutno mít TIA Portal pro správu certifikátů**
 - Nejbezpečnější metoda
- [SIOS – GDS Push](#)



- Uživatele oprávněného k přístupu k OPC UA serveru lze definovat v HW konfiguraci PLC
- Povolení uživatelského přístupu bez hesla (guest)
- Přístup pouze po zadání jména a hesla



- **Globální správa uživatelů v TIA projektu** – funguje zároveň s nastavením uživatelů v HW konfiguraci PLC
- **Jeden uživatelů má práva pro správu a přístup k více zařízením**

General user management

Note: User management via the project security settings is only enabled if the project status is set to protected with the settings options of the security settings.

☒ Enable additional user management via project security settings

Project tree

Devices | Plant objects

- ▶ HMI_3 [KTP400 Basic PN]
- ▶ PC-System_1 [SIMATIC PC station]
- ▶ WM-FPP58B9HOP2 [SIMATIC PC station]
- ▶ Drive unit_1 [S210 PN]
- ▶ Router_1 [SCALANCE M876-4]
- ▶ Security_1 [SCALANCE S615]
- ▶ XC208 [SCALANCE XC208]
- ▶ Ungrouped devices
- ▼ Security settings
 - Settings
 - Users and roles
 - ▶ Security features
 - Cross-device functions
 - Common data

DemoRack_V17 ▶ Security settings ▶ Users and roles

Users | User groups | Roles

Roles

Name	Description	Maximum sessi...	Comment
NET Diagnose	System-defined role "NET Diagnose"	30 Min	
Control panel	User-defined role	30 Min	
Unified administrator	User-defined role	30 Min	
UA_user	User-defined role	30 Min	
<Add new role>			

Engineering rights | Runtime rights | User-specific runtime rights

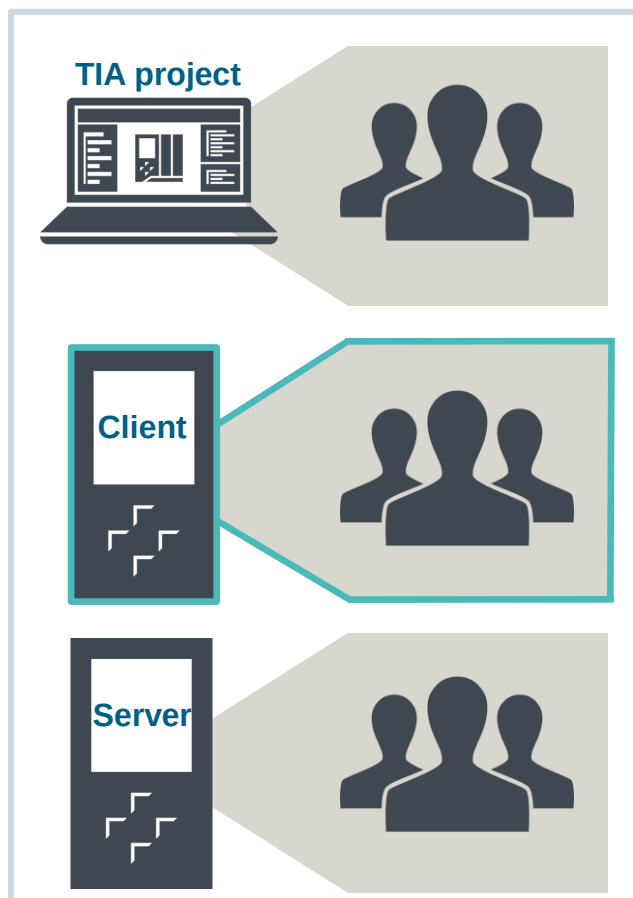
Function rights c...

▼ S7-1500 V2.9

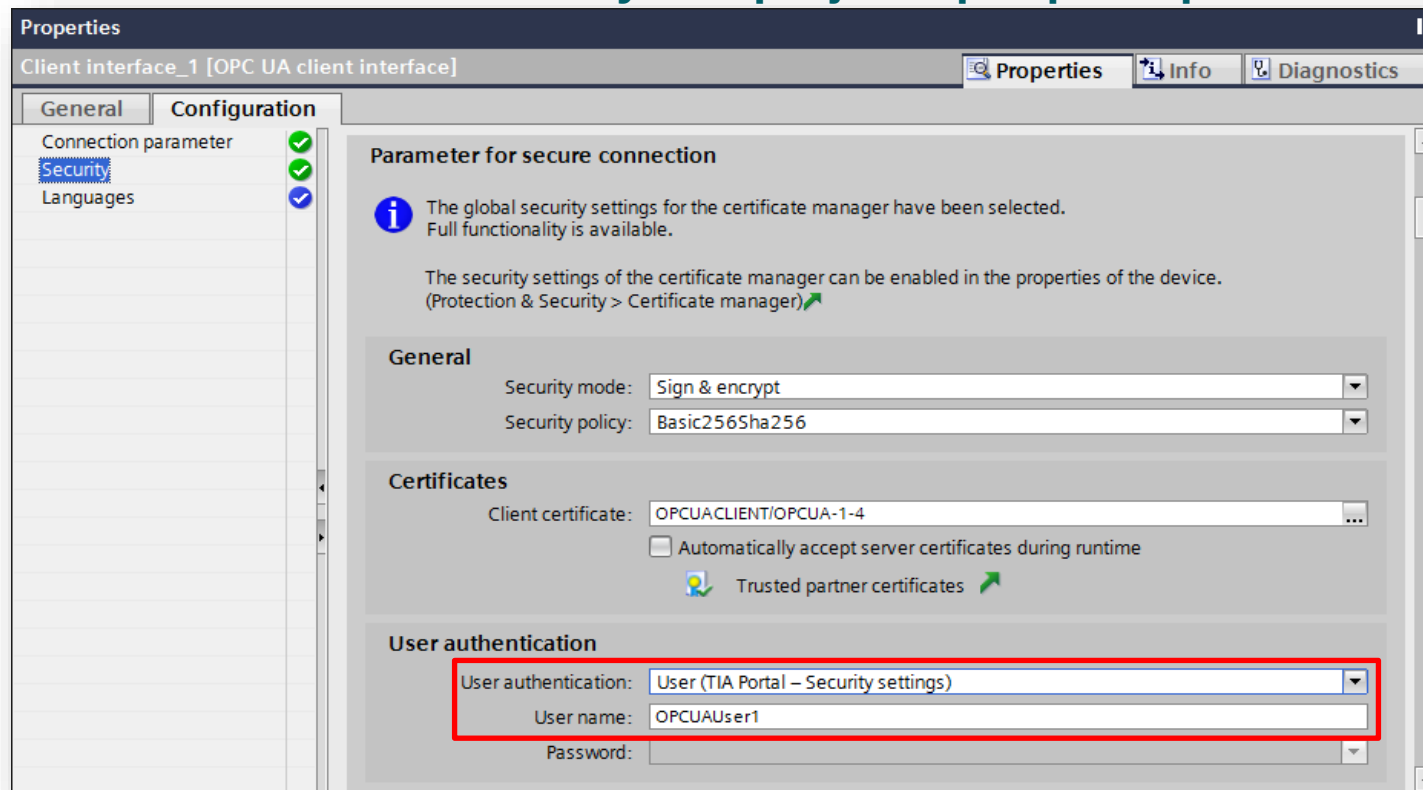
PLC_1

Function rights

Name	Group	Comment
☐ User authentication of the OPC UA client		
☒ OPC UA server access		
☐ Manage certificates		

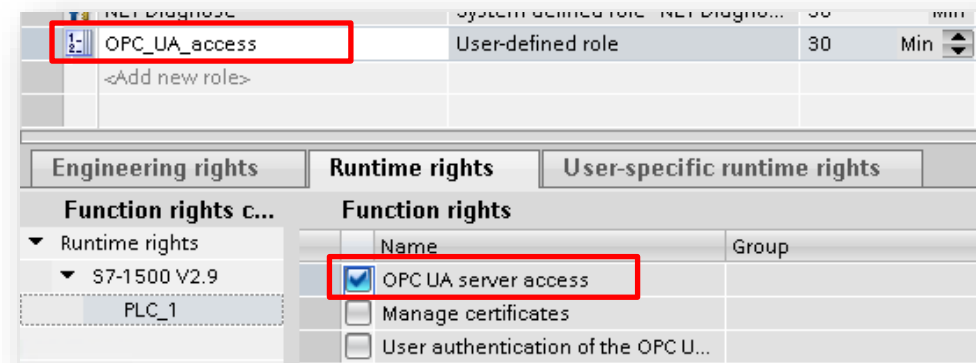


Použití uživatelů definovaných v projektu pro přístup k serveru:

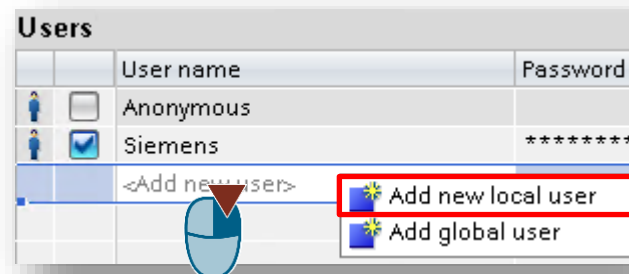




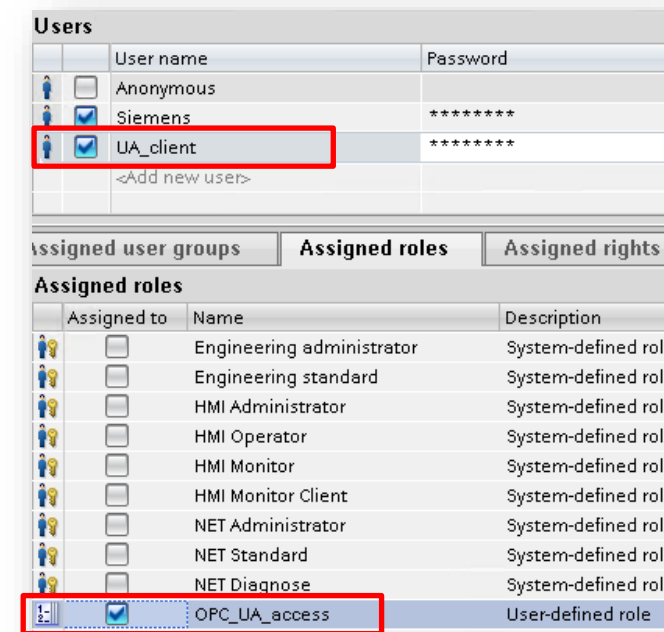
- V záložce Roles vytvořte novou roli
 - Roli přiřadte práva pro přístup k OPC UA server S7-1500



- Otevřete Security settings → Users and roles
- Vytvořte lokálního uživatele

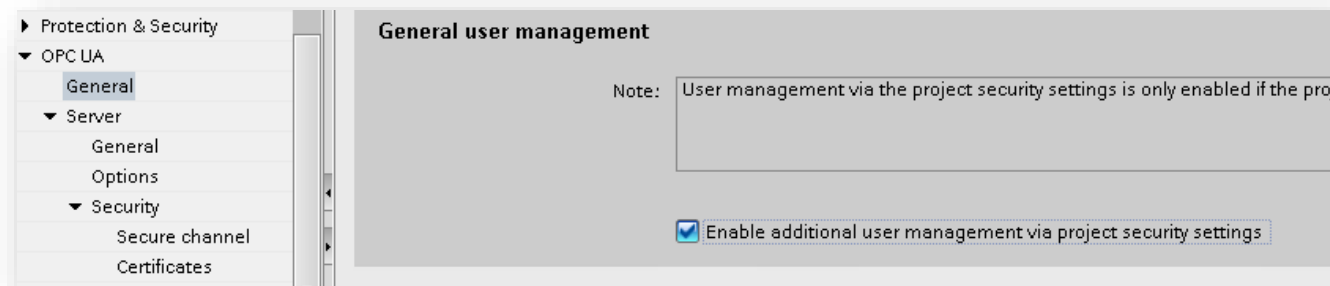


- V záložce Users vytvořte lokálního uživatele
 - Přiřadte mu nově vytvořenou roli OPC_UA_access



