black hat USA 2021 | OTORIO | August 4-5, 2021 BRIEFINGS

A Broken Chain:

Discovering OPC-UA Attack Surface and Exploiting the Supply-chain

By Eran Jacob

Who am I?

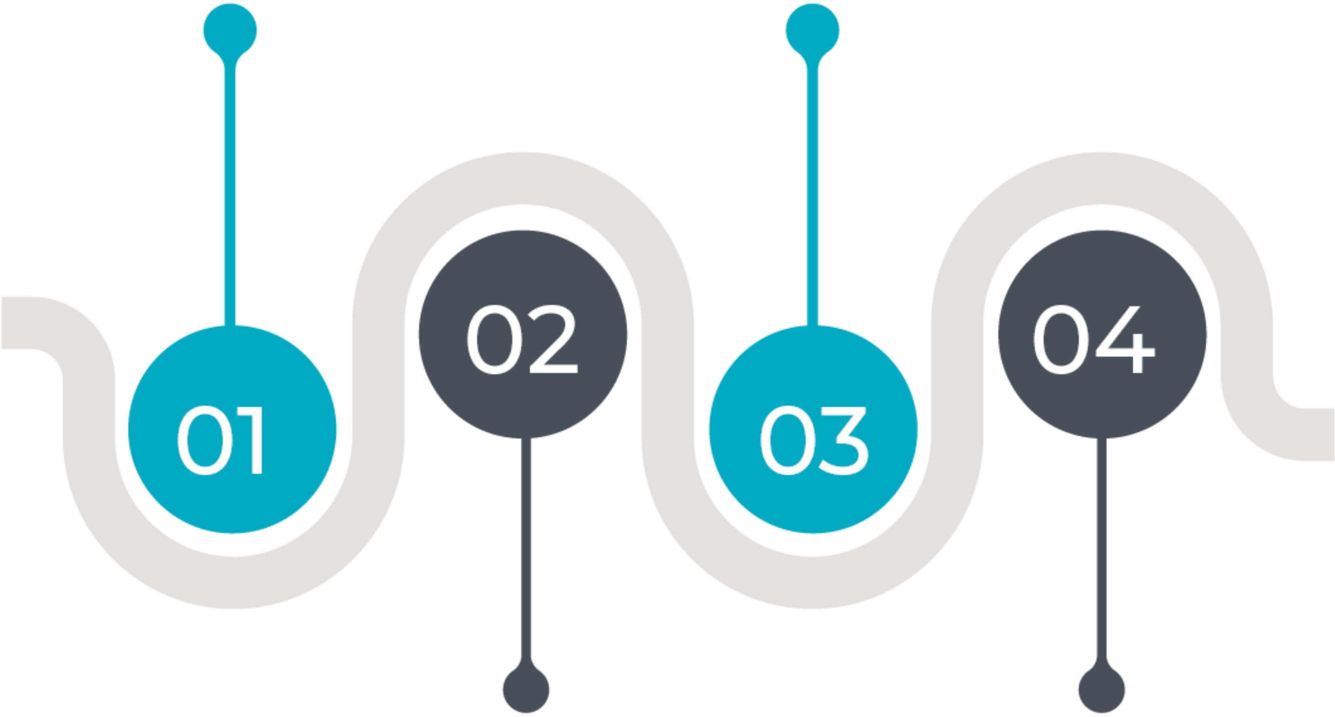
Eran Jacob
Security Research Team Leader

@EranJacob
linkedin.com/in/eranj

Roman Dvorkin
linkedin.com/in/roman-dvorkin

Alon Zini
linkedin.com/in/alon-zini-3b9698185

Agenda



01 Intro

02 The Attack Surface

03 Supply-chain Exploitation

04 Fuzzing

Automation Protocols

Manufacturing

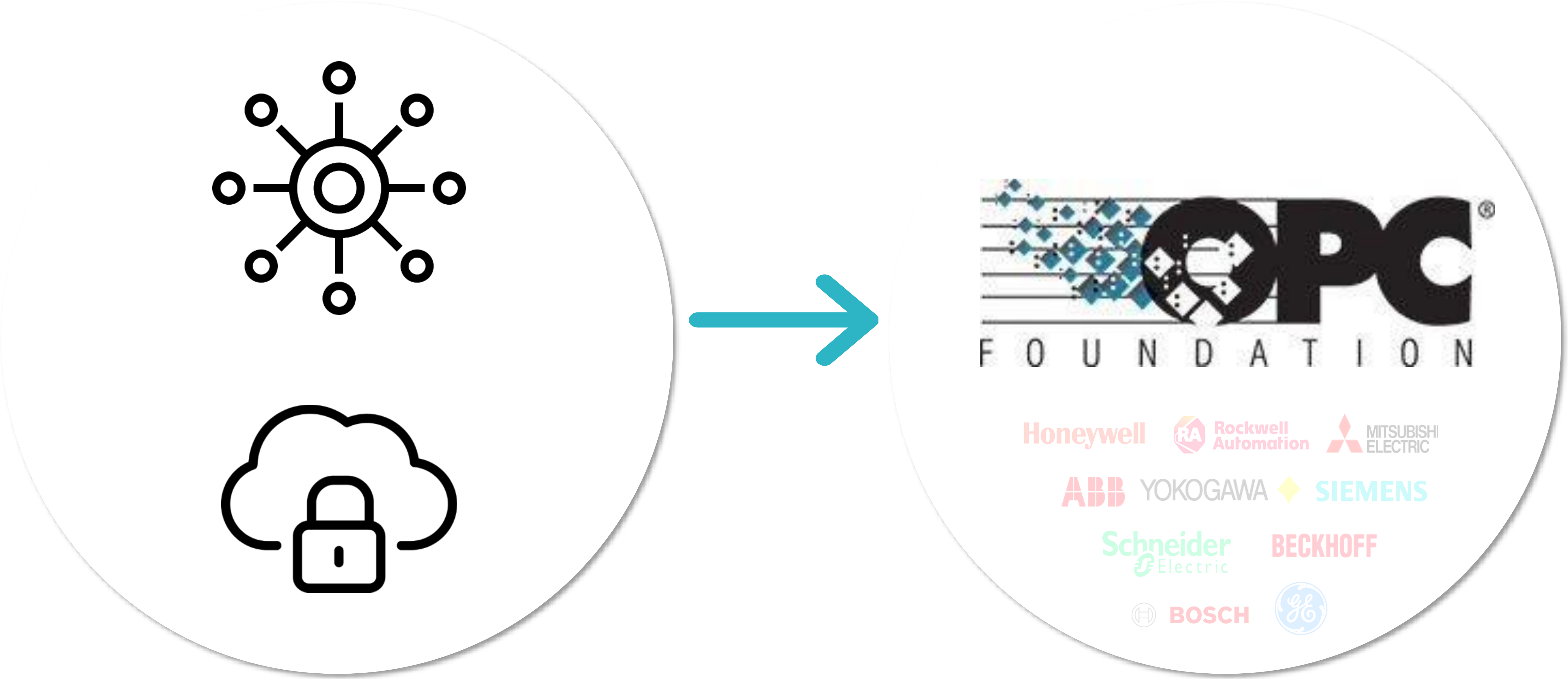
Critical Infrastructure

Buildings, Traffic..

Rockwell Automation ABB MITSUBISHI ELECTRIC BOSCH

Schneider Electric BECKHOFF YOKOGAWA SIEMENS GE Honeywell

Automation Protocols



OPC Classic

Open Platform Communications

OPC®

- Data Access
- Alarms and Events
- Historical Data Access

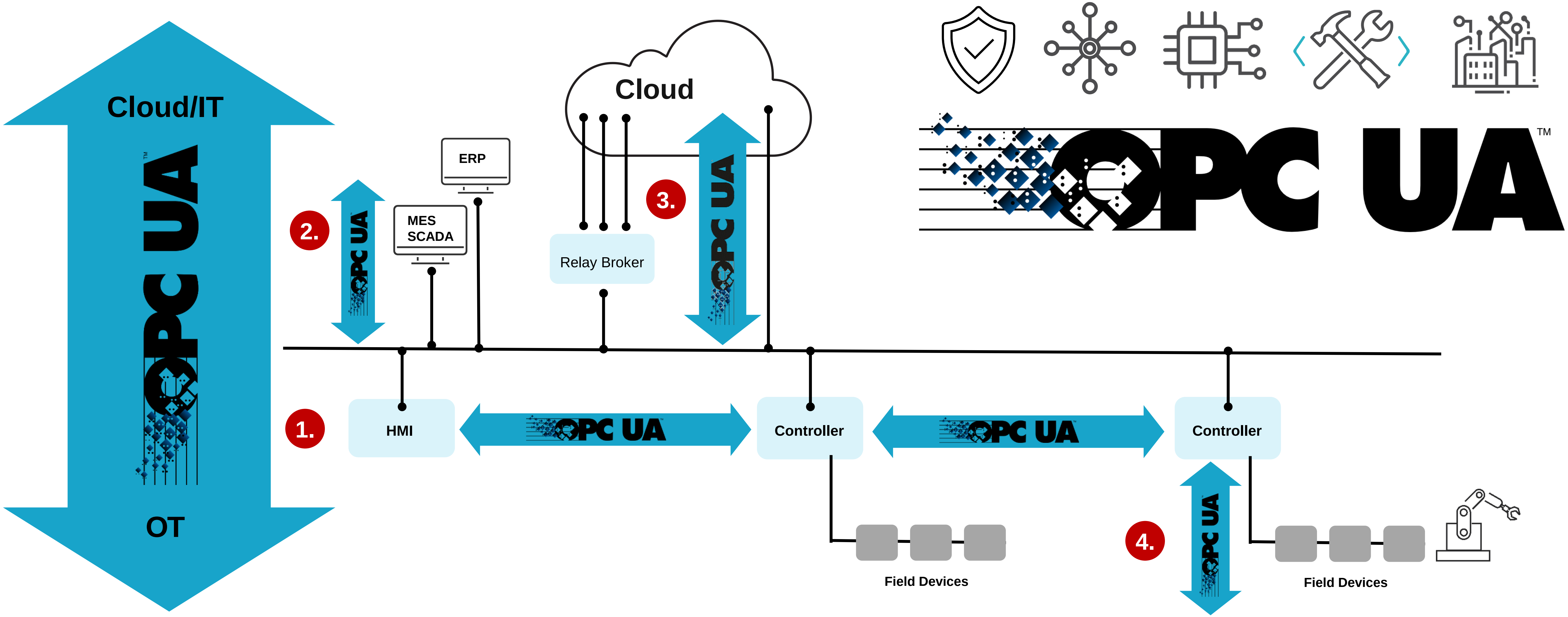
Microsoft

Distributed Component
Object Model

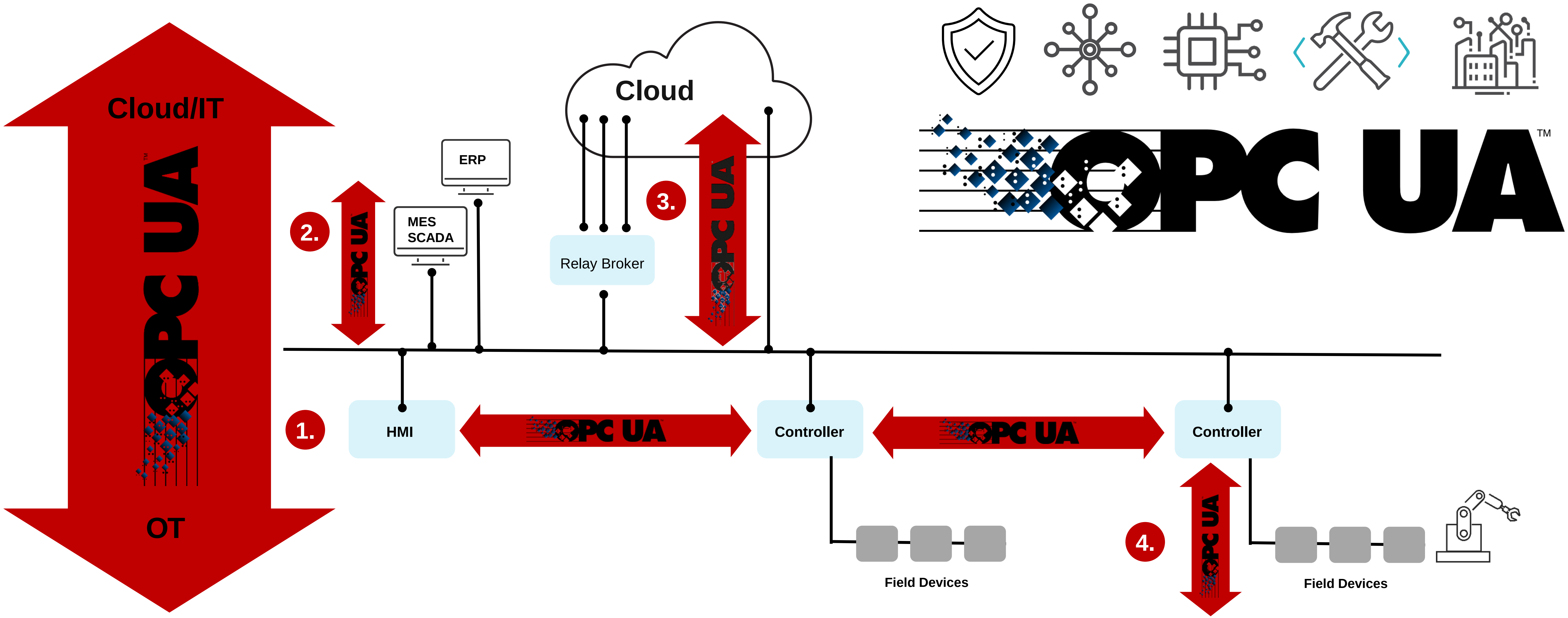
Firewall unfriendly

Security

OPC Unified Architecture



OPC Unified Architecture



Motivation for Research

- The “next-thing” in industrial communication
- Highly adopted
- **Significant potential impact**

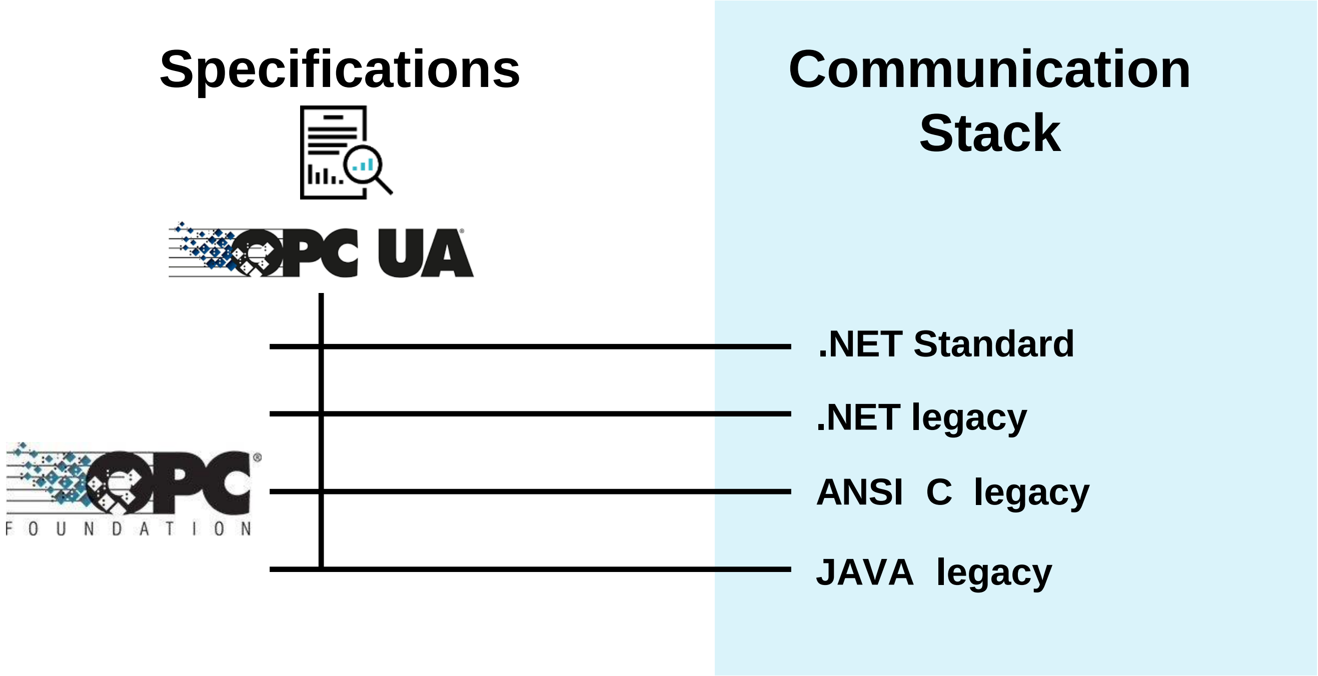
Smart Software Solutions
4CE Industry
A+B Solutions
ABB
Abbott
ACTSYS
advancis
ADVOSOL
Agilent
GILEO
Alarm IT Factory
Aletler
Allmendinger
ANALOG DEVICES
Another Ware
ANTARESVISION
ATS
RRA ENGINEERING
ARBURG
PcVue Solutions
ascolab
aspentech
assystem
Atlas Copco
ATMOS INTERNATIONAL
AUTOMIQ
Automsoft
AXITECH
azbil
B-Scada
B&R
bachmann.
BAKER HUGHES
BALLUFF
BAUER
Baumer Passion for Sensors
BECKHOFF
BELDEN
Bentley
BERGAUER
Bihl+Wiedemann
rexroth A Bosch Company
BR&L Consulting
BrightEye
C-Labs
Capgemini
cenit
atvise
Chemstations
CISCO
Codra
CCC
COMTROL
CONNEX SOFT
controlsee
COPADATA
Cyberlogic
Danfoss
DASSAULT SYSTEMES
Delphin Technology
SILENT DIG
DSI
Dynamics
EATON
eDF
EMPRISE
Endress+Hauser
Entrust Datacard
etm
EXOR EMBEDDED
Roche
FANUC
FESTO
FOX IT
Fraunhofer IOSB
Fuji Electric
FZI
GALLAGHER
GE
glaston
GOGLIO
GORDIC
TOPSTAR 拓斯达
R 速威 Real-Time Data
Pushing Performance
HERMOS
Hewlett Packard Enterprise
hischer
HIMA SAFETY NONSTOP
HITACHI Inspire the Next
HMS Connecting Devices
Honeywell THE POWER OF CONNECTED
HUAWEI
HUME INTEGRATION SOFTWARE
iba
IBHsoftec
IBM
iconics
imt.
INDEL
QuickHMI
inductive automation
Infoteam
Technische Hochschule Ingolstadt
Net ini
inmation integration unlimited
Innaq
INOSOFT
integration objects
intel
INTERSTATES CONTROL SYSTEMS, INC.
IoTium
BRAIN CUBE
IPCOMM GmbH
IPCOS
ISET
iTAC SOFTWARE
jemmac software
JTEKT 株式会社ジェイテクト
JUNOT
kalycito
KASPERSKY
KEBA
kepware
KEVISION SYSTEMS
KONGSBERG
KETI Korea Electronics Technology Institute
KUKA
LACHMANN & RINK
Sofrel LACROIX
Laetus
Lenze
Leuze electronic
LG CNS
MSYSTEM
M&M SOFTWARE
macq
MASES
MatrikonOPC
MERCK
METAWATER
METTLER TOLEDO
MICROMEDIA INTERNATIONAL
Microsoft
EIMV
MISSION COMMUNICATIONS
MITSUBISHI ELECTRIC Changes for the Better
MHPS GROUP
Modigm
molex
MONITOR ELECTRIC
MOXA
NATIONAL INSTRUMENTS
NAPCON
NETx AUTOMATION
NOVOTEK
NXP
Ocean Data Systems
OFFSHORE systems
OMRON
OPC Labs
etap
OPTO 22
OSIsoft.
OWL
Parker
PEPPERL+FUCHS
PHOENIX CONTACT
PILZ
Polytec
Prediktor
PI PROFIBUS · PROFINET
progea
ProInterface
PROMESS
ПРОРЫВ
ProSoft SYSTEMS
PROSYS OPC
Prosyst
Protomation
QED Technologies
R2
RTA
red lion
Refine TECHNOLOGY
RENESAS
ROBOTICS WARE
Rockwell Automation
Rothenbacher
ROVISYS
SAC
SAMSUNG
SAP
Savigent
Schlumberger
Schneider Electric
SDI
Seeq
TRAXEED
sense force
SeQent
sequor
SEW EURODRIVE
ZHANWAN
SICK Sensor Intelligence.
SIEMENS
Signify
SISCO
SMS group
optimize! softing
software AG
Software toolbox
Solar Turbines A Caterpillar Company
Sontheim
splunk
SYNCRONTECH
SYNOPSYS
SYSTECH
systerel
SyTech
TAKEBISHI
talsen team
TECHNOLOG
TECHNO software
TERRANOVA
ThyssenKrupp
TOSHIBA Leading Innovation
TRAEGER.de
TRIANGLE MICROWORKS, INC.
Trihedral
TRUMPF
TSUBAKI
TTTech
Uhlmann
Unified Automation
utthunga
Valmet
verifarma
VMG
VISCOM
VisuTech System
Vision
VOLKSWAGEN
VTT
WAGO
Wapice
WATERFALL
WEBfactory
Weidmüller
WEINTEK
WERUM
WIBU SYSTEMS
WIND
window master
XITASO
XMPRO Agile Industrial IoT
xspera
YOKOGAWA
中控·SUPCON

02

Discovering the Attack Surface

or at least some of it..