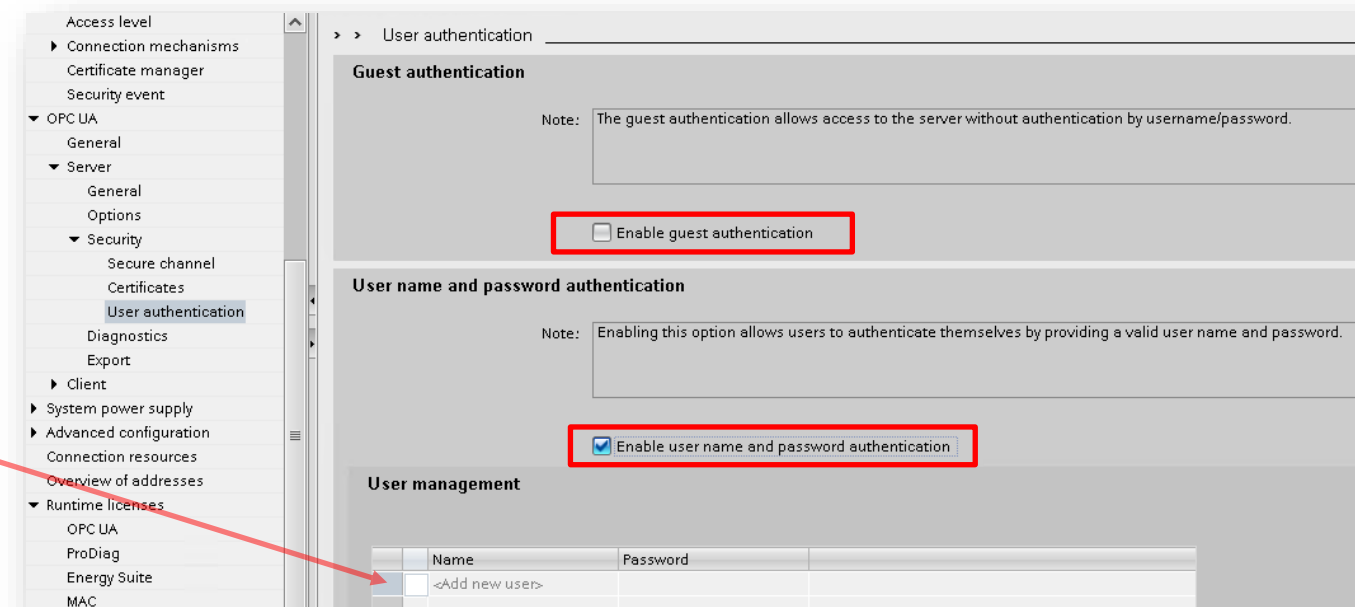


- Povolte správu OPC UA uživatelů ze security settings



- V nastavení OPC UA serveru vypněte přístup bez jména a hesla
- Povolte zabezpečení jménem a heslem
- Přehrajte HW konfiguraci PLC
- Připojte se z UA Experta
 - Nutno znovu vyhledat server!

Uživatelé definovaní v této tabulce mají přístup pouze do tohoto PLC a nelze jim definovat globální oprávnění

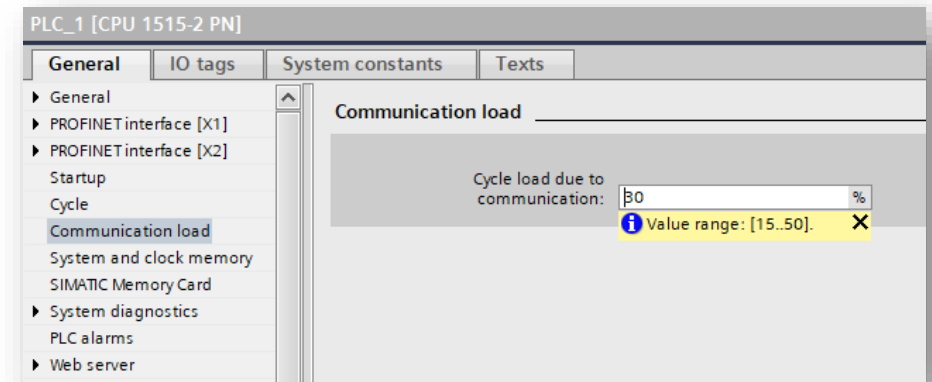


Výkon - optimalizace

Zatížení PLC komunikací

SIEMENS

- CPU je zatíženo nejen cyklickým programem, ale i komunikací
- Celková doba OB cyklu je součtem programové i komunikační fáze
- Využití celkové doby cyklu pro komunikaci lze omezit na 15 až 50%

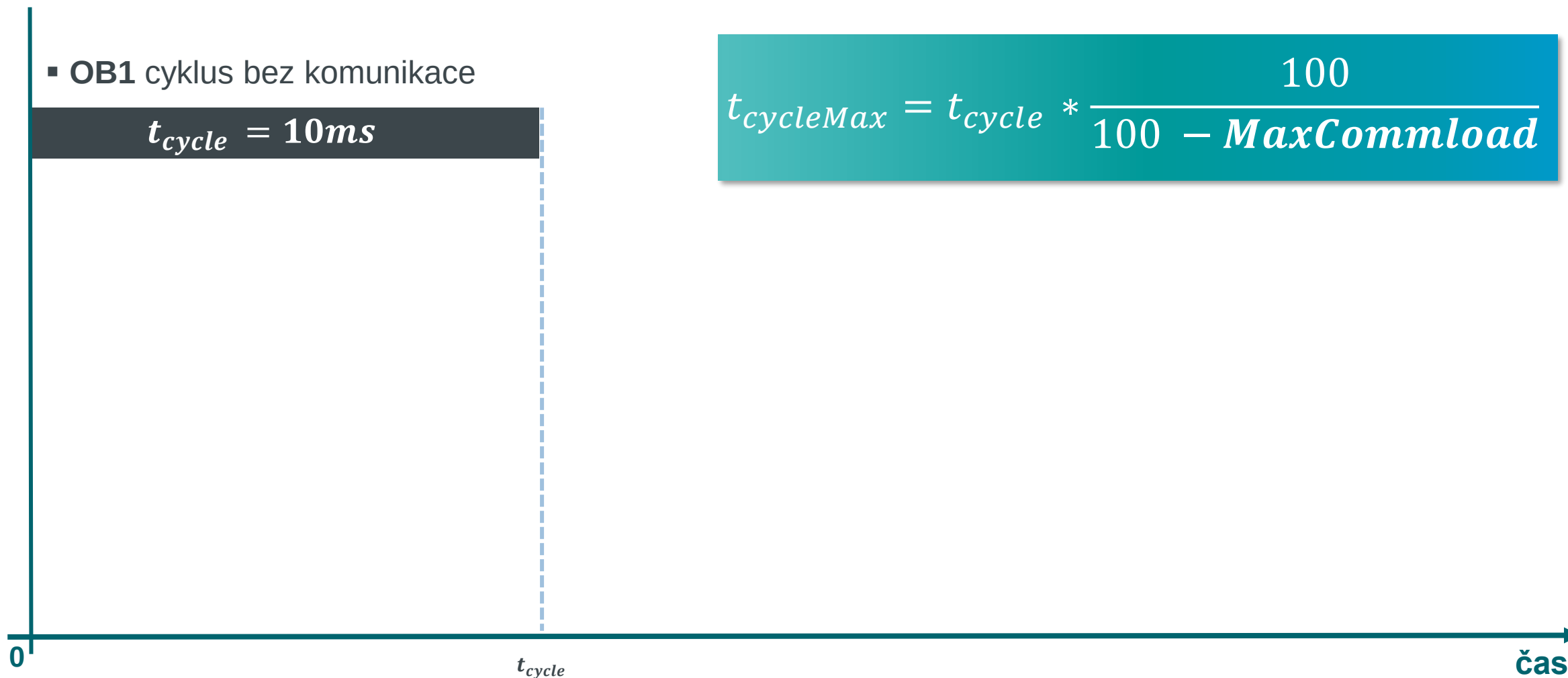


$$t_{cycleMax} = t_{cycle} * \frac{100}{100 - MaxCommload}$$

- **OB1** cyklus bez komunikace

$$t_{cycle} = 10ms$$

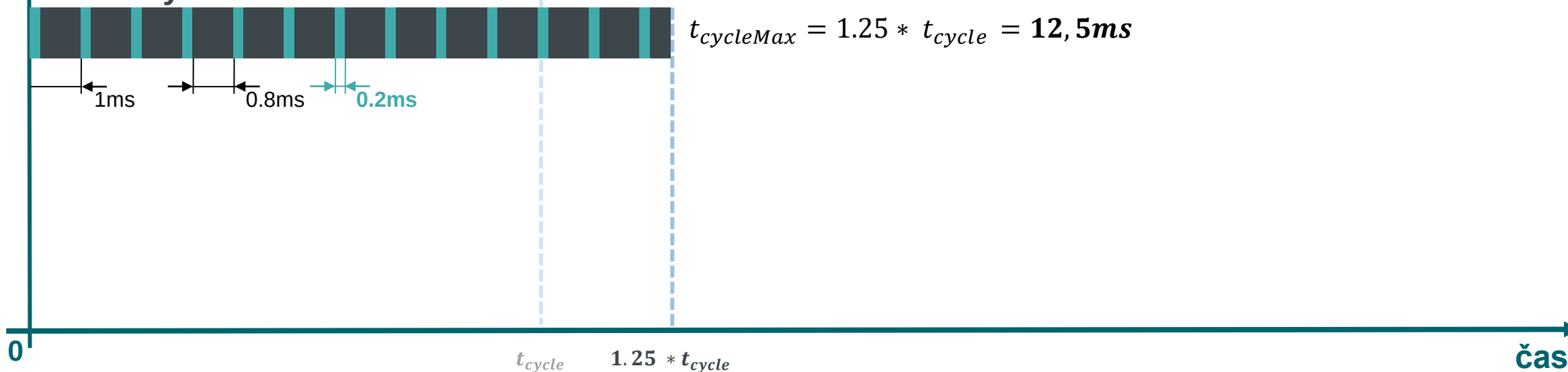
$$t_{cycleMax} = t_{cycle} * \frac{100}{100 - MaxCommload}$$