Mapping the surface



Specifications

Communication Stack

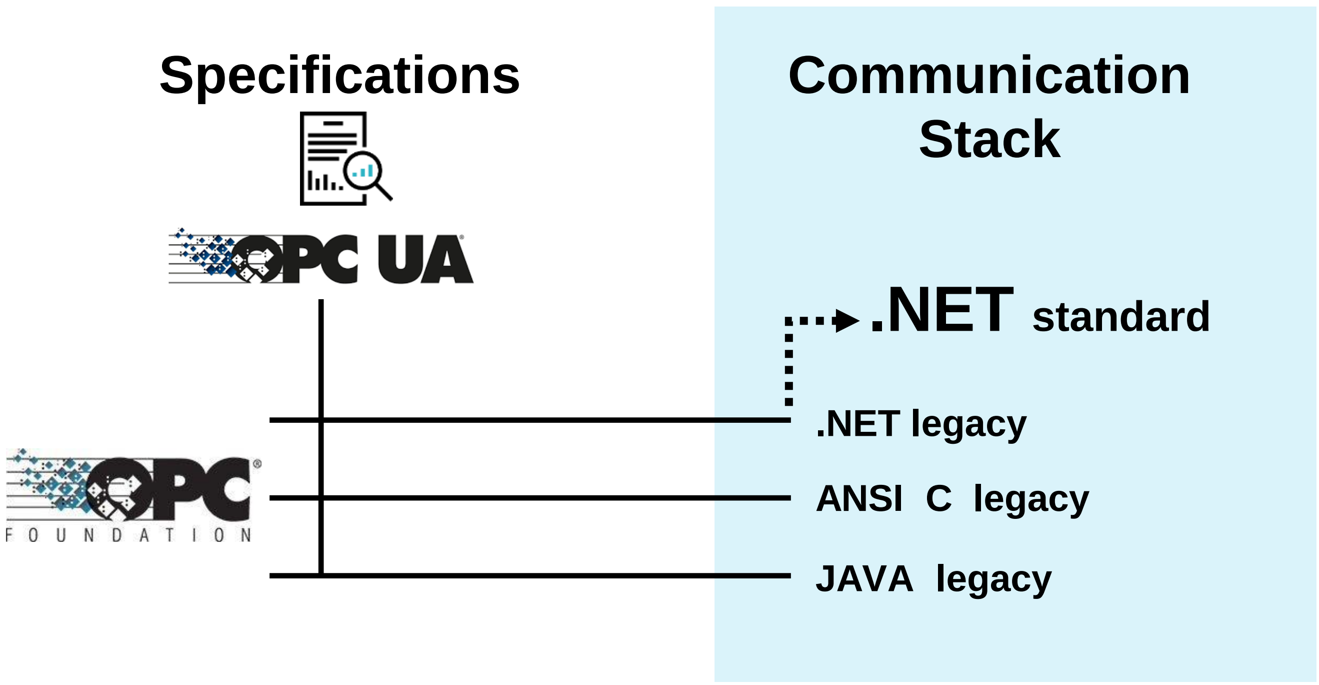
.NET Standard

.NET legacy

ANSI C legacy

JAVA legacy

Mapping the surface



Specifications

Communication Stack

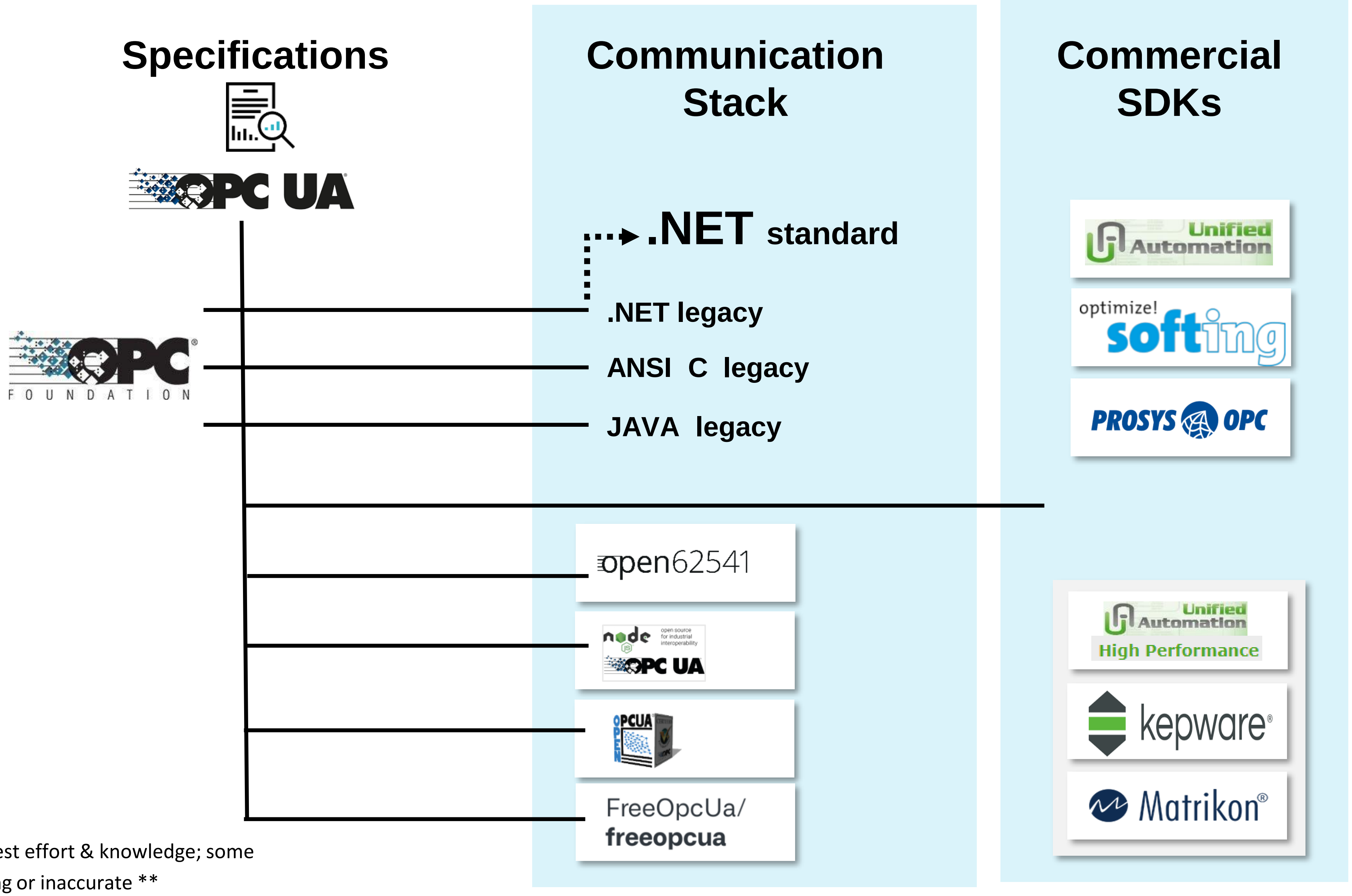
.NET standard

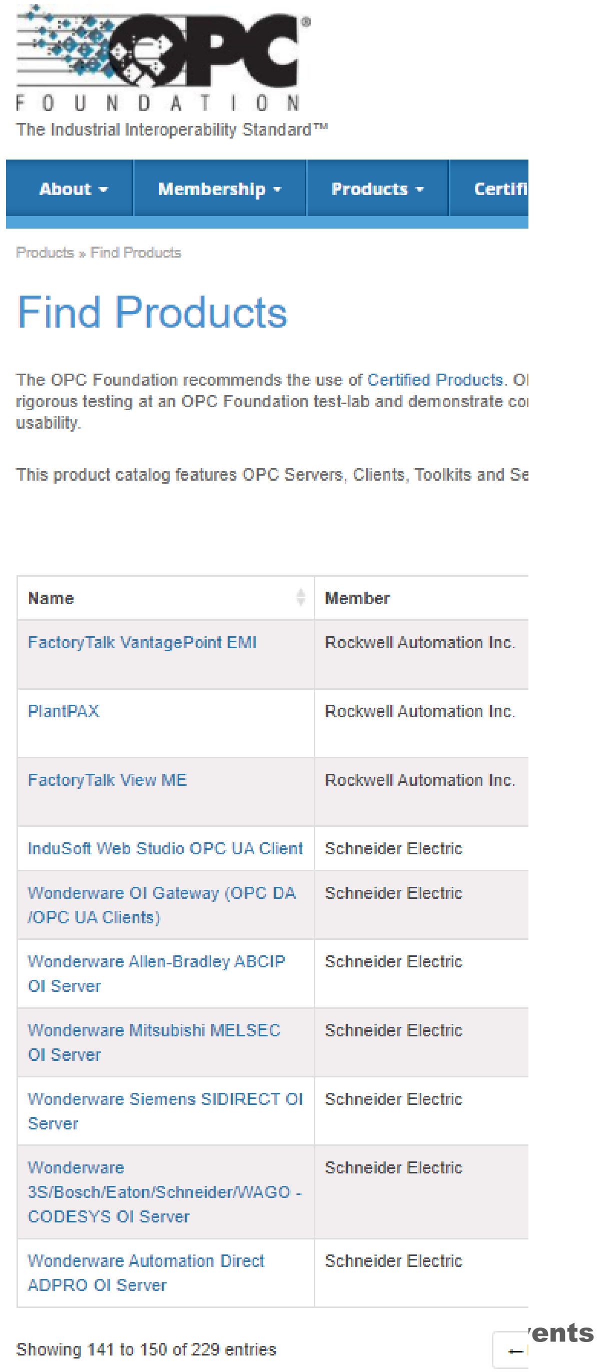
.NET legacy

ANSI C legacy

JAVA legacy

Mapping the surface





Find Products

The OPC Foundation recommends the use of Certified Products. O
rigorous testing at an OPC Foundation test-lab and demonstrate co
usability.

This product catalog features OPC Servers, Clients, Toolkits and Se

Name	Member
FactoryTalk VantagePoint EMI	Rockwell Automation Inc.
PlantPAX	Rockwell Automation Inc.
FactoryTalk View ME	Rockwell Automation Inc.
InduSoft Web Studio OPC UA Client	Schneider Electric
Wonderware OI Gateway (OPC DA /OPC UA Clients)	Schneider Electric
Wonderware Allen-Bradley ABCIP OI Server	Schneider Electric
Wonderware Mitsubishi MELSEC OI Server	Schneider Electric
Wonderware Siemens SIDIRECT OI Server	Schneider Electric
Wonderware 3S/Bosch/Eaton/Schneider/WAGO - CODESYS OI Server	Schneider Electric
Wonderware Automation Direct ADPRO OI Server	Schneider Electric

Showing 141 to 150 of 229 entries

ents

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

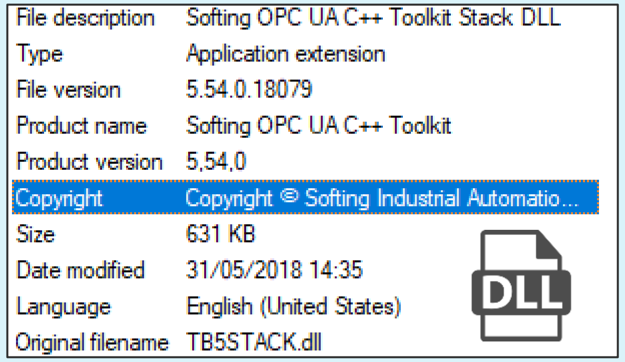
Mapping the surface

optimize! softing

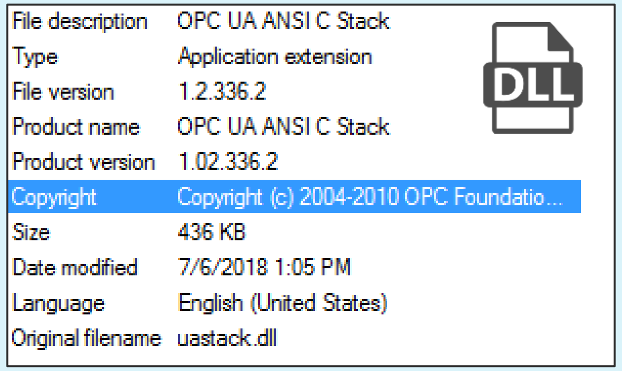
OPC FOUNDATION

Unified Automation

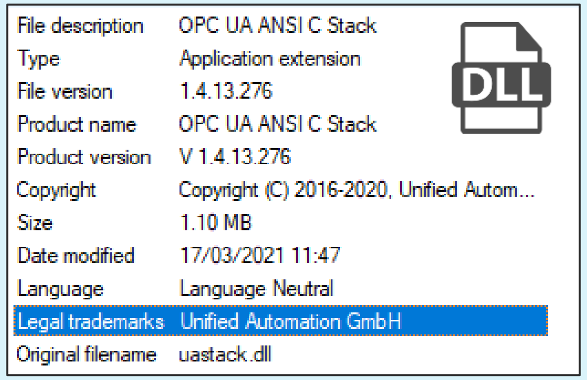
C / C++



File description	Softing OPC UA C++ Toolkit Stack DLL
Type	Application extension
File version	5.54.0.18079
Product name	Softing OPC UA C++ Toolkit
Product version	5,54,0
Copyright	Copyright © Softing Industrial Automatio...
Size	631 KB
Date modified	31/05/2018 14:35
Language	English (United States)
Original filename	TB5STACK.dll

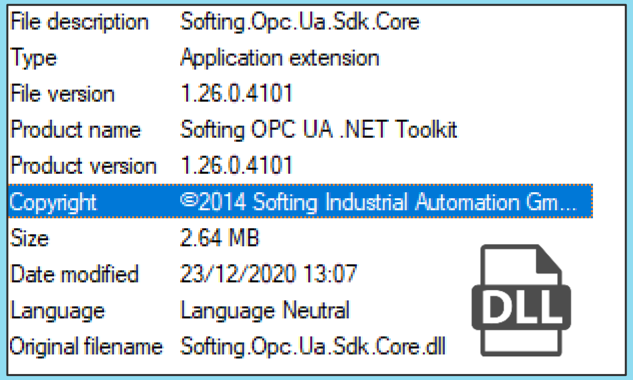


File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.2.336.2
Product name	OPC UA ANSI C Stack
Product version	1.02.336.2
Copyright	Copyright (c) 2004-2010 OPC Foundatio...
Size	436 KB
Date modified	7/6/2018 1:05 PM
Language	English (United States)
Original filename	uastack.dll

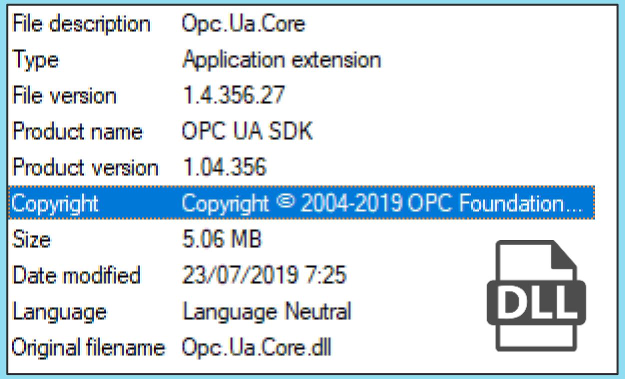


File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.4.13.276
Product name	OPC UA ANSI C Stack
Product version	V 1.4.13.276
Copyright	Copyright (C) 2016-2020, Unified Autom...
Size	1.10 MB
Date modified	17/03/2021 11:47
Language	Language Neutral
Legal trademarks	Unified Automation GmbH
Original filename	uastack.dll

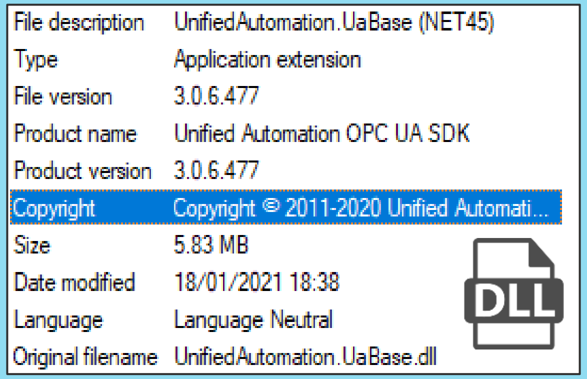
.NET



File description	Softing.Opc.Ua.Sdk.Core
Type	Application extension
File version	1.26.0.4101
Product name	Softing OPC UA .NET Toolkit
Product version	1.26.0.4101
Copyright	©2014 Softing Industrial Automation Gm...
Size	2.64 MB
Date modified	23/12/2020 13:07
Language	Language Neutral
Original filename	Softing.Opc.Ua.Sdk.Core.dll



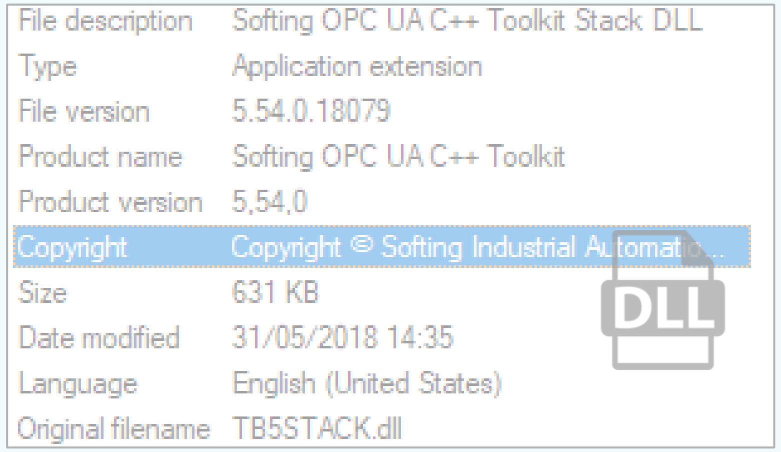
File description	Opc.Ua.Core
Type	Application extension
File version	1.4.356.27
Product name	OPC UA SDK
Product version	1.04.356
Copyright	Copyright © 2004-2019 OPC Foundation...
Size	5.06 MB
Date modified	23/07/2019 7:25
Language	Language Neutral
Original filename	Opc.Ua.Core.dll



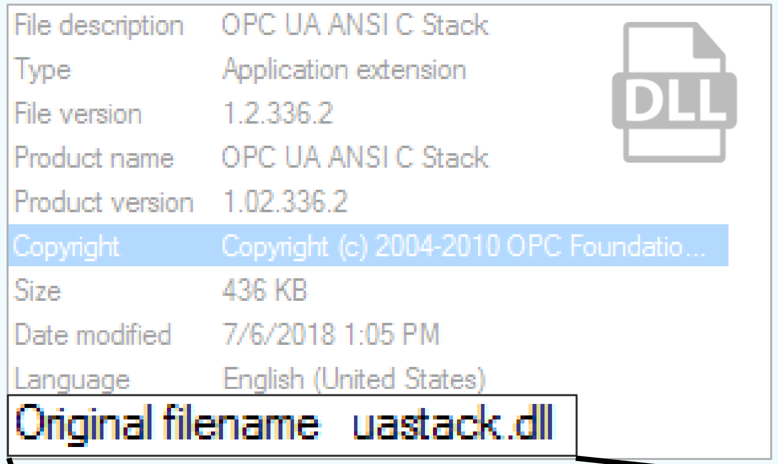
File description	UnifiedAutomation.UaBase (NET45)
Type	Application extension
File version	3.0.6.477
Product name	Unified Automation OPC UA SDK
Product version	3.0.6.477
Copyright	Copyright © 2011-2020 Unified Automati...
Size	5.83 MB
Date modified	18/01/2021 18:38
Language	Language Neutral
Original filename	UnifiedAutomation.UaBase.dll

Mapping the surface

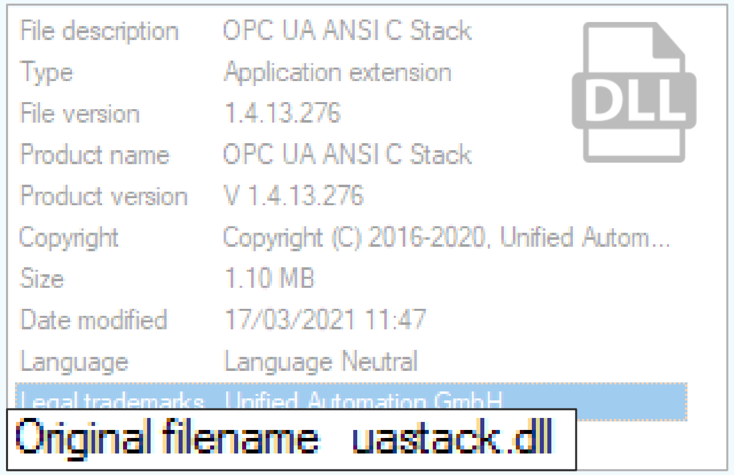
C / C++



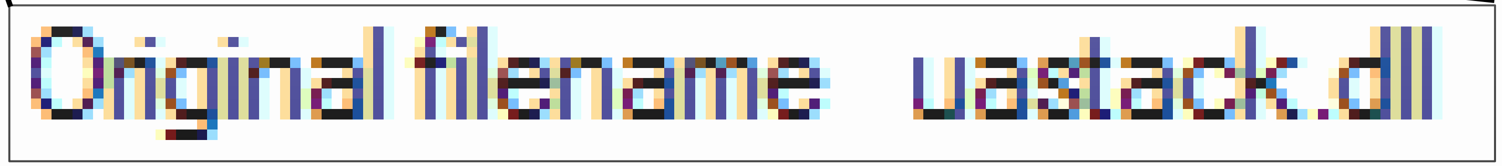
File description	Softing OPC UA C++ Toolkit Stack DLL
Type	Application extension
File version	5.54.0.18079
Product name	Softing OPC UA C++ Toolkit
Product version	5,54,0
Copyright	Copyright © Softing Industrial Automat...
Size	631 KB
Date modified	31/05/2018 14:35
Language	English (United States)
Original filename	TB5STACK.dll