- OB1 cyklus bez komunikace

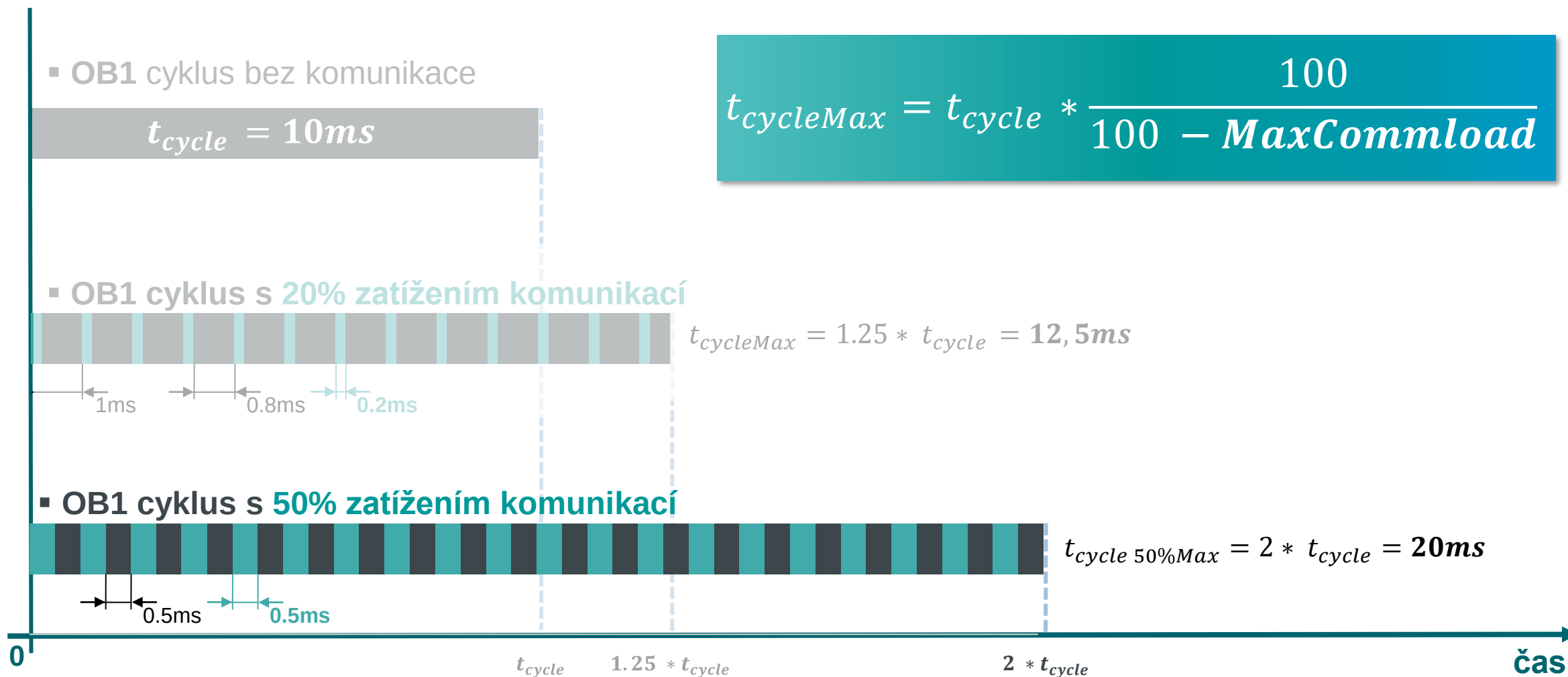
$$t_{cycle} = 10ms$$

- OB1 cyklus s 20% zatížením komunikací



$$t_{cycleMax} = t_{cycle} * \frac{100}{100 - MaxCommload}$$

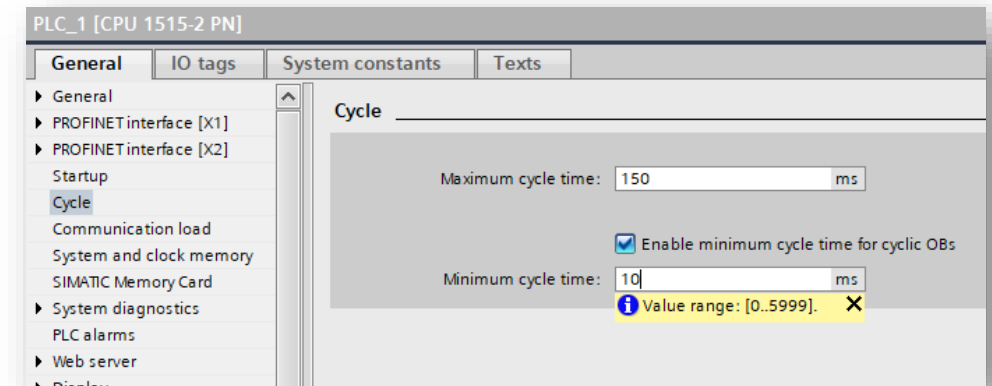
$$t_{cycleMax} = 1.25 * t_{cycle} = 12,5ms$$



Zatížení PLC komunikací

- CPU je zatíženo nejen cyklickým programem, ale i komunikací
- Celková doba cyklu je součtem programové i komunikační fáze
- Využití doby cyklu pro komunikaci lze omezit na 15 až 50%

- Prodloužením doby cyklu se prodlouží i čas pro komunikaci
- Pro časově nekritické aplikace lze nastavit minimální délku cyklu
- CPU se může věnovat pouze komunikaci



$$t_{cycleMax} = t_{cycle} * \frac{100}{100 - MaxCommload}$$

- **OB1** cyklus bez komunikace, min. cyklus 15ms

$$t_{cycle} = 10ms$$

$$t_{idle} = 5ms$$

0

čas

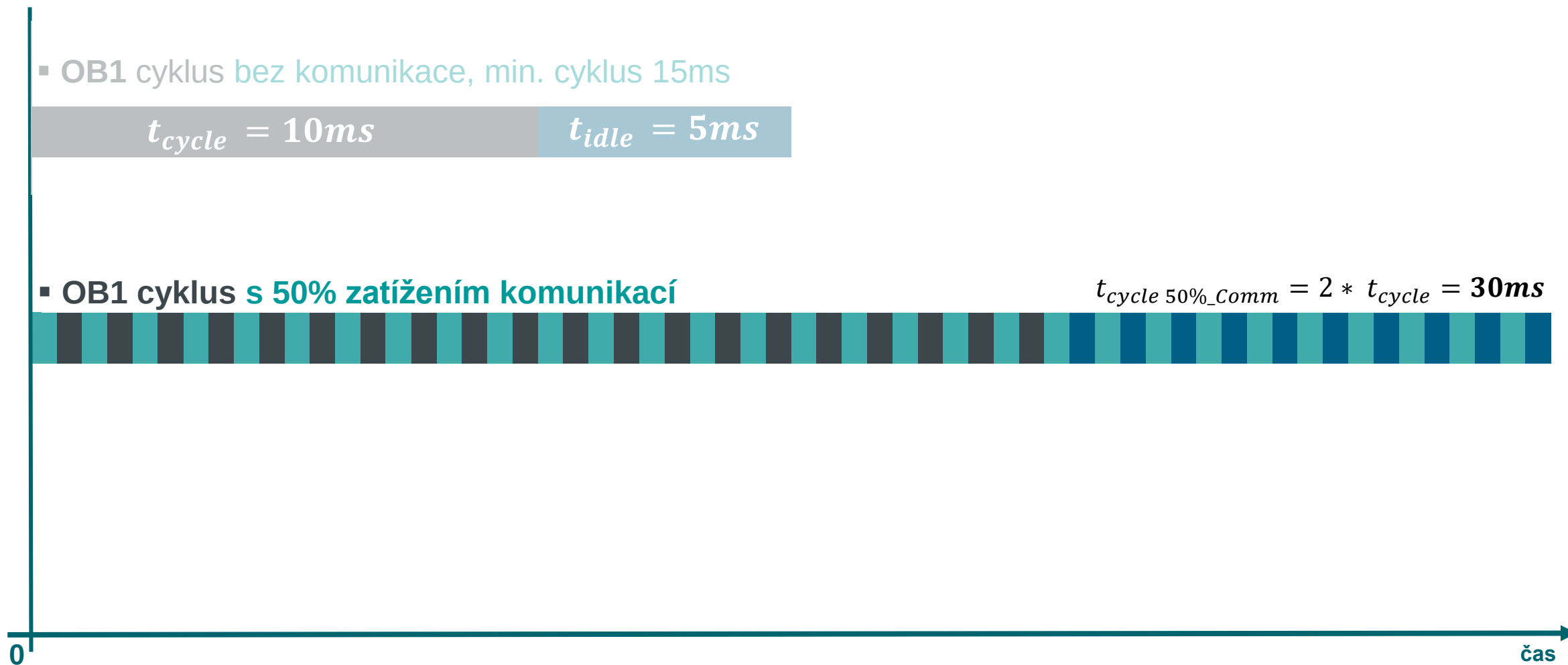
- OB1 cyklus bez komunikace, min. cyklus 15ms

$$t_{cycle} = 10ms$$

$$t_{idle} = 5ms$$

- OB1 cyklus s 50% zatížením komunikací

$$t_{cycle\ 50\%_{Comm}} = 2 * t_{cycle} = 30ms$$



- OB1 cyklus bez komunikace, min. cyklus 15ms

$$t_{cycle} = 10ms$$

$$t_{idle} = 5ms$$

- OB1 cyklus s 50% zatížením komunikací

$$t_{cycle\ 50\%_{Comm}} = 2 * t_{cycle} = 30ms$$

- OB1 cyklus s 50% zatížením komunikací s FW>2.6

Optimalizace
firmwaru

Cca 65% cyklu využito pro komunikaci

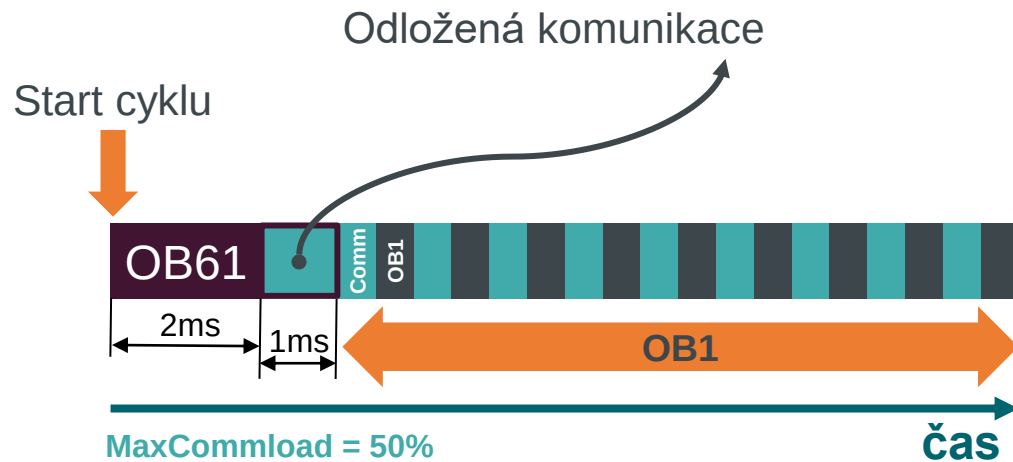
0

čas

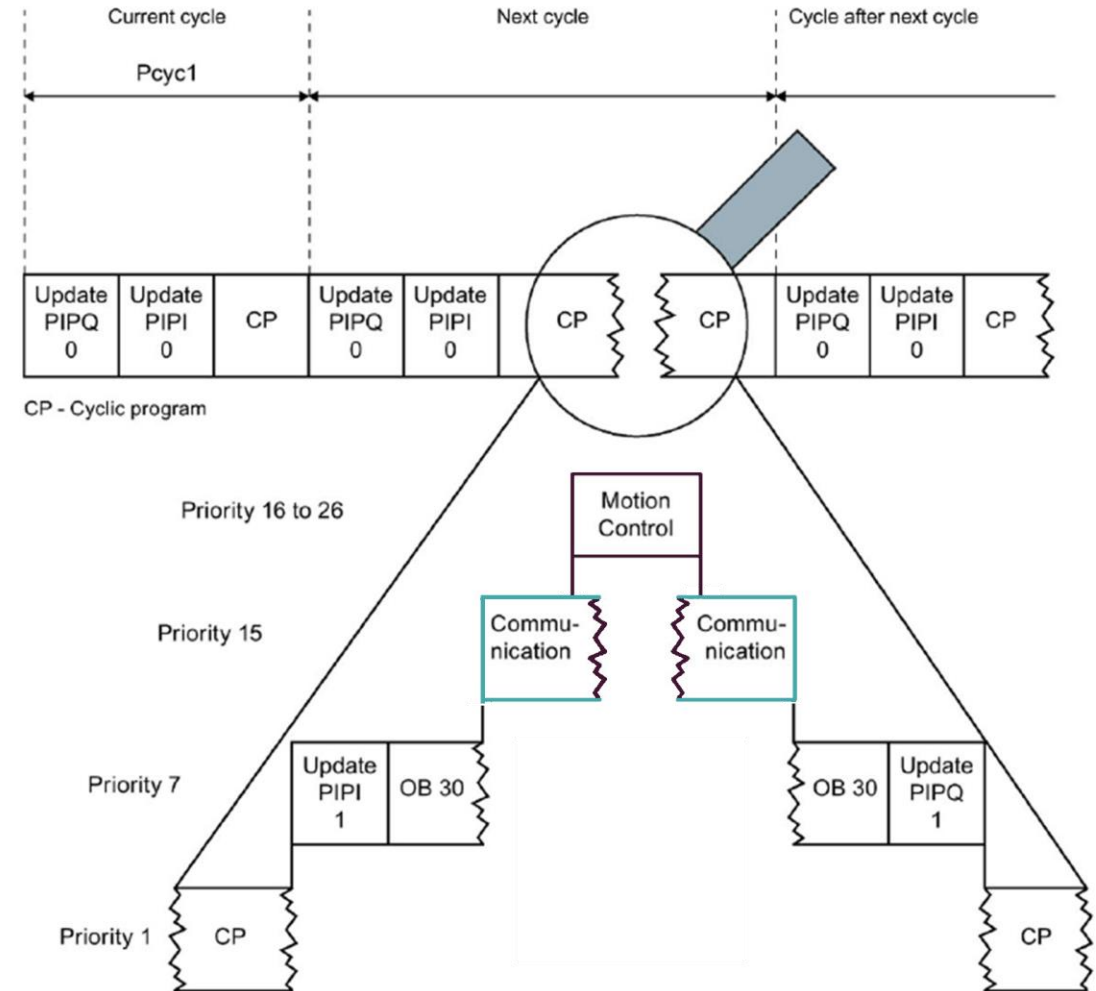
Priorita komunikace

- Priority v PLC mají úrovně od 1 do 26
- Komunikace má prioritu 15
- OB s vyšší prioritou mohou komunikaci zdržet
 - Motion control, cyclic interrupt...