File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.2.336.2
Product name	OPC UA ANSI C Stack
Product version	1.02.336.2
Copyright	Copyright (c) 2004-2010 OPC Foundatio...
Size	436 KB
Date modified	7/6/2018 1:05 PM
Language	English (United States)
Original filename	uastack.dll



File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.4.13.276
Product name	OPC UA ANSI C Stack
Product version	V 1.4.13.276
Copyright	Copyright (C) 2016-2020, Unified Autom...
Size	1.10 MB
Date modified	17/03/2021 11:47
Language	Language Neutral
Legal trademarks	Unified Automation GmbH
Original filename	uastack.dll

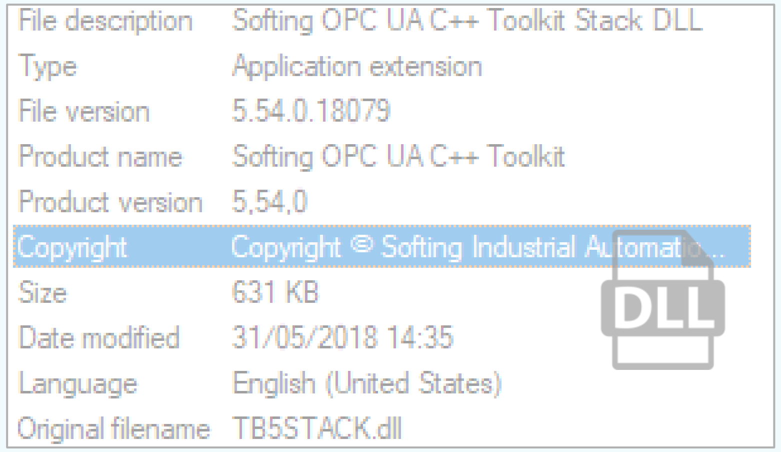


Original filename uastack.dll

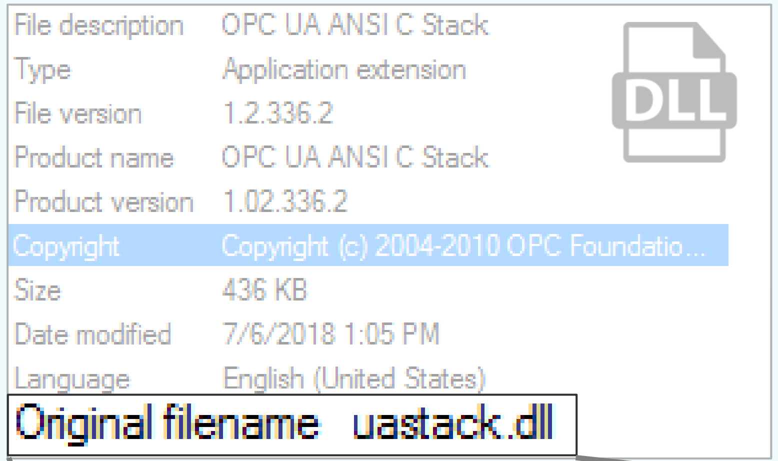
Mapping the surface

optimize! softing | OPC FOUNDATION | Unified Automation

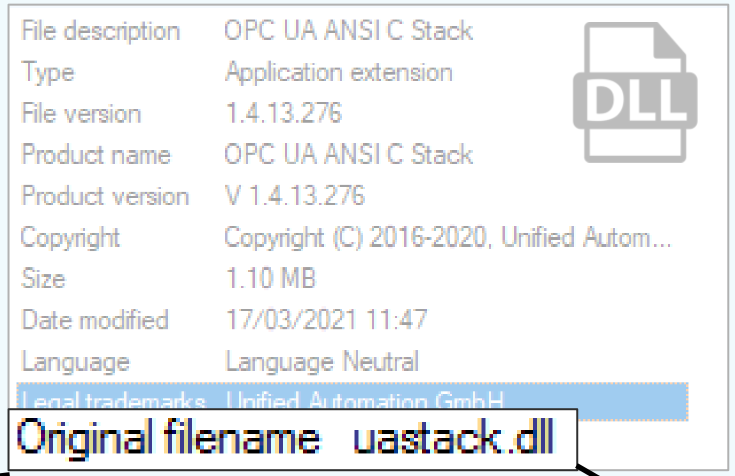
C / C++



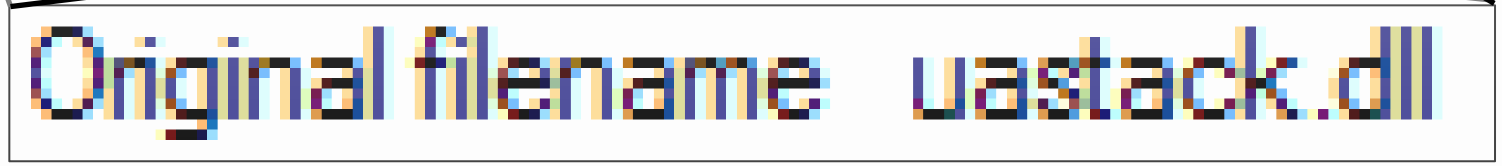
File description	Softing OPC UA C++ Toolkit Stack DLL
Type	Application extension
File version	5.54.0.18079
Product name	Softing OPC UA C++ Toolkit
Product version	5,54,0
Copyright	Copyright © Softing Industrial Automat...
Size	631 KB
Date modified	31/05/2018 14:35
Language	English (United States)
Original filename	TB5STACK.dll



File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.2.336.2
Product name	OPC UA ANSI C Stack
Product version	1.02.336.2
Copyright	Copyright (c) 2004-2010 OPC Foundatio...
Size	436 KB
Date modified	7/6/2018 1:05 PM
Language	English (United States)
Original filename	uastack.dll



File description	OPC UA ANSI C Stack
Type	Application extension
File version	1.4.13.276
Product name	OPC UA ANSI C Stack
Product version	V 1.4.13.276
Copyright	Copyright (C) 2016-2020, Unified Autom...
Size	1.10 MB
Date modified	17/03/2021 11:47
Language	Language Neutral
Legal trademarks	Unified Automation GmbH
Original filename	uastack.dll

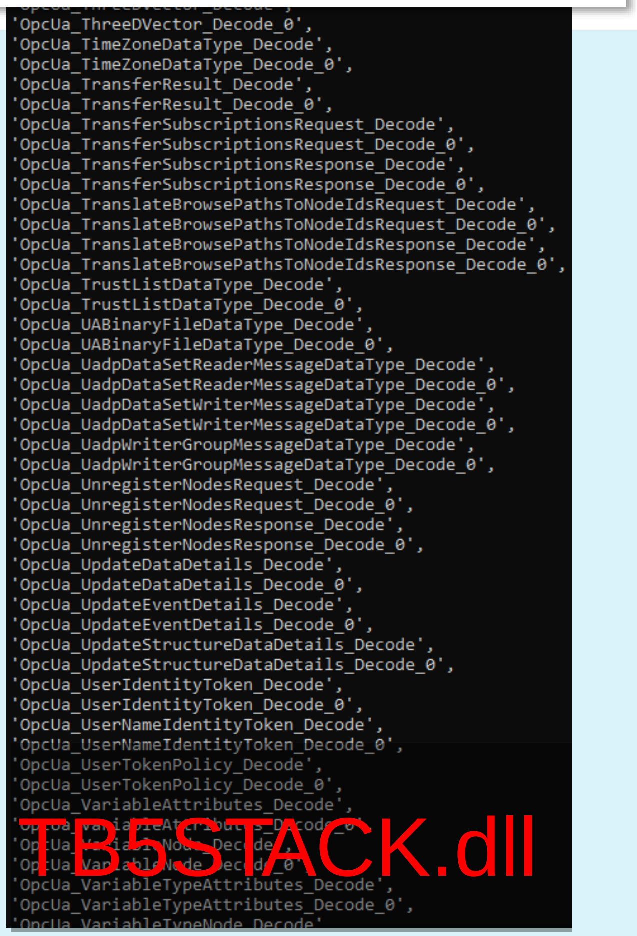


Original filename uastack.dll

Mapping the surface

C / C++

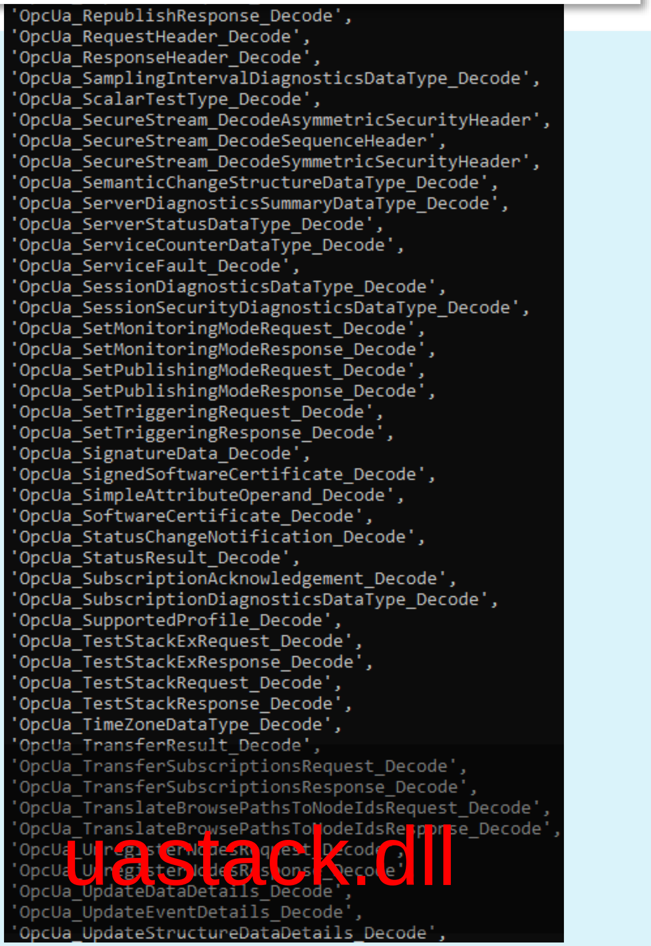
optimize! softing



```
'OpcUa_ThreeDVector_Decode',
'OpcUa_ThreeDVector_Decode_0',
'OpcUa_TimeZoneDataType_Decode',
'OpcUa_TimeZoneDataType_Decode_0',
'OpcUa_TransferResult_Decode',
'OpcUa_TransferResult_Decode_0',
'OpcUa_TransferSubscriptionsRequest_Decode',
'OpcUa_TransferSubscriptionsRequest_Decode_0',
'OpcUa_TransferSubscriptionsResponse_Decode',
'OpcUa_TransferSubscriptionsResponse_Decode_0',
'OpcUa_TranslateBrowsePathsToNodeIdsRequest_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsRequest_Decode_0',
'OpcUa_TranslateBrowsePathsToNodeIdsResponse_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsResponse_Decode_0',
'OpcUa_TrustListDataType_Decode',
'OpcUa_TrustListDataType_Decode_0',
'OpcUa_UABinaryFileDataType_Decode',
'OpcUa_UABinaryFileDataType_Decode_0',
'OpcUa_UadpDataSetReaderMessageDataType_Decode',
'OpcUa_UadpDataSetReaderMessageDataType_Decode_0',
'OpcUa_UadpDataSetWriterMessageDataType_Decode',
'OpcUa_UadpDataSetWriterMessageDataType_Decode_0',
'OpcUa_UadpWriterGroupMessageDataType_Decode',
'OpcUa_UadpWriterGroupMessageDataType_Decode_0',
'OpcUa_UnregisterNodesRequest_Decode',
'OpcUa_UnregisterNodesRequest_Decode_0',
'OpcUa_UnregisterNodesResponse_Decode',
'OpcUa_UnregisterNodesResponse_Decode_0',
'OpcUa_UpdateDataDetails_Decode',
'OpcUa_UpdateDataDetails_Decode_0',
'OpcUa_UpdateEventDetails_Decode',
'OpcUa_UpdateEventDetails_Decode_0',
'OpcUa_UpdateStructureDataDetails_Decode',
'OpcUa_UpdateStructureDataDetails_Decode_0',
'OpcUa_UserIdentityToken_Decode',
'OpcUa_UserIdentityToken_Decode_0',
'OpcUa_UserNameIdentityToken_Decode',
'OpcUa_UserNameIdentityToken_Decode_0',
'OpcUa_UserTokenPolicy_Decode',
'OpcUa_UserTokenPolicy_Decode_0',
'OpcUa_VariableAttributes_Decode',
'OpcUa_VariableAttributes_Decode_0',
'OpcUa_VariableNode_Decode',
'OpcUa_VariableNode_Decode_0',
'OpcUa_VariableTypeAttributes_Decode',
'OpcUa_VariableTypeAttributes_Decode_0',
'OpcUa_VariableTypeNode_Decode'
```

TB5STACK.dll

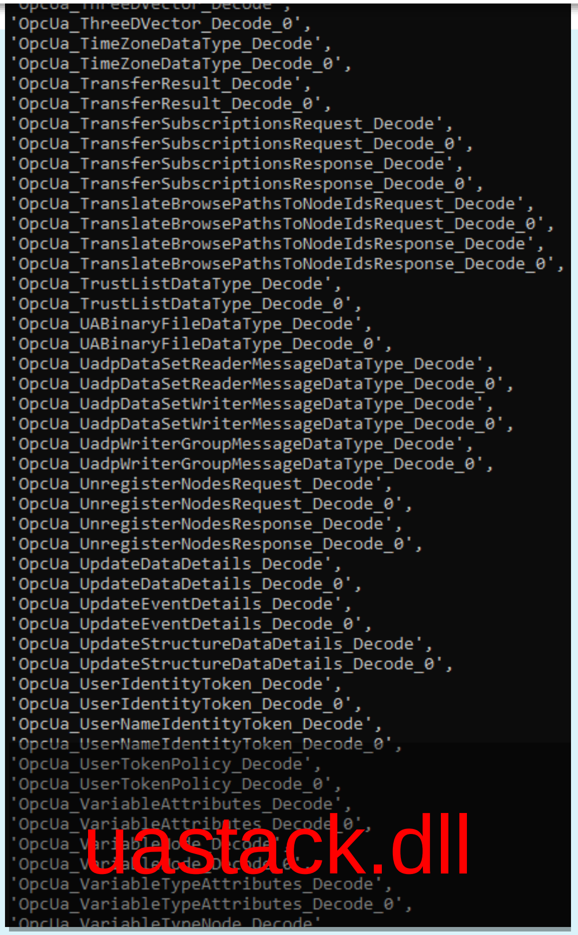
OPC FOUNDATION



```
'OpcUa_RepublishResponse_Decode',
'OpcUa_RequestHeader_Decode',
'OpcUa_ResponseHeader_Decode',
'OpcUa_SamplingIntervalDiagnosticsDataType_Decode',
'OpcUa_ScalarTestType_Decode',
'OpcUa_SecureStream_DecodeAsymmetricSecurityHeader',
'OpcUa_SecureStream_DecodeSequenceHeader',
'OpcUa_SecureStream_DecodeSymmetricSecurityHeader',
'OpcUa_SemanticChangeStructureDataType_Decode',
'OpcUa_ServerDiagnosticsSummaryDataType_Decode',
'OpcUa_ServerStatusDataType_Decode',
'OpcUa_ServiceCounterDataType_Decode',
'OpcUa_ServiceFault_Decode',
'OpcUa_SessionDiagnosticsDataType_Decode',
'OpcUa_SessionSecurityDiagnosticsDataType_Decode',
'OpcUa_SetMonitoringModeRequest_Decode',
'OpcUa_SetMonitoringModeResponse_Decode',
'OpcUa_SetPublishingModeRequest_Decode',
'OpcUa_SetPublishingModeResponse_Decode',
'OpcUa_SetTriggeringRequest_Decode',
'OpcUa_SetTriggeringResponse_Decode',
'OpcUa_SignatureData_Decode',
'OpcUa_SignedSoftwareCertificate_Decode',
'OpcUa_SimpleAttributeOperand_Decode',
'OpcUa_SoftwareCertificate_Decode',
'OpcUa_StatusChangeNotification_Decode',
'OpcUa_StatusResult_Decode',
'OpcUa_SubscriptionAcknowledgement_Decode',
'OpcUa_SubscriptionDiagnosticsDataType_Decode',
'OpcUa_SupportedProfile_Decode',
'OpcUa_TestStackExRequest_Decode',
'OpcUa_TestStackExResponse_Decode',
'OpcUa_TestStackRequest_Decode',
'OpcUa_TestStackResponse_Decode',
'OpcUa_TimeZoneDataType_Decode',
'OpcUa_TransferResult_Decode',
'OpcUa_TransferSubscriptionsRequest_Decode',
'OpcUa_TransferSubscriptionsResponse_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsRequest_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsResponse_Decode',
'OpcUa_UnregisterNodesRequest_Decode',
'OpcUa_UnregisterNodesResponse_Decode',
'OpcUa_UpdateDataDetails_Decode',
'OpcUa_UpdateEventDetails_Decode',
'OpcUa_UpdateStructureDataDetails_Decode',
```

uastack.dll

Unified Automation



```
'OpcUa_ThreeDVector_Decode',
'OpcUa_ThreeDVector_Decode_0',
'OpcUa_TimeZoneDataType_Decode',
'OpcUa_TimeZoneDataType_Decode_0',
'OpcUa_TransferResult_Decode',
'OpcUa_TransferResult_Decode_0',
'OpcUa_TransferSubscriptionsRequest_Decode',
'OpcUa_TransferSubscriptionsRequest_Decode_0',
'OpcUa_TransferSubscriptionsResponse_Decode',
'OpcUa_TransferSubscriptionsResponse_Decode_0',
'OpcUa_TranslateBrowsePathsToNodeIdsRequest_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsRequest_Decode_0',
'OpcUa_TranslateBrowsePathsToNodeIdsResponse_Decode',
'OpcUa_TranslateBrowsePathsToNodeIdsResponse_Decode_0',
'OpcUa_TrustListDataType_Decode',
'OpcUa_TrustListDataType_Decode_0',
'OpcUa_UABinaryFileDataType_Decode',
'OpcUa_UABinaryFileDataType_Decode_0',
'OpcUa_UadpDataSetReaderMessageDataType_Decode',
'OpcUa_UadpDataSetReaderMessageDataType_Decode_0',
'OpcUa_UadpDataSetWriterMessageDataType_Decode',
'OpcUa_UadpDataSetWriterMessageDataType_Decode_0',
'OpcUa_UadpWriterGroupMessageDataType_Decode',
'OpcUa_UadpWriterGroupMessageDataType_Decode_0',
'OpcUa_UnregisterNodesRequest_Decode',
'OpcUa_UnregisterNodesRequest_Decode_0',
'OpcUa_UnregisterNodesResponse_Decode',
'OpcUa_UnregisterNodesResponse_Decode_0',
'OpcUa_UpdateDataDetails_Decode',
'OpcUa_UpdateDataDetails_Decode_0',
'OpcUa_UpdateEventDetails_Decode',
'OpcUa_UpdateEventDetails_Decode_0',
'OpcUa_UpdateStructureDataDetails_Decode',
'OpcUa_UpdateStructureDataDetails_Decode_0',
'OpcUa_UserIdentityToken_Decode',
'OpcUa_UserIdentityToken_Decode_0',
'OpcUa_UserNameIdentityToken_Decode',
'OpcUa_UserNameIdentityToken_Decode_0',
'OpcUa_UserTokenPolicy_Decode',
'OpcUa_UserTokenPolicy_Decode_0',
'OpcUa_VariableAttributes_Decode',
'OpcUa_VariableAttributes_Decode_0',
'OpcUa_VariableNode_Decode',
'OpcUa_VariableNode_Decode_0',
'OpcUa_VariableTypeAttributes_Decode',
'OpcUa_VariableTypeAttributes_Decode_0',
'OpcUa_VariableTypeNode_Decode'
```

uastack.dll

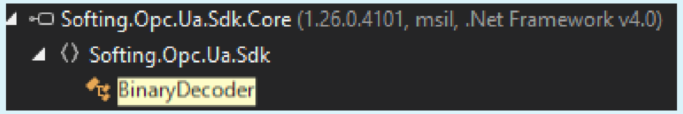
Mapping the surface

optimize! softing

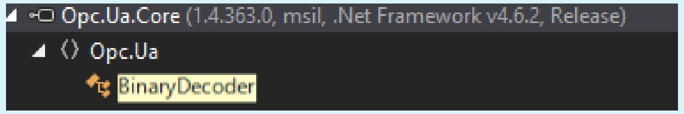
OPC FOUNDATION

Unified Automation

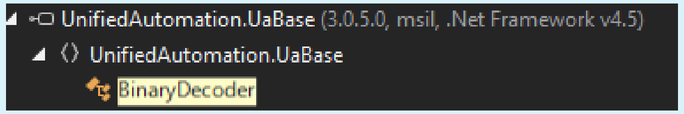
.NET



```
◢ ▫ Softing.Opc.Ua.Sdk.Core (1.26.0.4101, msil, .Net Framework v4.0)
  ◢ {} Softing.Opc.Ua.Sdk
       BinaryDecoder
```

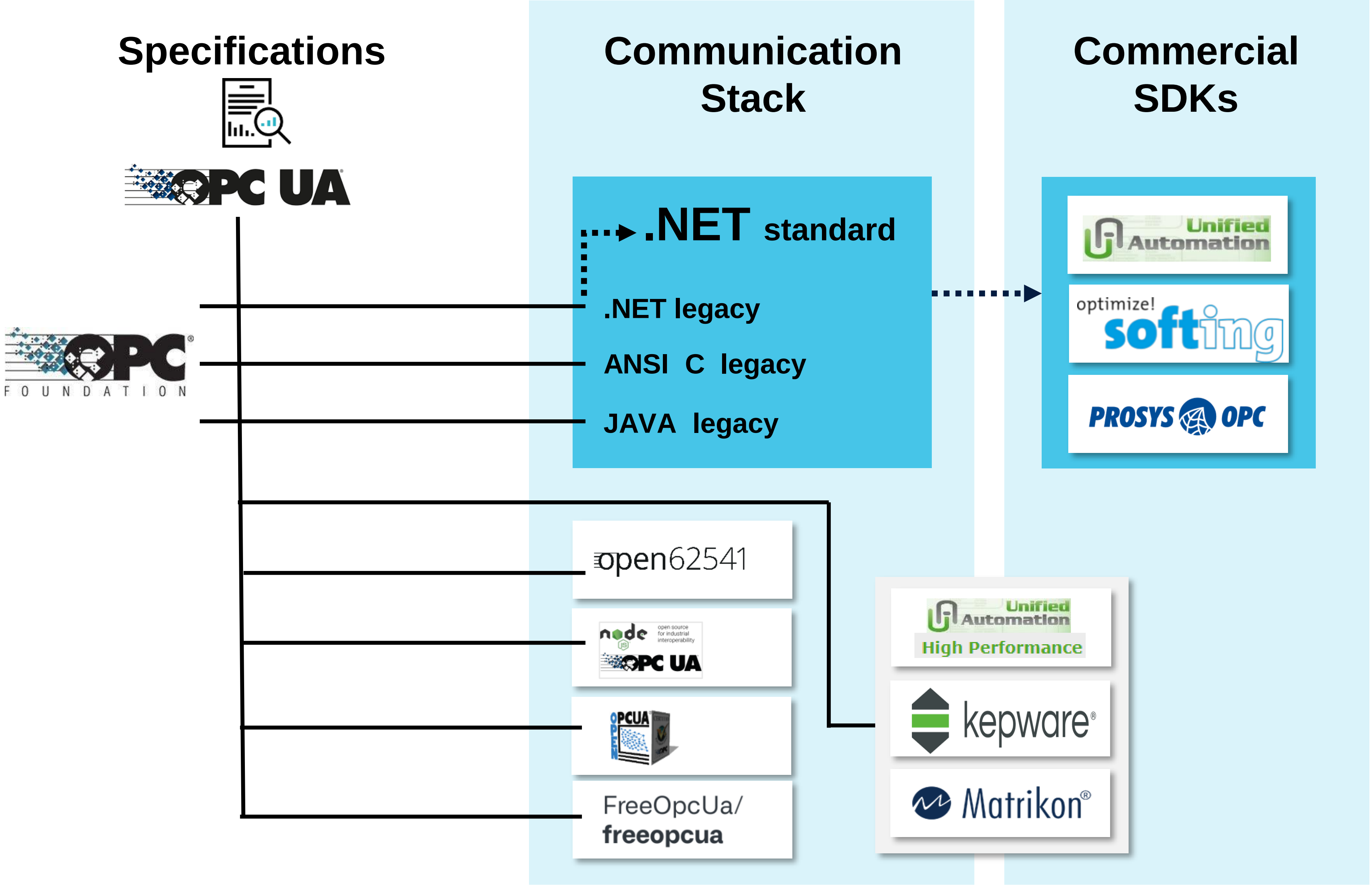


```
◢ ▫ Opc.Ua.Core (1.4.363.0, msil, .Net Framework v4.6.2, Release)
  ◢ {} Opc.Ua
       BinaryDecoder
```



```
◢ ▫ UnifiedAutomation.UaBase (3.0.5.0, msil, .Net Framework v4.5)
  ◢ {} UnifiedAutomation.UaBase
       BinaryDecoder
```

Mapping the surface



Specifications

Communication Stack

Commercial SDKs

.NET standard

.NET legacy

ANSI C legacy

JAVA legacy

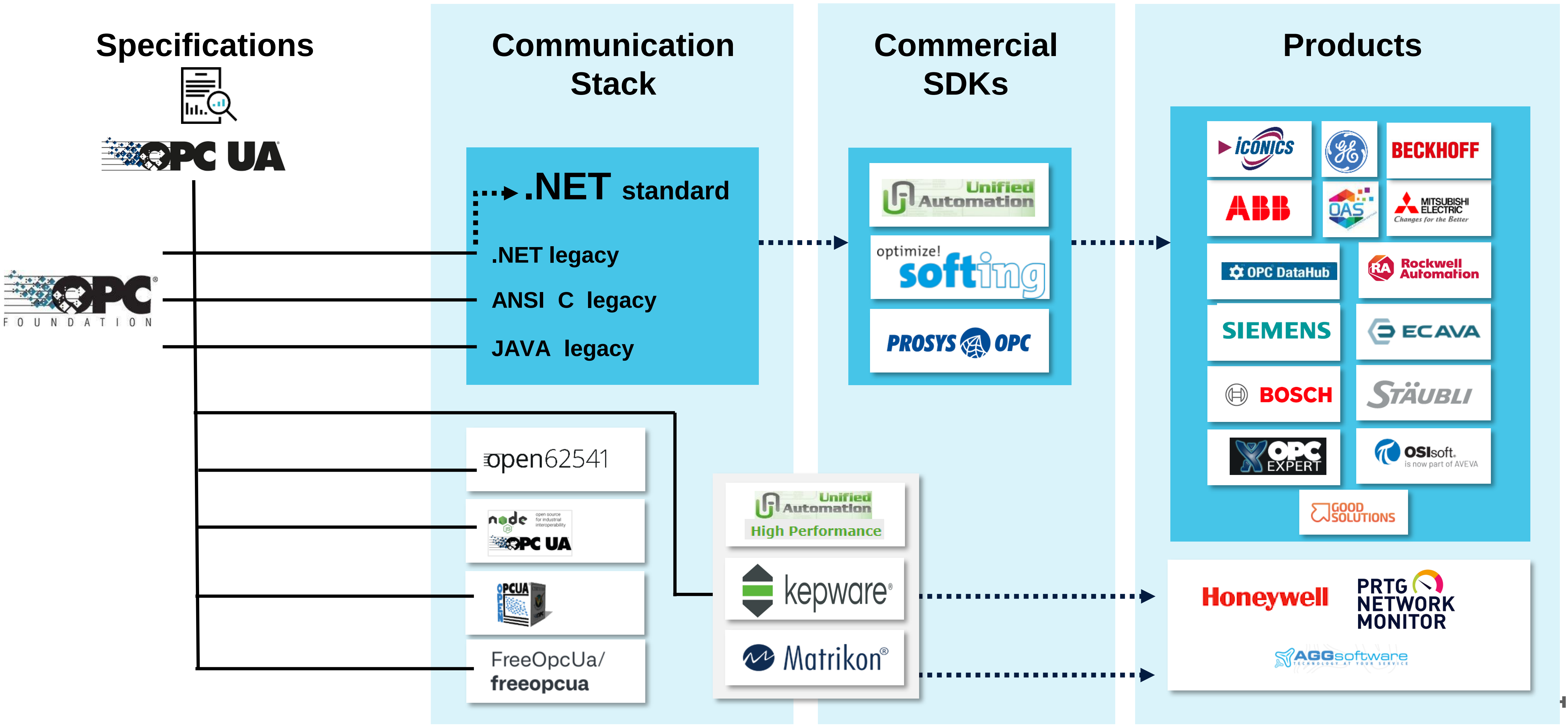
FreeOpcUa/ **freeopcua**

“The **vast majority of OPC UA products are based** on these commercial OPC UA SDK/**Toolkits**”