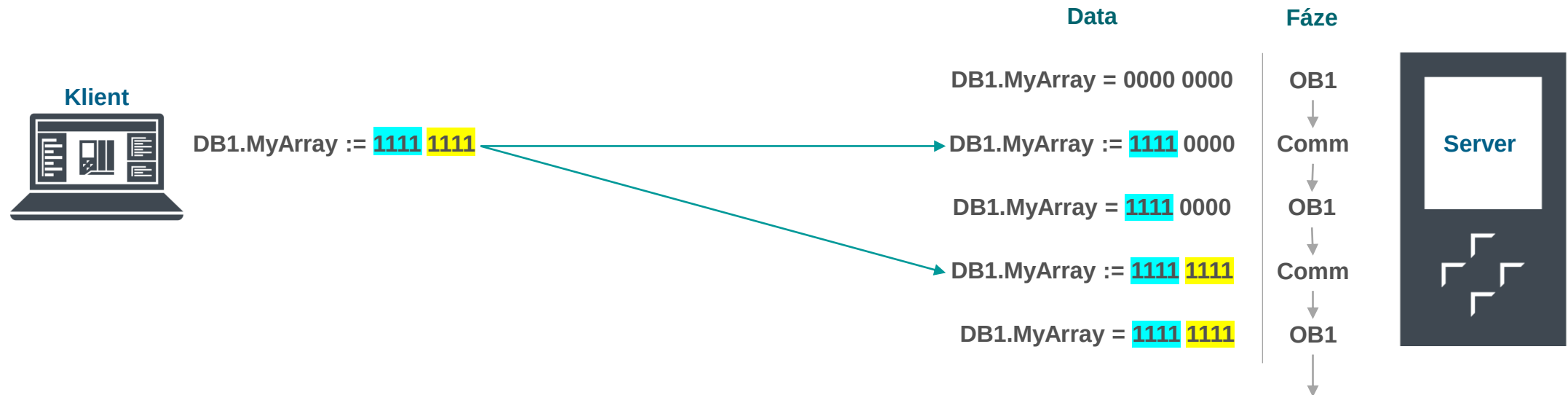
→ vzorkovací a komunikační interval OPC UA nemusí být dodržen!



SIEMENS



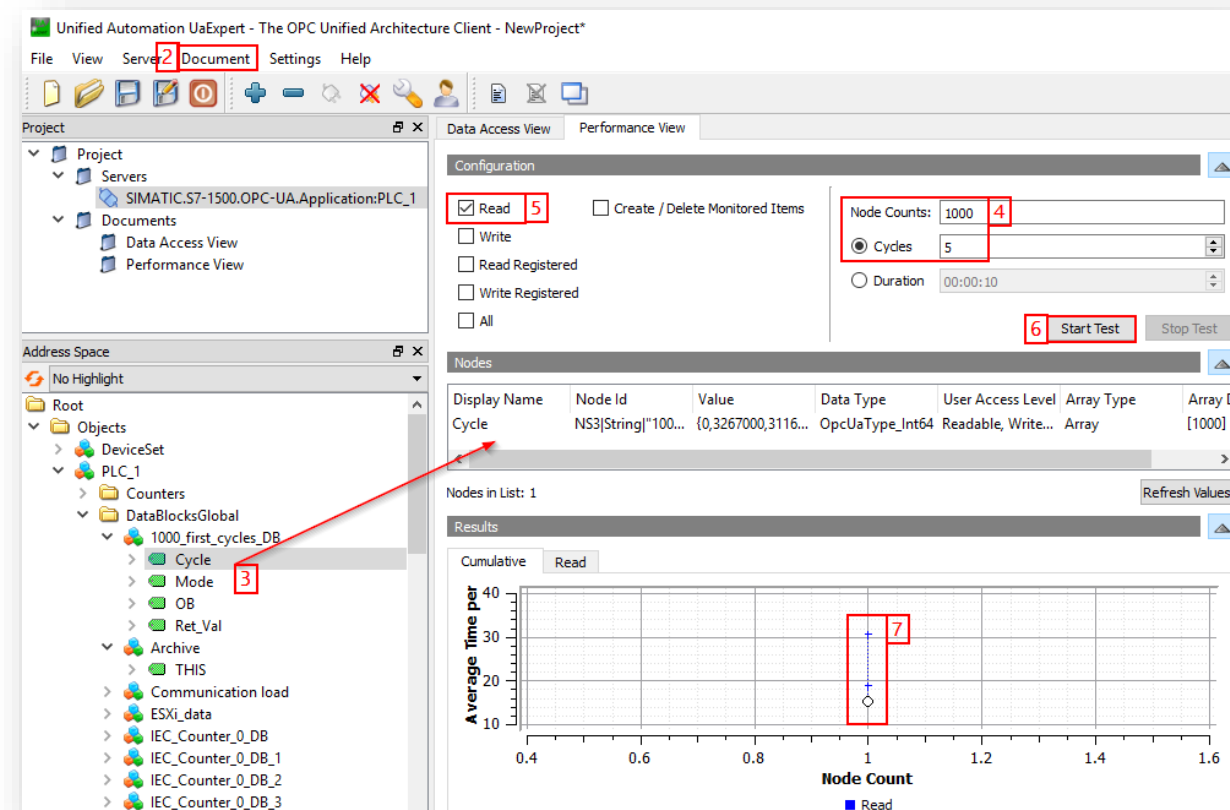
- Komunikační úlohy a cyklický program se střídají
- Cyklický program může přerušit komunikaci
- Při zápisu strukturovaných datových typů může dojít k zápisu pouze části dat mezi dvěma OB cykly (skalární datové typy jsou vždy konzistentní)
- Program poté pracuje s nekonzistentními daty





Cílem testu je zjistit vliv datového typu, šifrování a použitého rozhraní na rychlost čtení, zápisu a registrace sledovaných proměnných

- 1) Připojit se UA Expertem k OPC UA serveru
- 2) Vložit “Performance View” (Document → Add...)
- 3) Vybrat požadovaná data
- 4) Změnit node count a počet cyklů (min 5)
- 5) Vybrat požadovaný test (může být více najednou)
- 6) Spustit test
- 7) Zaznamenat hodnoty do tabulky (min – max)



- **Standard Simatic Interface**

Čas v ms (min – max)	Read	Registered Read	Write	Create Monitored Items
500x Int				
1x Array [0 .. 499] of Int				
1x Struct (500x Int)				

- **User Interface**

Čas v ms (min – max)	Read	Registered Read	Write	Create Monitored Items
500x Int				
1x Array [0 .. 499] of Int				
1x Struct (500x Int)				

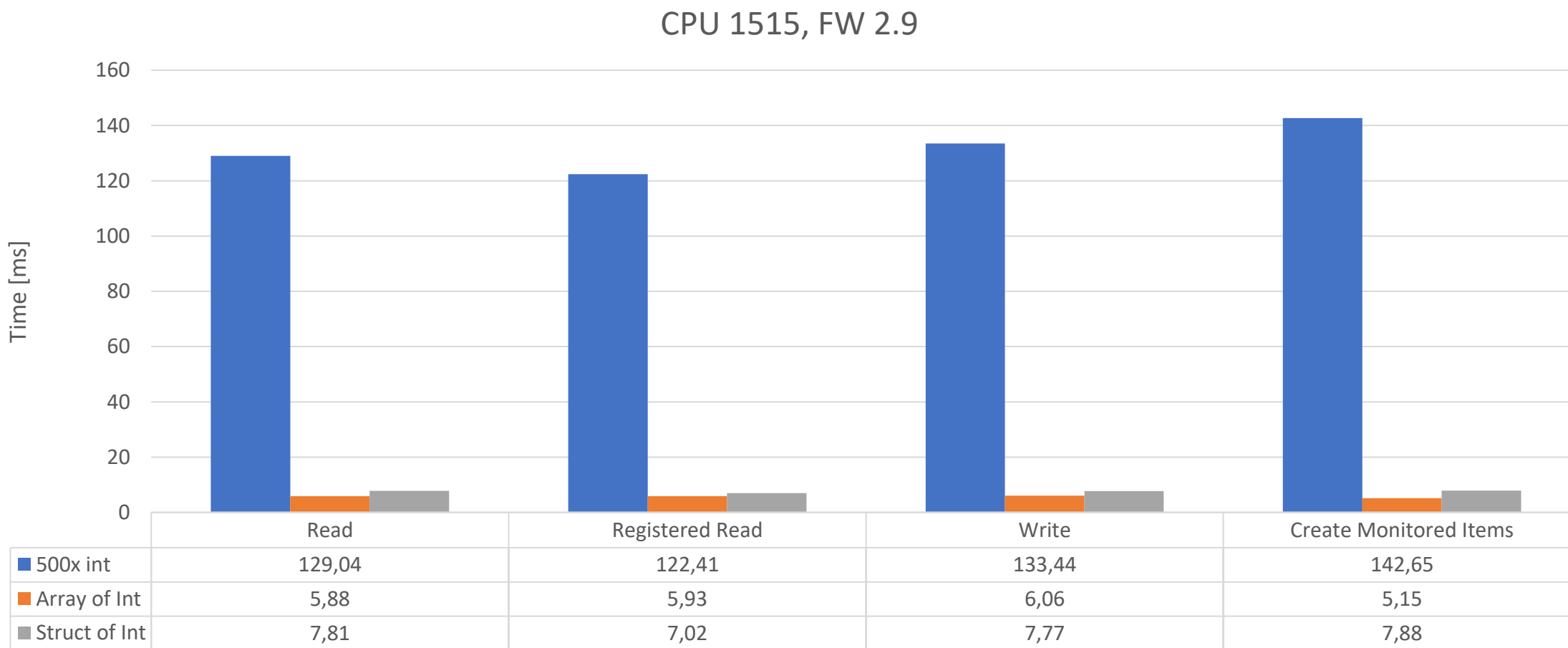
- **Security: “None”**

Čas v ms (min – max)	Read	Registered Read	Write	Create Monitored Items
500x Int				
1x Array [0 .. 499] of Int				
1x Struct (500x Int)				

- **Security: “Basic256Sha256 S&E”**

Čas v ms (min – max)	Read	Registered Read	Write	Create Monitored Items
500x Int				
1x Array [0 .. 499] of Int				
1x Struct (500x Int)				

- Basic256Sha256 S&E, user interface, 10 cyklů, bez programu, cyklus OB 1ms, 50% comm load

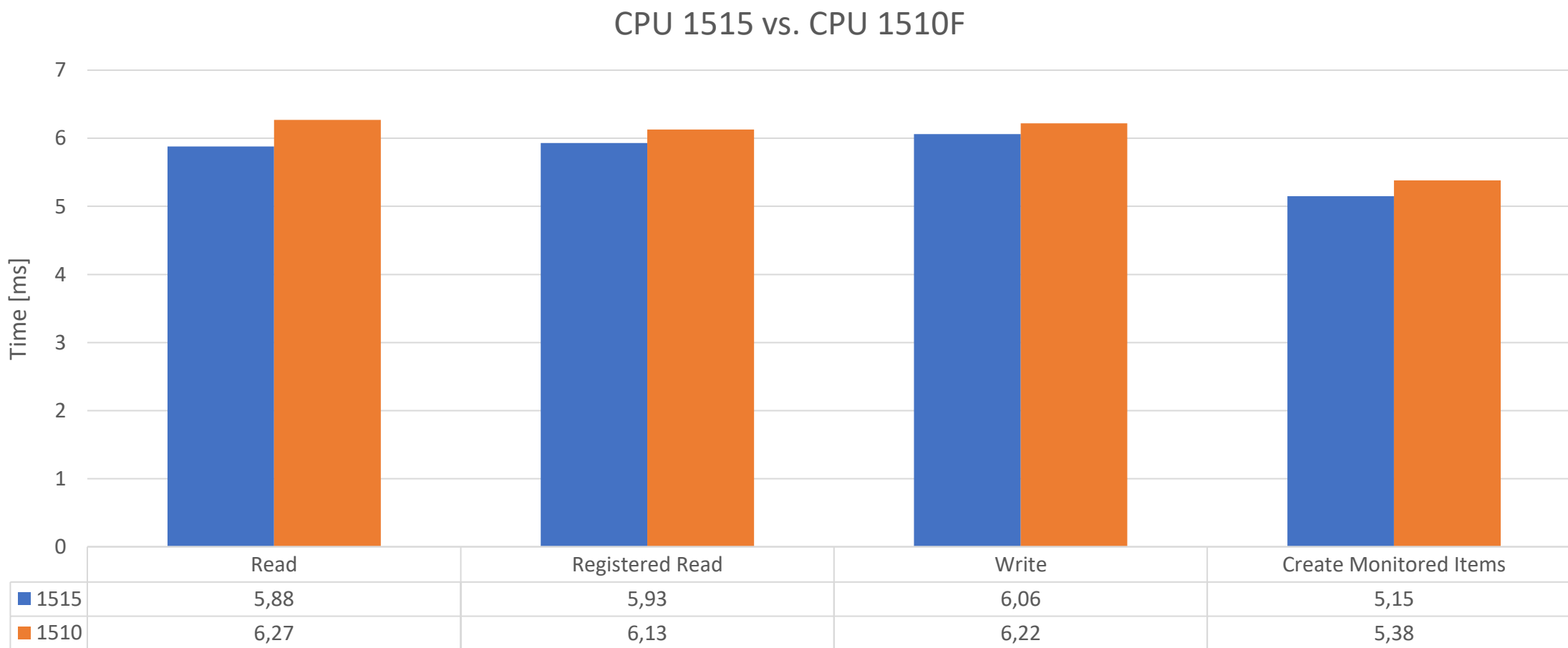


- Basic256Sha256 S&E, user interface, 10 cyklů, cyklus OB 4ms, 50% comm load
- 1 technologický objekt, testovací program, jiné komunikace (NTP, MQTT, OUC)

CPU 1515, FW 2.9



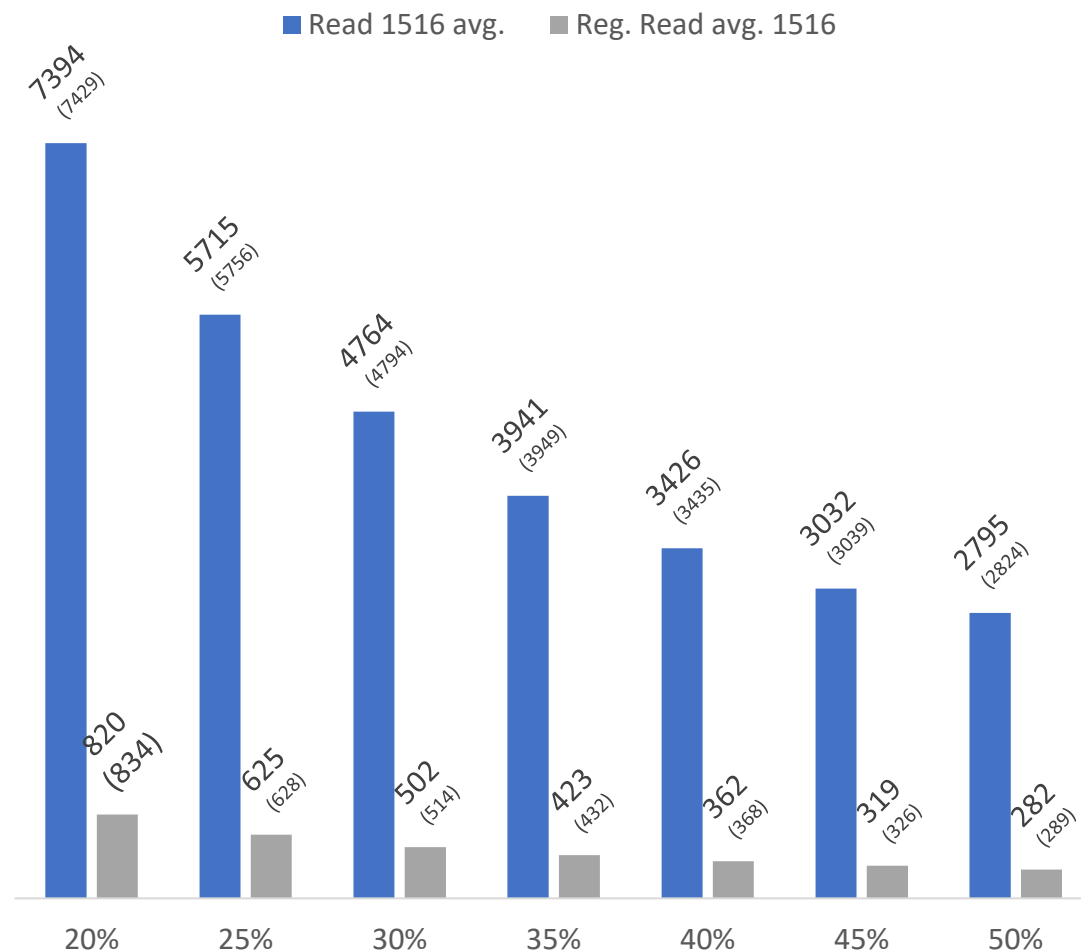
- Basic256Sha256 S&E, user interface, 10 cyklů, bez programu, cyklus OB 1ms, 50% comm load



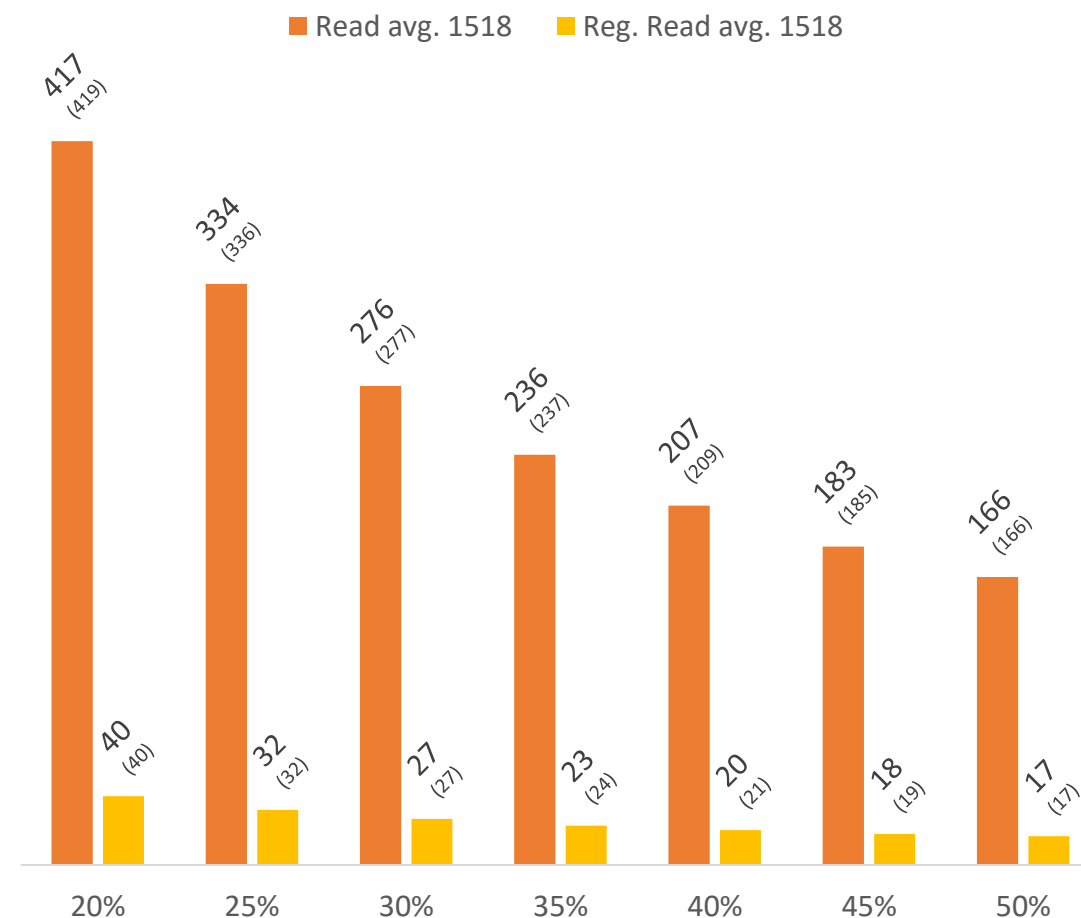
Rychlost čtení dat

SIEMENS

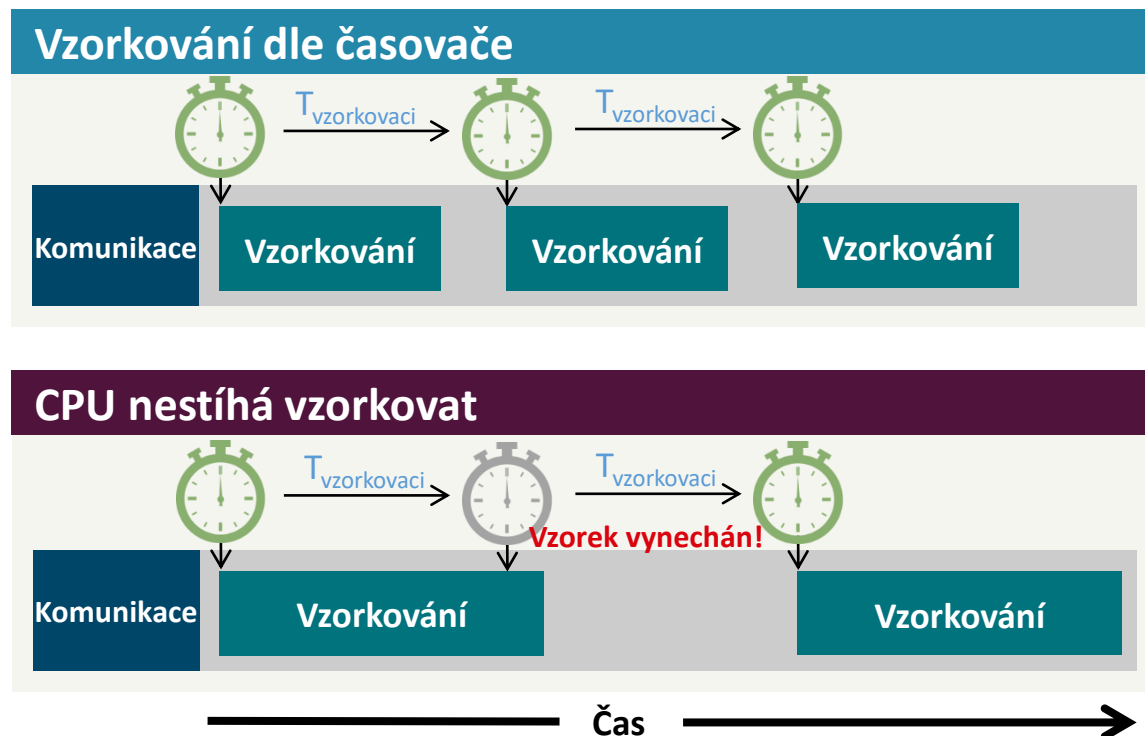
CPU 1516



CPU 1518



- Vzorkovací perioda pro subscription může být od 10ms (CPU1518) až po 5000ms
- Interní časovač hlídá vzorkování (kontrolu změn všech monitorovaných proměnných)
- Vzorkování je provedeno jen pokud časovač doběhl a předchozí vzorkování bylo dokončeno