OPC Foundation

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Mapping the surface



Specifications

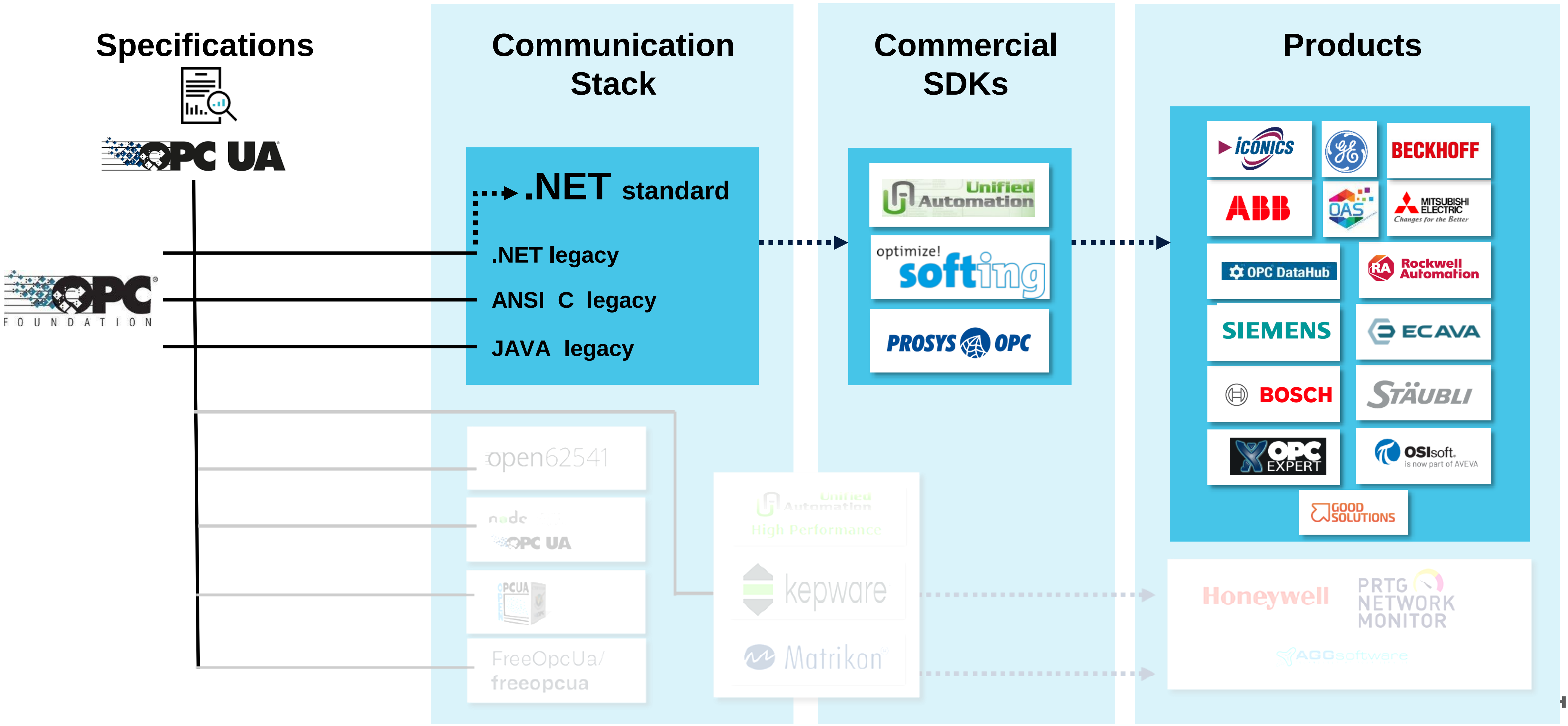
Communication Stack

Commercial SDKs

Products

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Chain of Dependency



Specifications

Communication Stack

Commercial SDKs

Products

.NET standard

.NET legacy

ANSI C legacy

JAVA legacy

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Pervious Work

OPC FOUNDATION

Active

OPC Foundation Security Working Group

Bundesamt für Sicherheit in der Informationstechnik

2017

German Office for Information Security (BSI)