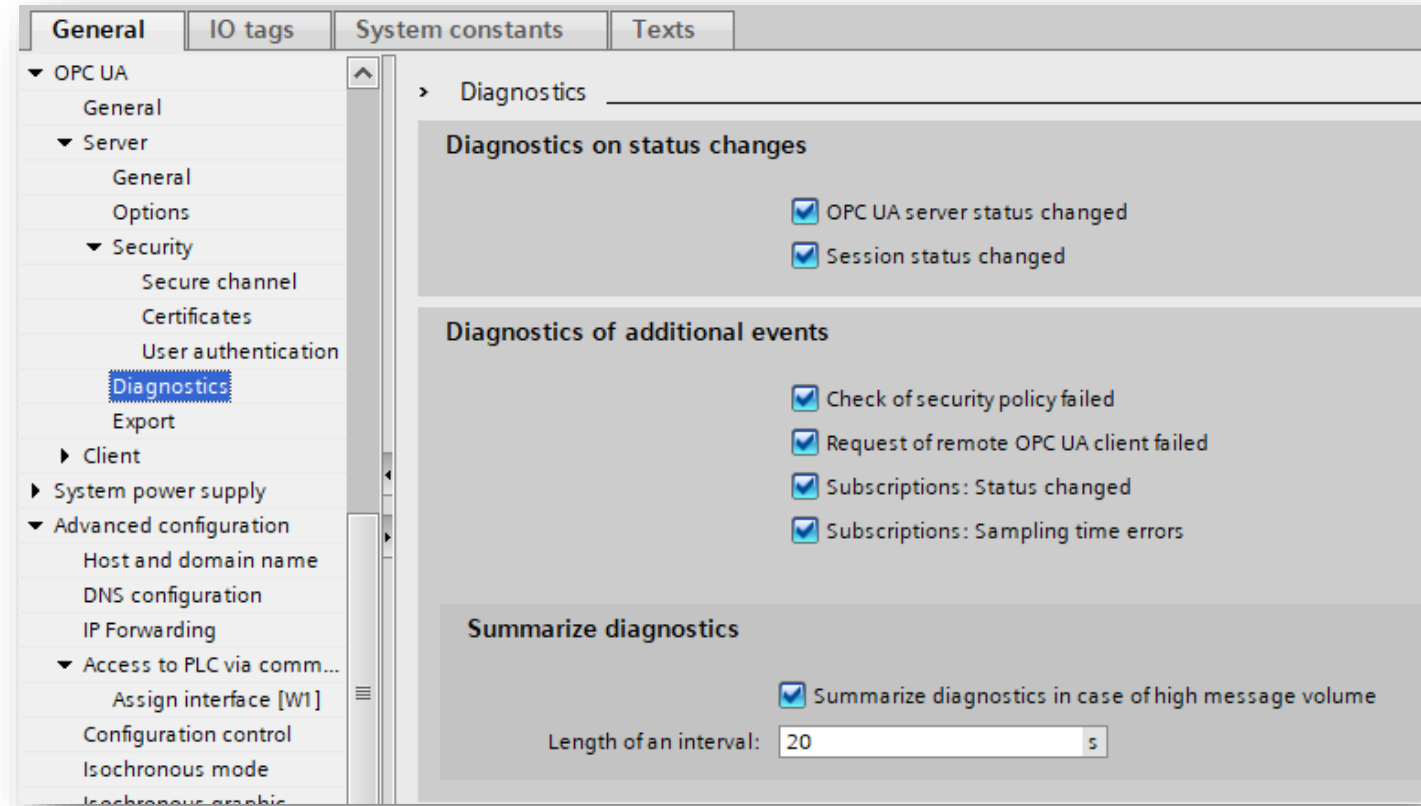
- Pokud vzorkování nebylo dokončeno včas je vygenerována chyba “Good_overload”

“Sampling has slowed down due to resource limitations”

- **Vzorek je vynechán**
 - Chyba generována pro každou monitorovanou proměnnou
 - I pokud se hodnota proměnné nezměnila
 - Odeslání této informace také generuje provoz na síti
- změnit vzorkování nebo použít výkonnější CPU

Diagnostika

- Diagnostické záznamy OPC UA server v diagnostickém bufferu PLC
- Stav serveru (Např. restart při přehrání PLC)
- Stav spojení s klientem (připojení, odpojení)
- Chyba zabezpečení
 - Špatné jméno nebo heslo
 - Chyba certifikátu
 - Kanál již není dostupný
- Chybný požadavek klienta
 - Zápis/čtení neexistující proměnné
 - Špatný parametr funkce
 - Nedostatek paměti
- Subscription
 - Změna stavu
 - Špatné vzorkování dat
- Shrnutí diagnostických zpráv za určitý interval (pro případ velkého počtu stejných zpráv)



- Diagnostický buffer obsahuje popis jednotlivých zpráv

No.	Date and time	Event
1	1/17/2022 2:37:38.875 PM	Error in parameter assignment/configuration/commissioning
2	1/17/2022 2:37:38.863 PM	Error in parameter assignment/configuration/commissioning
3	1/17/2022 2:22:45.667 PM	OPC UA Server: Wrong usage of a service. Summary message for 38 occurrences during the last 20 second(s)
4	1/17/2022 2:22:38.624 PM	OPC UA Server: Session state changed to Closed - Session ID: 4043298947.
5	1/17/2022 2:22:38.616 PM	OPC UA Server: Session state changed to Timeout - Session ID: 4043298947.
6	1/17/2022 2:22:26.249 PM	OPC UA Server: Subscription state changed to Normal - Subscription ID: 2632385123.
7	1/17/2022 2:22:26.239 PM	OPC UA Server: Subscription state changed to Creating - Subscription ID: 2632385123.
8	1/17/2022 2:22:24.449 PM	OPC UA Server: Wrong usage of service Read in session ID 2383024085.
9	1/17/2022 2:22:24.448 PM	OPC UA Server: Wrong usage of service Read in session ID 2383024085.

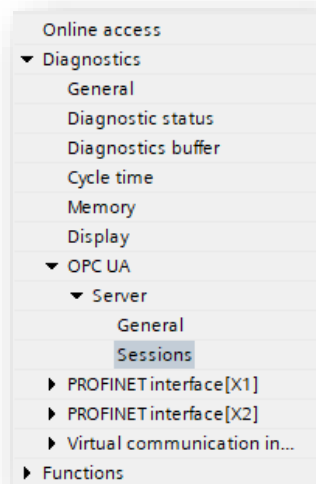
Klient odpojen – 30 sekund bez výměny dat

Klient se snaží číst proměnnou, která neexistuje

Shrnutí většího množství zpráv do jedné

- **Přehled spojení s klienty**

- ID pro každý session a subscription
- Zde je spojení se dvěma klienty (2x UA Expert)
- Statistiky o komunikaci (počet monitorovaných hodnot, počet poslaných dat, datum a čas posledního připojení...)



Session/subscription diagnostics

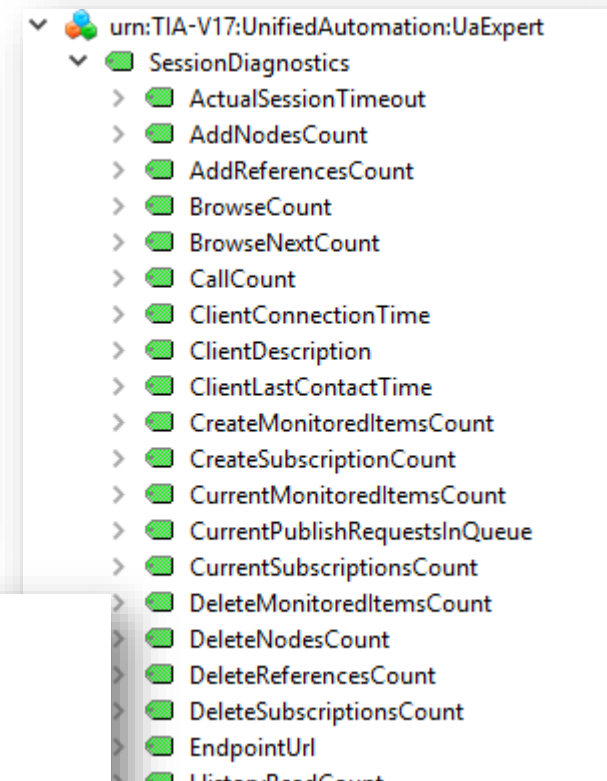
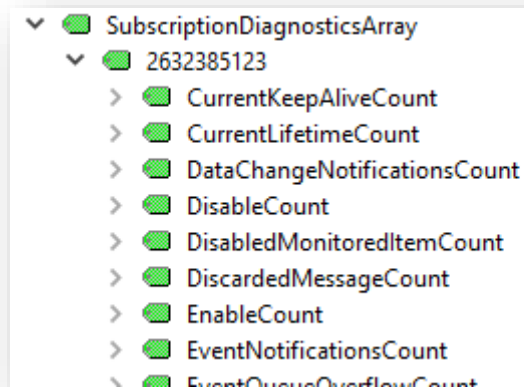
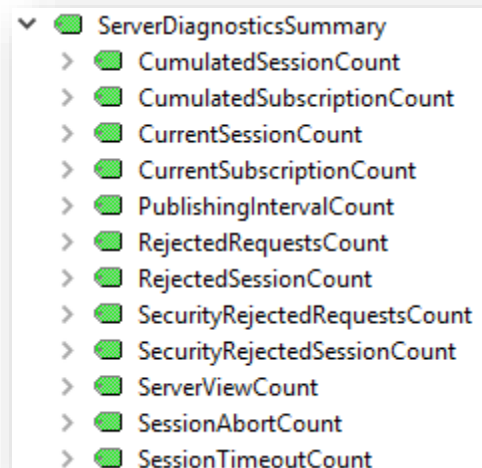
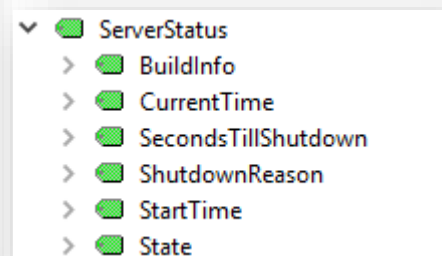
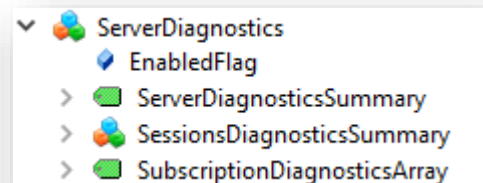
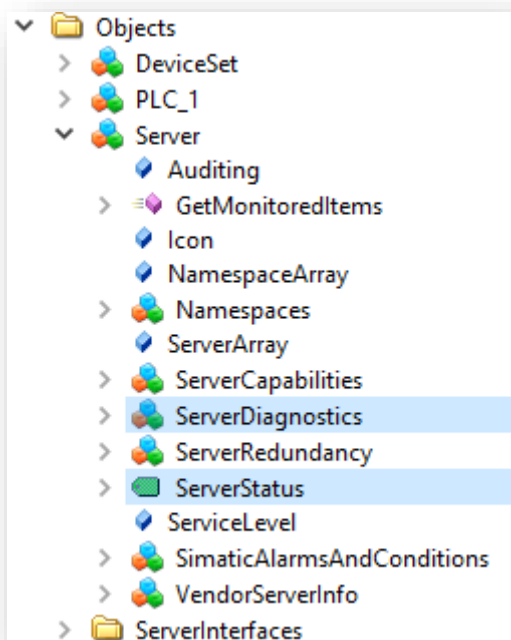
	Id	Name	Endpoint URL	Subscriptions	Monitored items	Timeout	Last contact of the client
🔴	▼ 2383024085	urn:TIA-V17:UnifiedAutomation:U...	opc.tcp://192.168.137.2:4840	3	9	788 of 30000 ms	2022-Jan-17; 14:48:06.245
🟢	■ 2632385123	Subscription_2632385123			1	30 of 1500	
🟢	■ 2632385125	Subscription_2632385125			1	5 of 600	
🟢	■ 2632385126	Subscription_2632385126			7	1 of 600	
🔴	▼ 2183893482	urn:TIA-V17:UnifiedAutomation:U...	opc.tcp://192.168.137.2:4840	2	2	745 of 30000 ms	2022-Jan-17; 14:48:06.288
🟢	■ 2632385124	Subscription_2632385124			1	7 of 1500	
🟢	■ 2632385127	Subscription_2632385127			1	5 of 600	