kaspersky

2018, 2020

Kaspersky

CLAROTY Clarity for OT Networks

2021

Claroty

…

Academic papers

2021

- Practical Pitfalls for Security in OPC UA

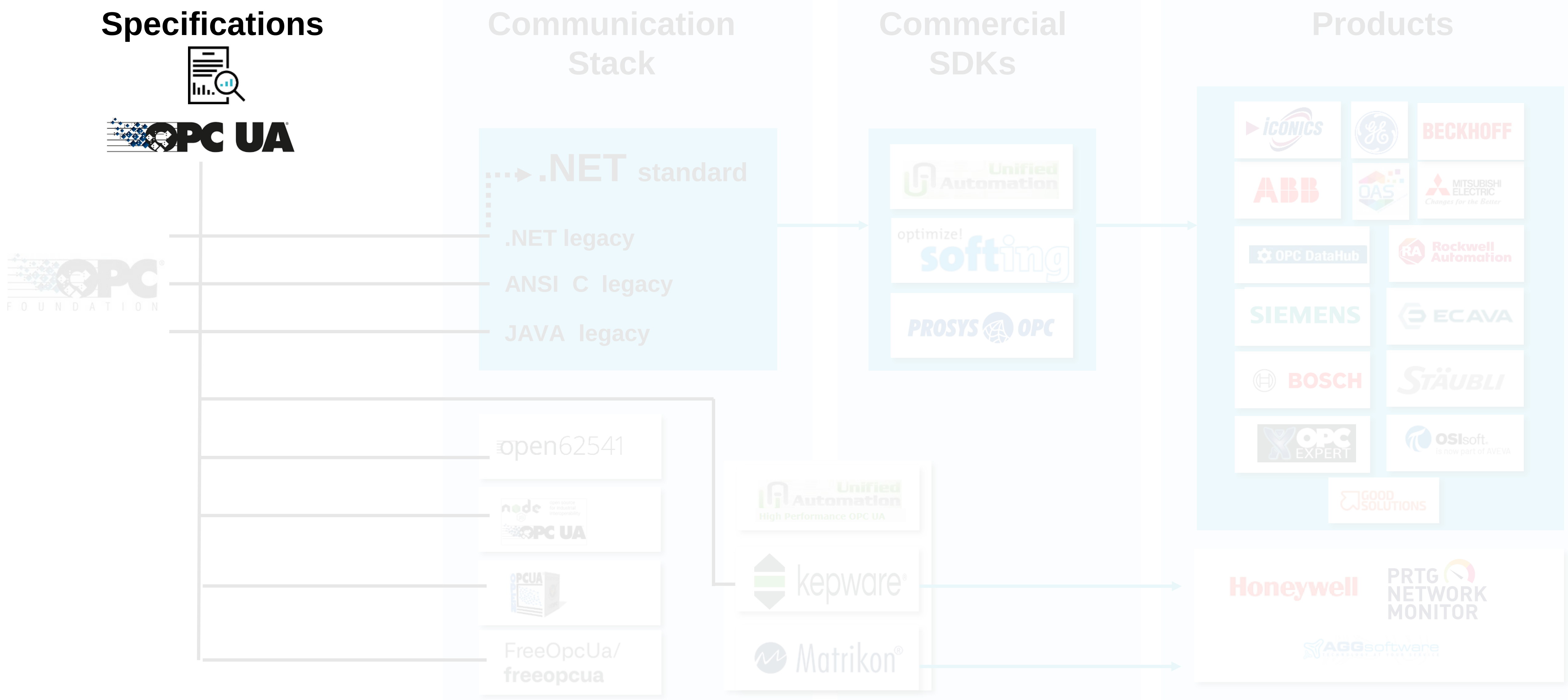
2020

- Assessing the Security of OPC UA Deployments
- …

03

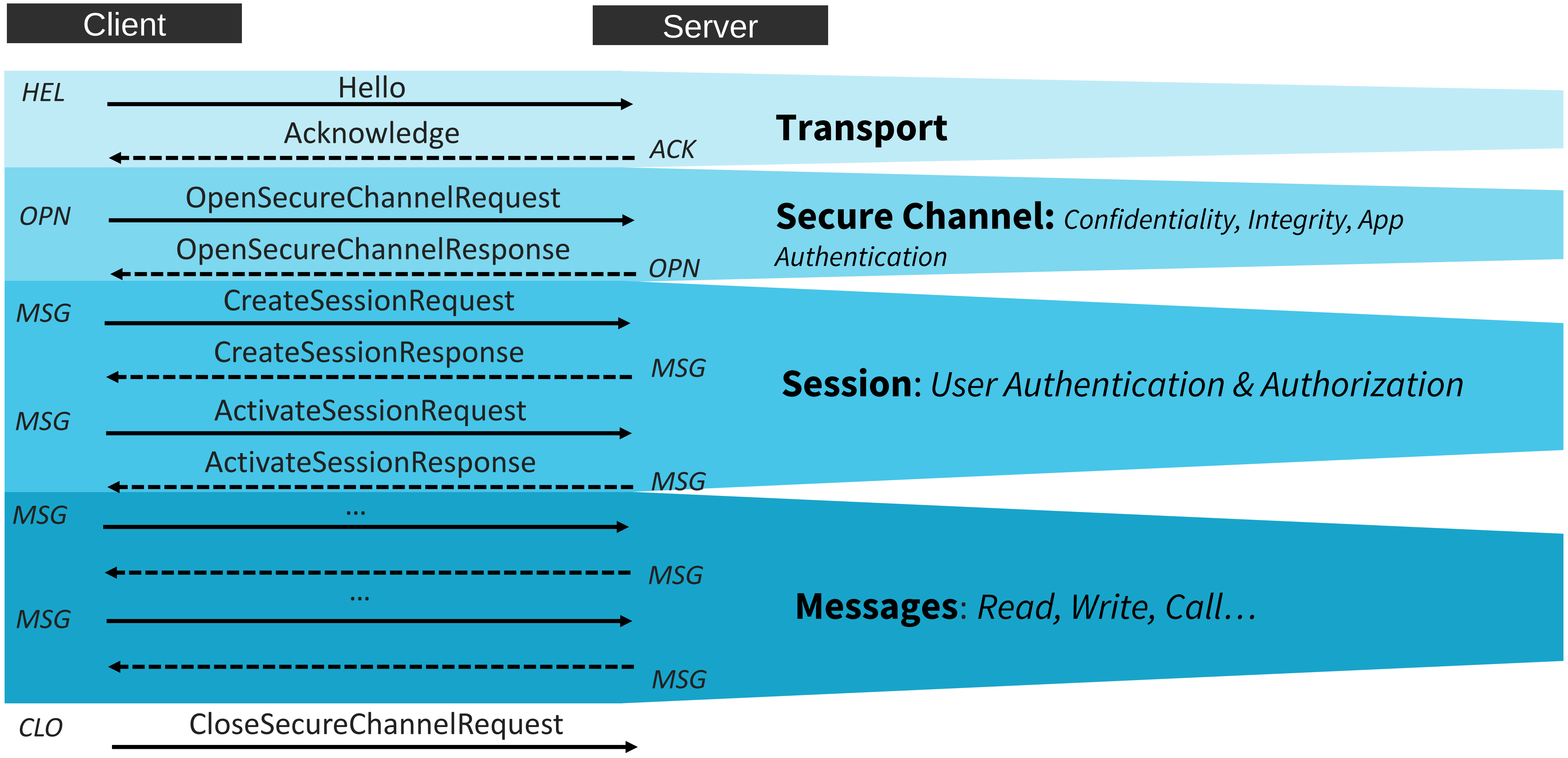
Exploiting the supply chain

Chain of Dependency



** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

OPC UA Connection



Client

Server

HEL Hello

Acknowledge ACK

Transport

OPN OpenSecureChannelRequest

OpenSecureChannelResponse OPN

Secure Channel: *Confidentiality, Integrity, App Authentication*

MSG CreateSessionRequest

CreateSessionResponse MSG

MSG ActivateSessionRequest

ActivateSessionResponse MSG

Session: *User Authentication & Authorization*

MSG …

MSG

MSG …

MSG

Messages: *Read, Write, Call…*

CLO CloseSecureChannelRequest

Reading the Reference

Complex Datatypes

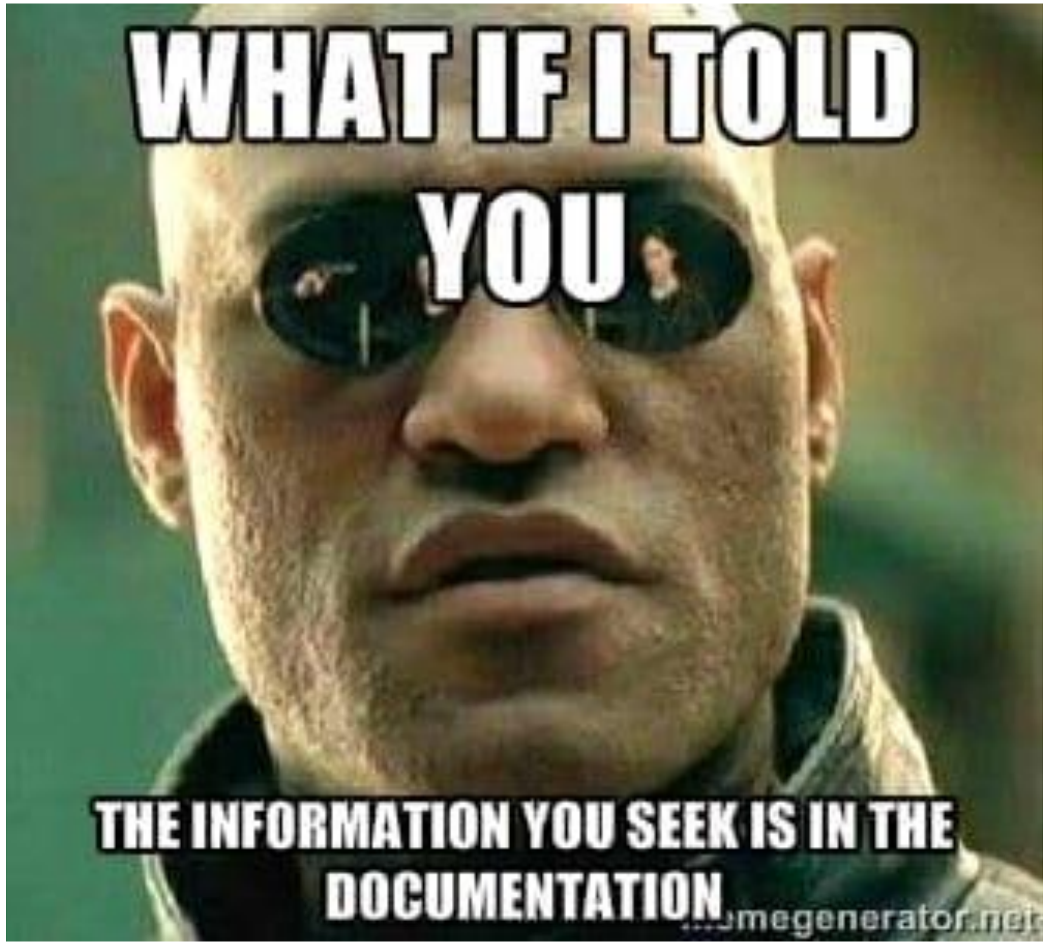
Variants, Extension Objects, Structures

Flexible Encoding

Binary, XML, JSON

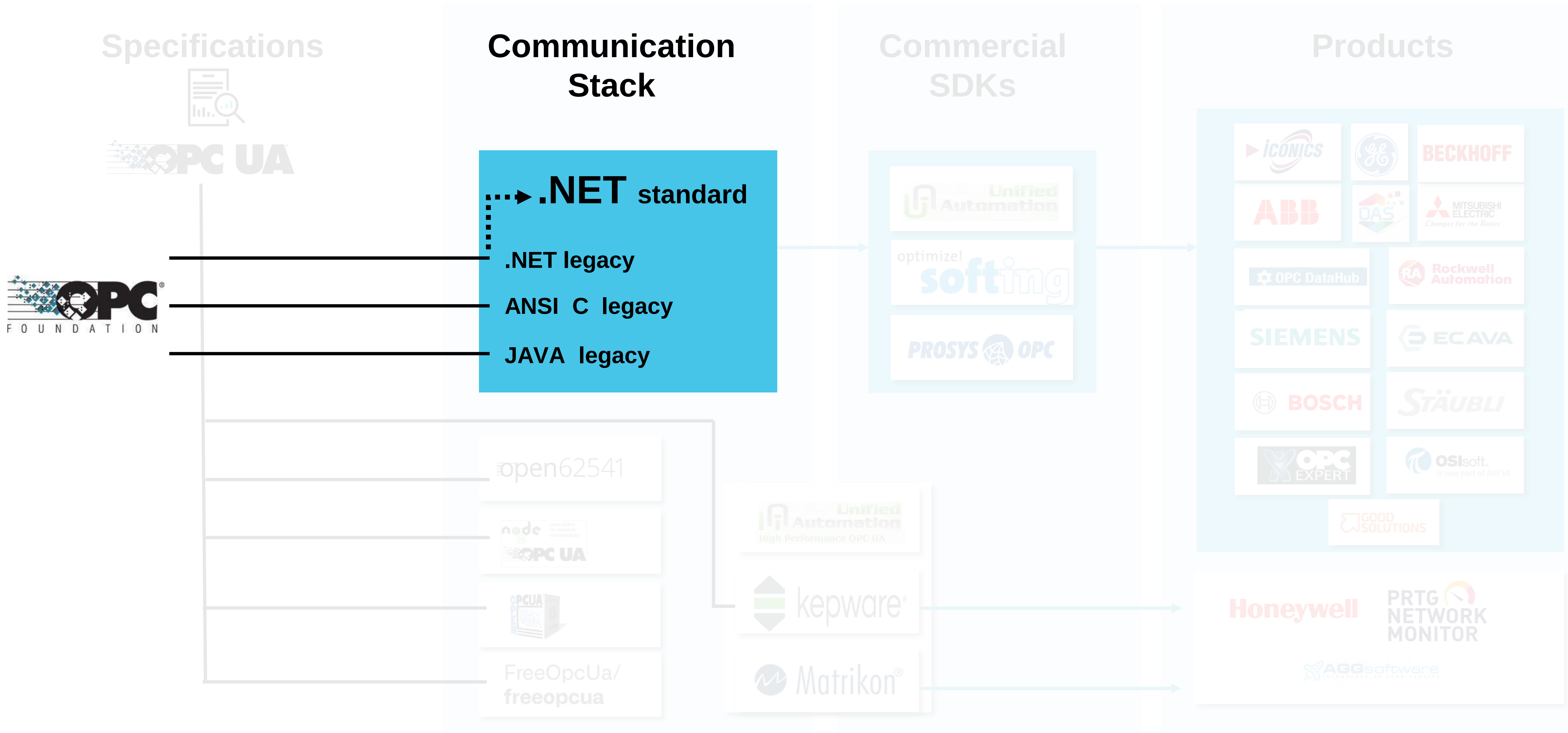
Pre-security messages

(OpenSecureChannel, GetEndpoints , FindServers…)



https://tyk.io/great-api-documentation-requires-code-examples/

Chain of Dependency



Specifications

Communication Stack

.NET standard

.NET legacy

ANSI C legacy

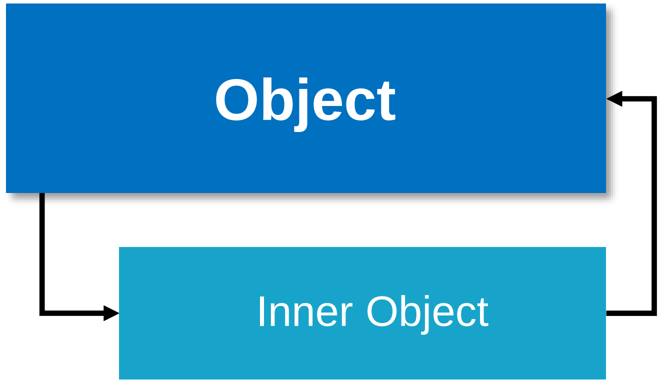
JAVA legacy

Commercial SDKs

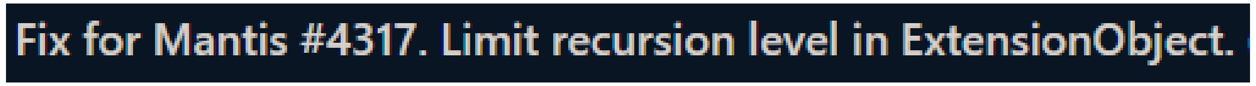
Products

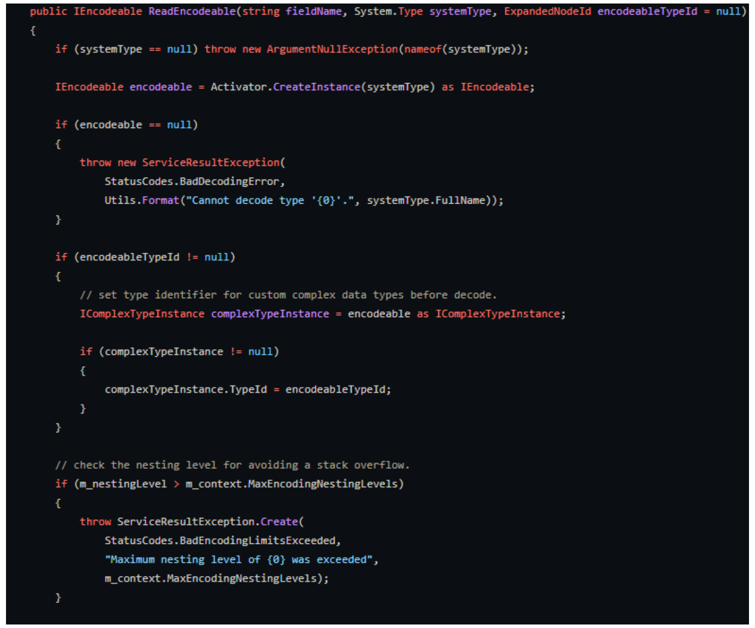
** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Breaking the .NET Stack

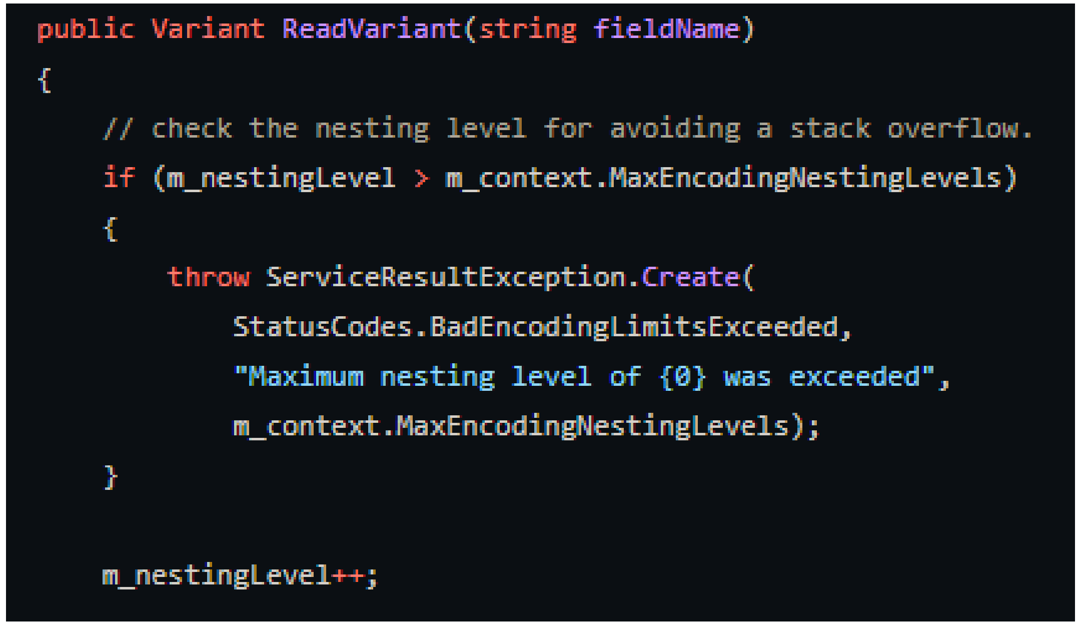


- NET doesn’t like deep function calls…
- The reference alerts of such risk when describing nested data types.
- A related issue was already found in the past (CVE-2018-12086):

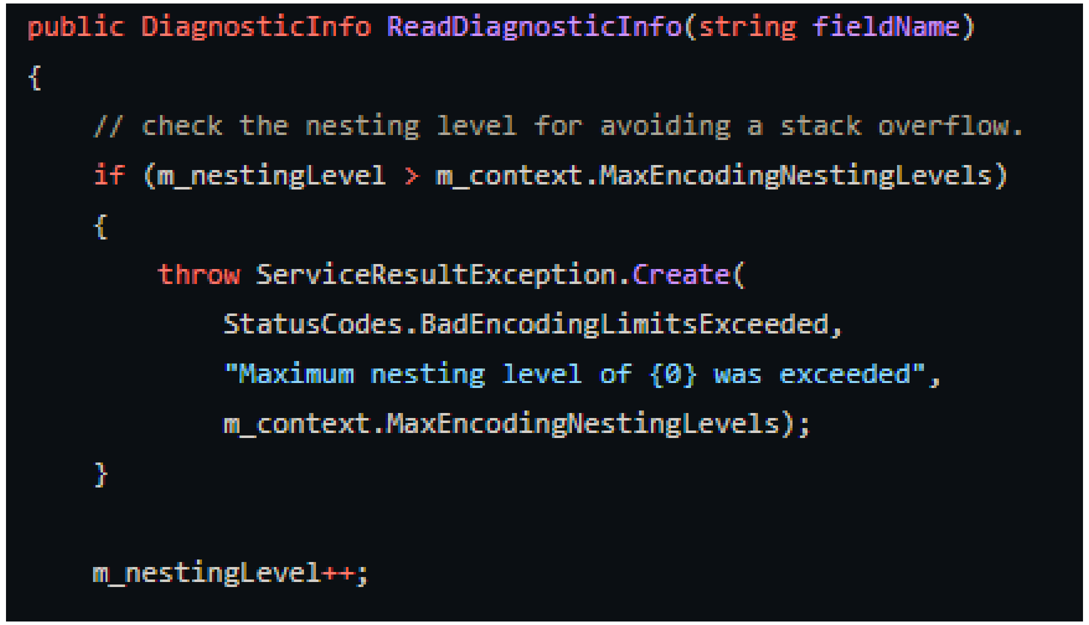

Fix for Mantis #4317. Limit recursion level in ExtensionObject.



```
public IEncodeable ReadEncodeable(string fieldName, System.Type systemType, ExpandedNodeId encodeableTypeId = null)
{
    if (systemType == null) throw new ArgumentNullException(nameof(systemType));

    IEncodeable encodeable = Activator.CreateInstance(systemType) as IEncodeable;

    if (encodeable == null)
    {
        throw new ServiceResultException(
            StatusCodes.BadDecodingError,
            Utils.Format("Cannot decode type '{0}'.", systemType.FullName));
    }

    if (encodeableTypeId != null)
    {
        // set type identifier for custom complex data types before decode.
        IComplexTypeInstance complexTypeInstance = encodeable as IComplexTypeInstance;

        if (complexTypeInstance != null)
        {
            complexTypeInstance.TypeId = encodeableTypeId;
        }
    }

    // check the nesting level for avoiding a stack overflow.
    if (m_nestingLevel > m_context.MaxEncodingNestingLevels)
    {
        throw ServiceResultException.Create(
            StatusCodes.BadEncodingLimitsExceeded,
            "Maximum nesting level of {0} was exceeded",
            m_context.MaxEncodingNestingLevels);
    }
```