Freeze display

Details on selected session/subscription:

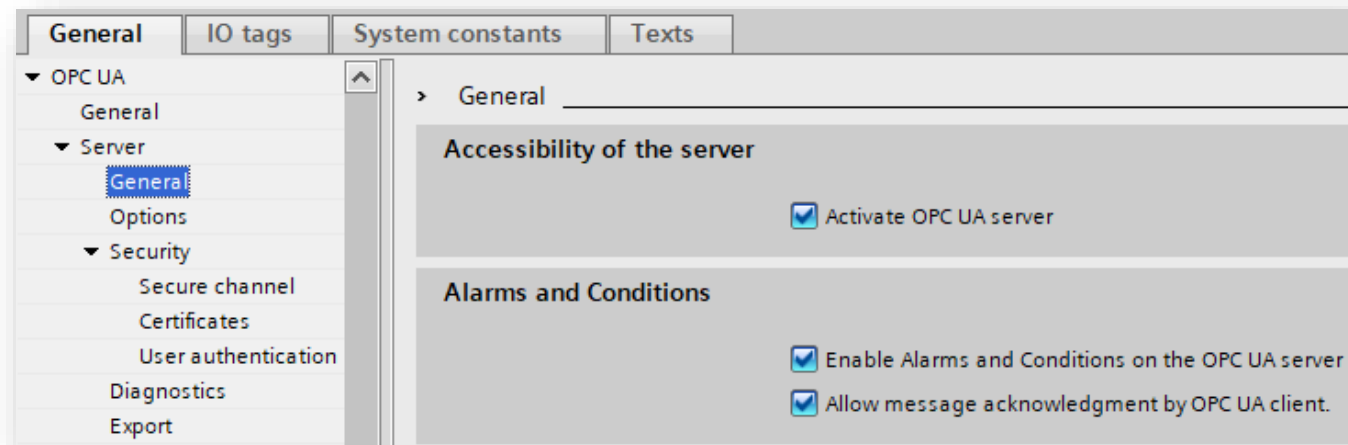
Description: TransferredToSameClientCount = 0
PublishRequestCount = 60
DataChangeNotificationsCount = 62
EventNotificationsCount = 0
NotificationsCount = 56
LatePublishRequestCount = 0
CurrentKeepAliveCount = 1
TransferredToAltClientCount = 0

- Server poskytuje proměnné, ve kterých jsou diagnostické záznamy



OPC UA – off topic

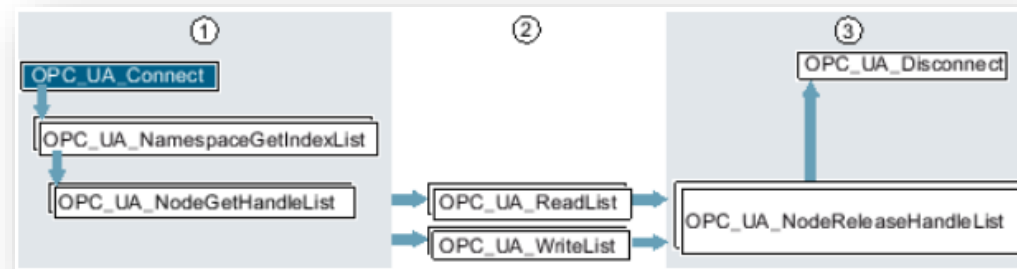
- OPC 10000-9: OPC Unified Architecture Part 9: Alarms & Conditions
- OPC UA server poskytuje hlášení z PLC
- Systémové i programové alarmy a stavy, ProDiag, GRAPH
- Možnost kvitace alarmů



- OPC UA metody poskytují přístup k programu PLC
- Zvolená část programu je ohraničena OPC UA bloky
 - OPC-UA-ServerMethodPre
 - → volaná funkce
 - OPC-UA-ServerMethodPost
 - Tyto instrukce poskytují rozhraní pro vstupní a výstupní parametry
- OPC UA metody zajišťují konzistentní přes strukturovaných proměnných
- Pouze jeden klient může volat danou instrukci

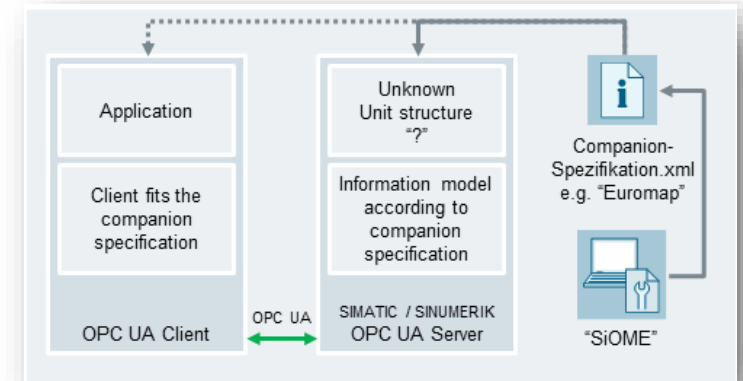
- Simatic S7-1500 podporuje i roli klienta
- Čtení, zápis dat a volání metod

- 1) Spojení, vyčtení namespace indexů, registrace čtených proměnných
- 2) Čtení a zápis dat
- 3) Odpojení registrovaných proměnných, přerušení spojení

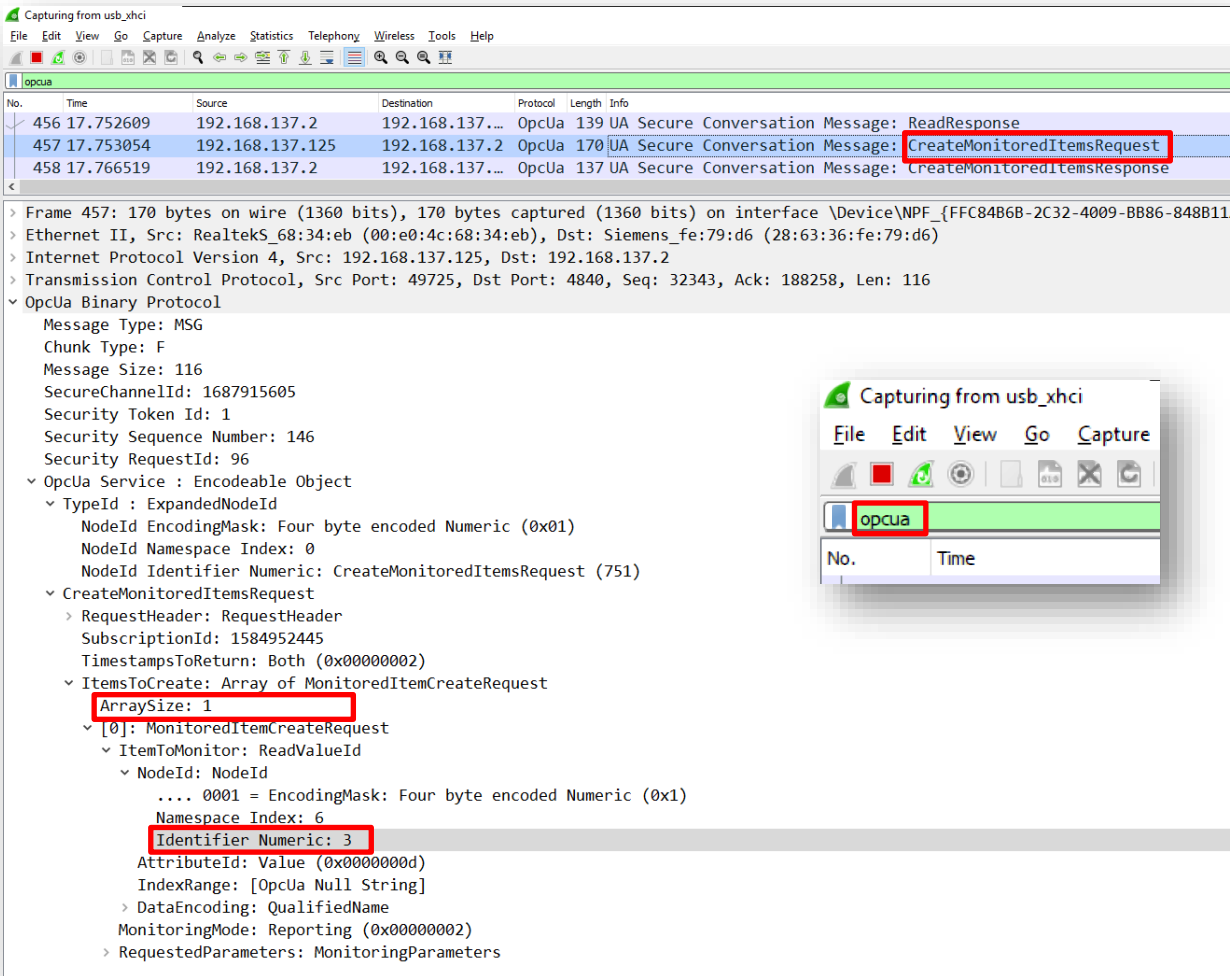


- Od FW V2.8 jsou podporovány kompaktní instrukce
 - `OPC-UA-ReadList_C`, `OPC-UA-WriteList_C`, `OPC-UA-MethodCall_C`

- **Siemens OPC UA Modelling Editor**
- **Nástroj pro pokročilé generování uživatelského rozhraní OPC UA serveru**
 - Rozhraní může být přímo namapováno k PLC z TIA Projektu
 - Do TIA lze importovat již namapované rozhraní
- **Nástroj pro mapování standardních rozhraní (PackML, OMAC) k PLC**
 - Klient nemusí znát HW/SW konfiguraci stroje, stačí mu standardní rozhraní ke komunikaci
 - Vytváření vlastního standardu!
- **OPC UA klient**
- **GDS Push**
 - **Správa certifikátů OPC UA serveru, klientů a certifikační autority**
- **Event view**
 - **Zobrazení a kvitace alarmů**
- **Dostupný zdarma**



• Diagnostický nástroj pro sledování ethernetu



Capturing from usb_xhci

No.	Time	Source	Destination	Protocol	Length	Info
456	17.752609	192.168.137.2	192.168.137.2	OpcUa	139	UA Secure Conversation Message: ReadResponse
457	17.753054	192.168.137.125	192.168.137.2	OpcUa	170	UA Secure Conversation Message: CreateMonitoredItemsRequest
458	17.766519	192.168.137.2	192.168.137.2	OpcUa	137	UA Secure Conversation Message: CreateMonitoredItemsResponse

> Frame 457: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface \Device\NPF_{FFC84B6B-2C32-4009-BB86-848B11}

> Ethernet II, Src: RealtekS_68:34:eb (00:e0:4c:68:34:eb), Dst: Siemens_fe:79:d6 (28:63:36:fe:79:d6)

> Internet Protocol Version 4, Src: 192.168.137.125, Dst: 192.168.137.2

> Transmission Control Protocol, Src Port: 49725, Dst Port: 4840, Seq: 32343, Ack: 188258, Len: 116

▼ OpcUa Binary Protocol

Message Type: MSG

Chunk Type: F

Message Size: 116

SecureChannelId: 1687915605

Security Token Id: 1

Security Sequence Number: 146

Security RequestId: 96

▼ OpcUa Service : Encodeable Object

▼ TypeId : ExpandedNodeId

NodeId EncodingMask: Four byte encoded Numeric (0x01)

NodeId Namespace Index: 0

NodeId Identifier Numeric: CreateMonitoredItemsRequest (751)

▼ CreateMonitoredItemsRequest

> RequestHeader: RequestHeader

SubscriptionId: 1584952445

TimestampsToReturn: Both (0x00000002)

▼ ItemsToCreate: Array of MonitoredItemCreateRequest

ArraySize: 1

▼ [0]: MonitoredItemCreateRequest

▼ ItemToMonitor: ReadValueId

▼ NodeId: NodeId

... 0001 = EncodingMask: Four byte encoded Numeric (0x1)

Namespace Index: 6

Identifier Numeric: 3

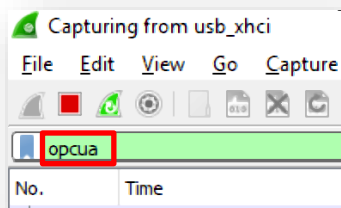
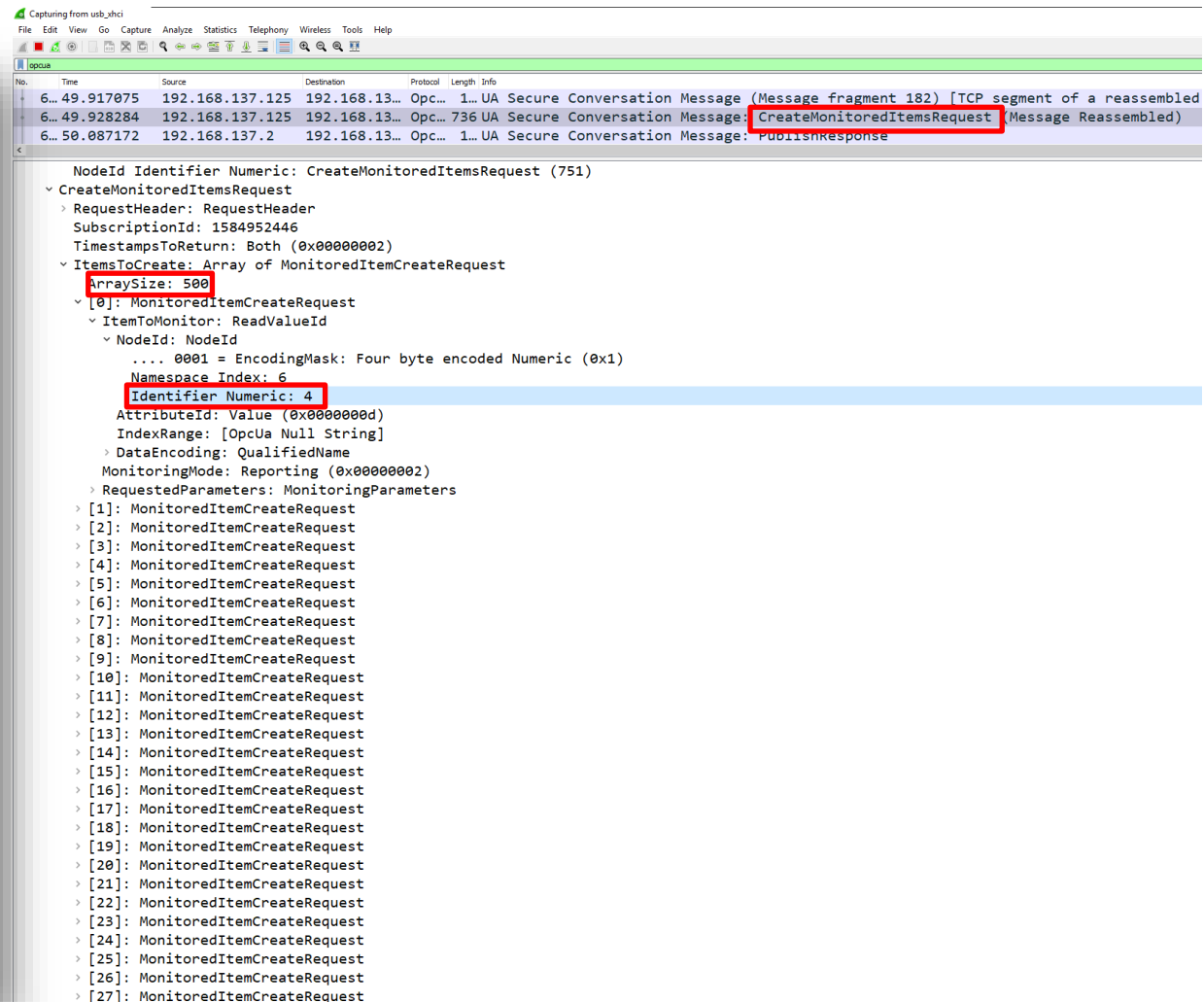
AttributeId: Value (0x0000000d)

IndexRange: [OpcUa Null String]

> DataEncoding: QualifiedName

MonitoringMode: Reporting (0x00000002)

> RequestedParameters: MonitoringParameters

Capturing from usb_xhci

No.	Time	Source	Destination	Protocol	Length	Info
6...	49.917075	192.168.137.125	192.168.137.2	OpcUa	1...	UA Secure Conversation Message (Message fragment 182) [TCP segment of a reassembled
6...	49.928284	192.168.137.125	192.168.137.2	OpcUa	736	UA Secure Conversation Message: CreateMonitoredItemsRequest (Message Reassembled)
6...	50.087172	192.168.137.2	192.168.137.2	OpcUa	1...	UA Secure Conversation Message: PublishResponse

▼ CreateMonitoredItemsRequest (751)

> CreateMonitoredItemsRequest

> RequestHeader: RequestHeader

SubscriptionId: 1584952445

TimestampsToReturn: Both (0x00000002)

> ItemsToCreate: Array of MonitoredItemCreateRequest

ArraySize: 500

▼ [0]: MonitoredItemCreateRequest

▼ ItemToMonitor: ReadValueId

▼ NodeId: NodeId

... 0001 = EncodingMask: Four byte encoded Numeric (0x1)

Namespace Index: 6

Identifier Numeric: 4

AttributeId: Value (0x0000000d)

IndexRange: [OpcUa Null String]

> DataEncoding: QualifiedName

MonitoringMode: Reporting (0x00000002)

> RequestedParameters: MonitoringParameters

> [1]: MonitoredItemCreateRequest

> [2]: MonitoredItemCreateRequest

> [3]: MonitoredItemCreateRequest

> [4]: MonitoredItemCreateRequest

> [5]: MonitoredItemCreateRequest

> [6]: MonitoredItemCreateRequest

> [7]: MonitoredItemCreateRequest

> [8]: MonitoredItemCreateRequest

> [9]: MonitoredItemCreateRequest

> [10]: MonitoredItemCreateRequest

> [11]: MonitoredItemCreateRequest

> [12]: MonitoredItemCreateRequest

> [13]: MonitoredItemCreateRequest

> [14]: MonitoredItemCreateRequest

> [15]: MonitoredItemCreateRequest

> [16]: MonitoredItemCreateRequest

> [17]: MonitoredItemCreateRequest

> [18]: MonitoredItemCreateRequest

> [19]: MonitoredItemCreateRequest

> [20]: MonitoredItemCreateRequest

> [21]: MonitoredItemCreateRequest

> [22]: MonitoredItemCreateRequest

> [23]: MonitoredItemCreateRequest

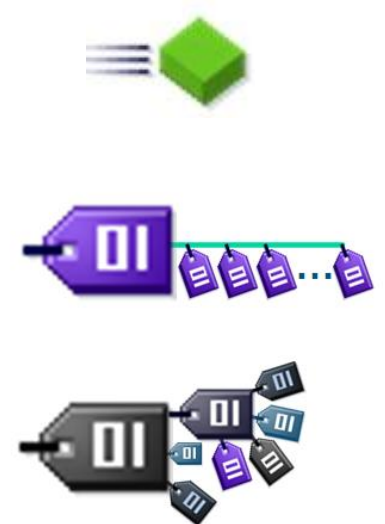
> [24]: MonitoredItemCreateRequest

> [25]: MonitoredItemCreateRequest

> [26]: MonitoredItemCreateRequest

> [27]: MonitoredItemCreateRequest

- **OPC UA server podporován od FW 4.4 (TIA V16)**
 - Pouze server, nikoliv klient
 - Nepodporuje standard simatic interface, pouze uživatelsky definovaný
 - Nepodporuje strukturované datové typy (pole, struktury, UDT)
 - Nepodporuje registered read/write
 - Nepodporuje metody
 - Bez diagnostiky v TIA Portalu
 - Restartuje server při každém nahrání do PLC
- **FW 4.5 (TIA V17)**
 - Podpora metod
 - Podpora strukturovaných datových typů
 - Diagnostika v TIA Portalu
 - Navýšení limitů
- **Pozor na výkon CPU!**



OPC UA rekapitulace

Doporučení pro optimální konfiguraci

- **Zapnout pouze zabezpečenou komunikaci** (Rsa256Sha256)
- **Vypnout automatické akceptování certifikátů druhé strany**
 - Doporučená je i autentizace jménem a heslem
- **Vlastní server interface či companion specification**
 - Efektivní využití paměti PLC, rychlejší komunikace
 - Standardizace → SiOME
- **Pole a struktury**
 - Efektivní využití paměti PLC, až 100x rychlejší komunikace
- **Registered read či subscription**
 - Až 10x rychlejší než běžné čtení (read)
- **Globální správa certifikátů a uživatelů**
- **Omezení ostatní komunikace**
 - OPC UA sdílí prostředky CPU s ostatní NRT komunikací (TCP, UDP, HMI, S7....)

[YouTube: Mister Automation: SIMATIC OPC UA](#)

[Online support: Siemens OPC Modeling Editor \(SiOME\)](#)

[Online support: OPC UA method](#)

[Online Support: .NET OPC UA client](#)

[Online support: S7-1500 OPC UA client](#)

[Online support: Internal and external OPC UA connection with virtual Ethernet adapter of software controllers](#)

[Online support: Performance measurements of typical OPC UA configuration](#)

[Online support: How do you best configure an OPC UA client to communicate efficiently](#)

Děkuji za pozornost!

SIEMENS



Marek Semanský (RC-CZ DI FA SUP)

Technický poradce

marek.semansky@siemens.com

Siemens s.r.o.

Siemensova 1, Praha 13

+420 800 909 090

siemens.cz@siemens.com

Technická podpora

Česko: www.siemens.cz/podpora

Globálně: SIOS

siemens.cz