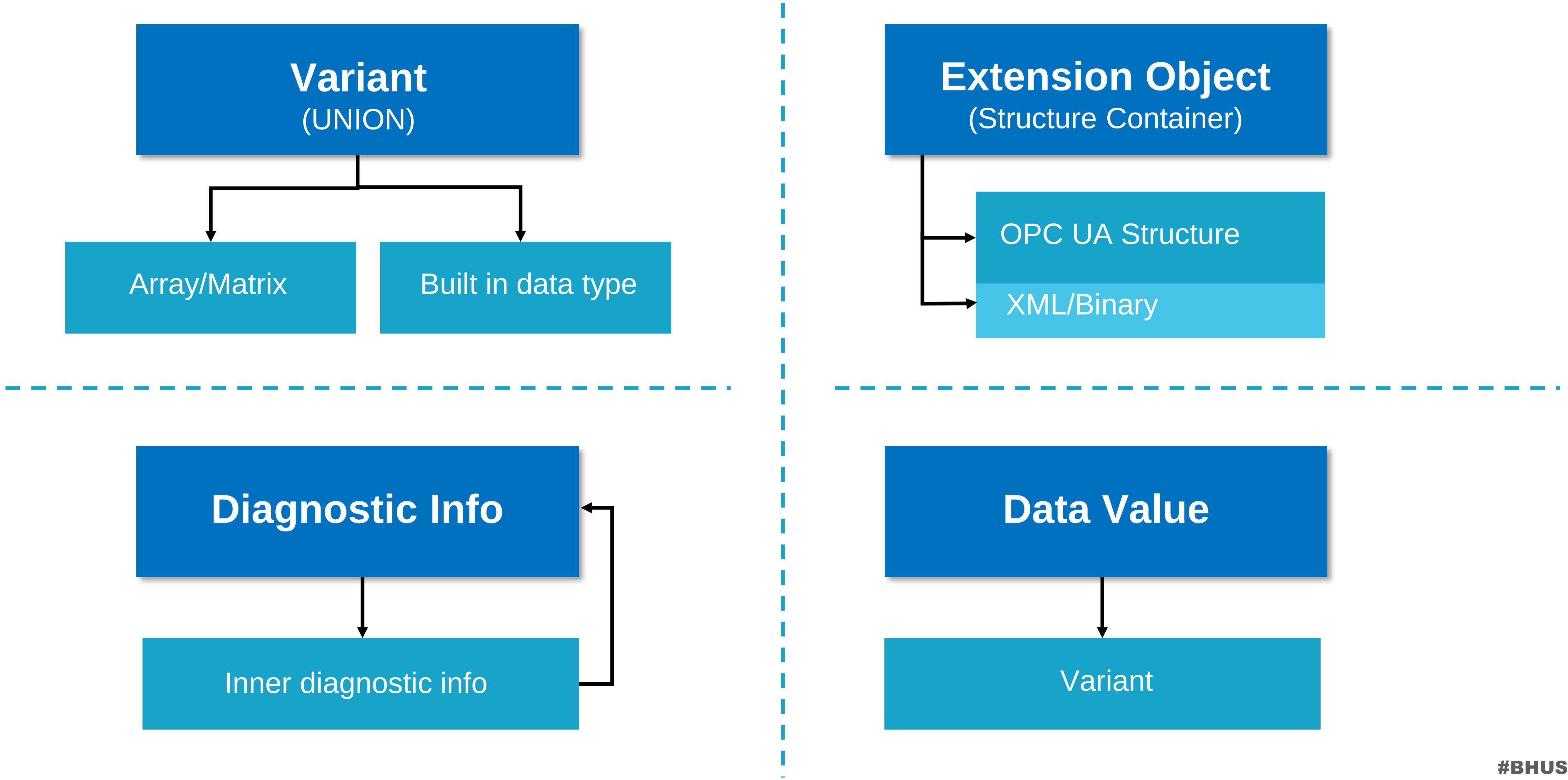


```
public Variant ReadVariant(string fieldName)
{
    // check the nesting level for avoiding a stack overflow.
    if (m_nestingLevel > m_context.MaxEncodingNestingLevels)
    {
        throw ServiceResultException.Create(
            StatusCodes.BadEncodingLimitsExceeded,
            "Maximum nesting level of {0} was exceeded",
            m_context.MaxEncodingNestingLevels);
    }

    m_nestingLevel++;
```



```
public DiagnosticInfo ReadDiagnosticInfo(string fieldName)
{
    // check the nesting level for avoiding a stack overflow.
    if (m_nestingLevel > m_context.MaxEncodingNestingLevels)
    {
        throw ServiceResultException.Create(
            StatusCodes.BadEncodingLimitsExceeded,
            "Maximum nesting level of {0} was exceeded",
            m_context.MaxEncodingNestingLevels);
    }

    m_nestingLevel++;
```

Nested Data Types



Variant
(UNION)

Array/Matrix

Built in data type

Extension Object
(Structure Container)

OPC UA Structure

XML/Binary

Diagnostic Info

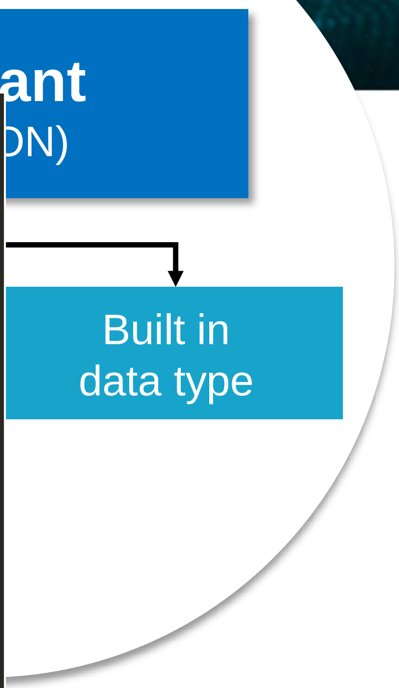
Inner diagnostic info

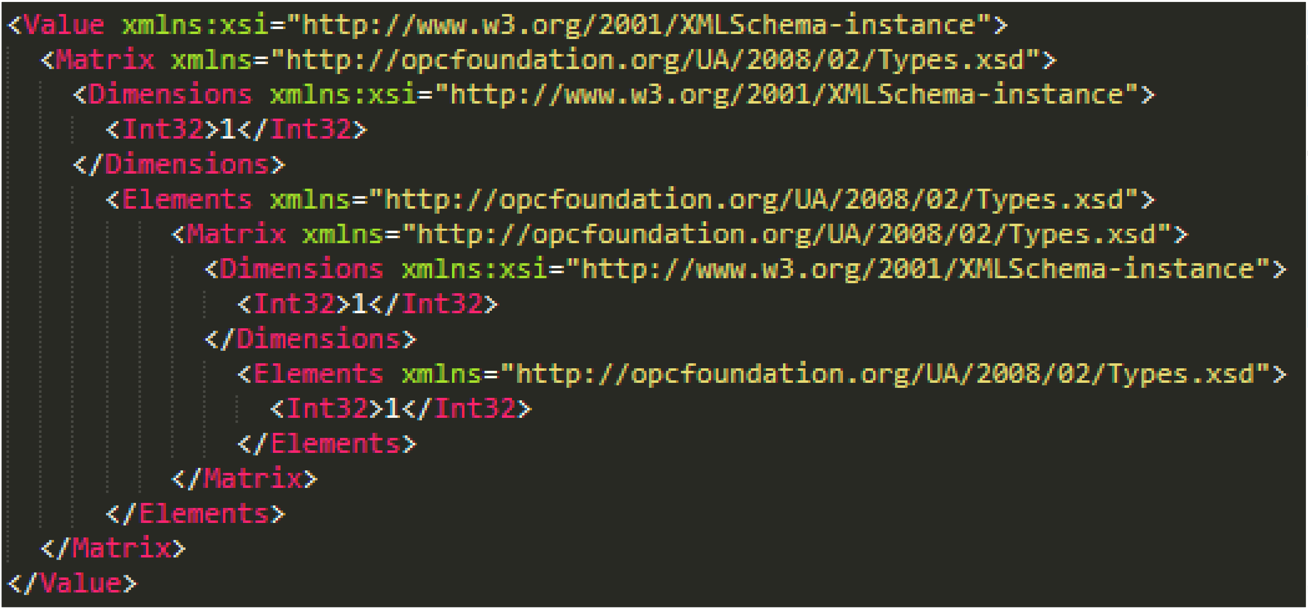
Data Value

Variant

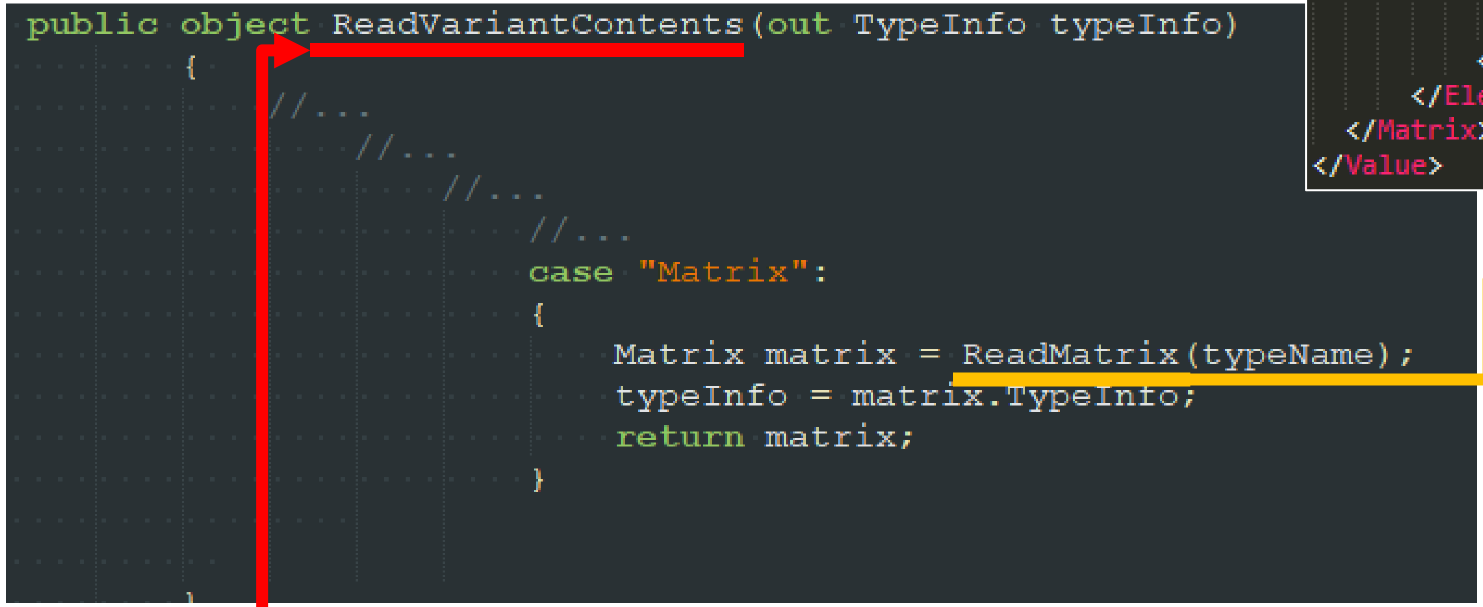
Unlimited Nesting

XML OPC UA Decoder

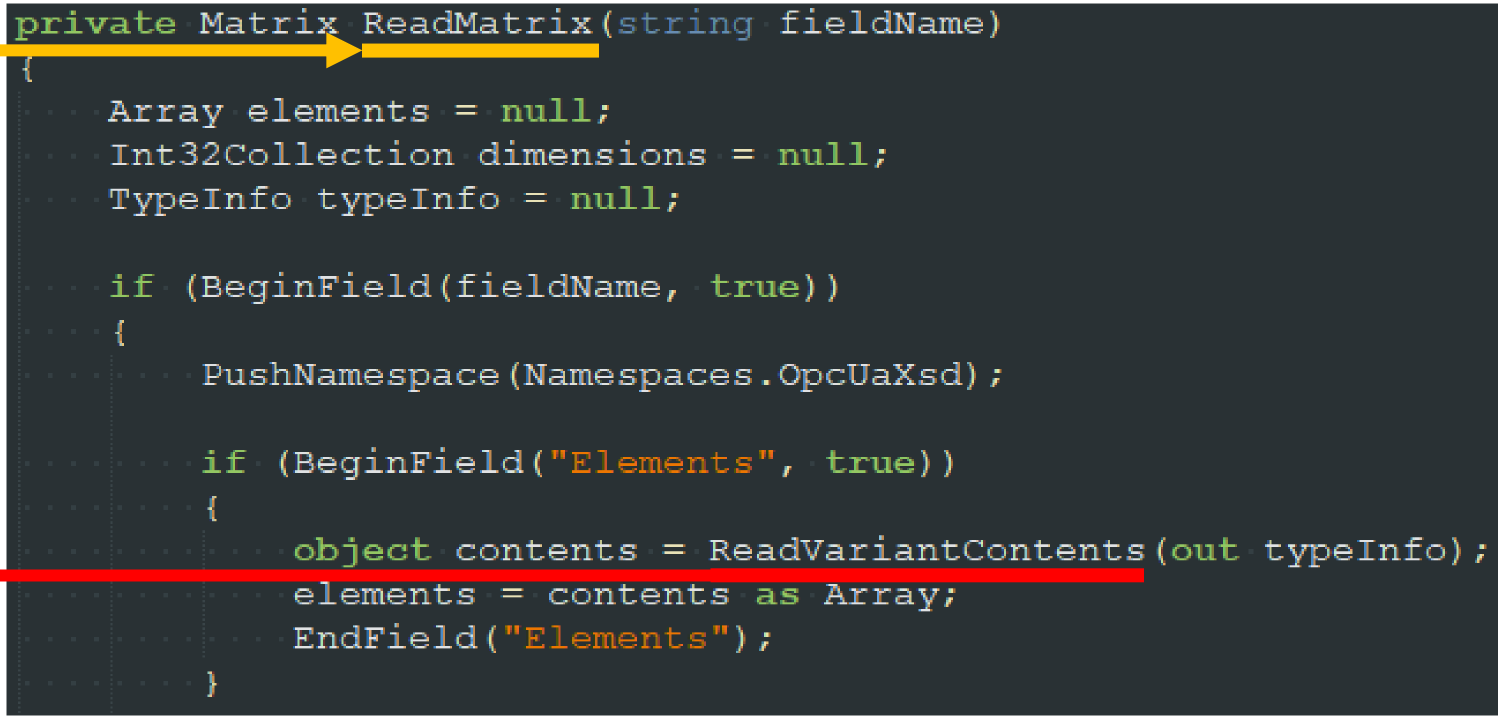




```xml
<Value xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Matrix xmlns="http://opcfoundation.org/UA/2008/02/Types.xsd">
    <Dimensions xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Int32>1</Int32>
    </Dimensions>
      <Elements xmlns="http://opcfoundation.org/UA/2008/02/Types.xsd">
          <Matrix xmlns="http://opcfoundation.org/UA/2008/02/Types.xsd">
            <Dimensions xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
              <Int32>1</Int32>
            </Dimensions>
              <Elements xmlns="http://opcfoundation.org/UA/2008/02/Types.xsd">
                <Int32>1</Int32>
              </Elements>
          </Matrix>
      </Elements>
  </Matrix>
</Value>
```



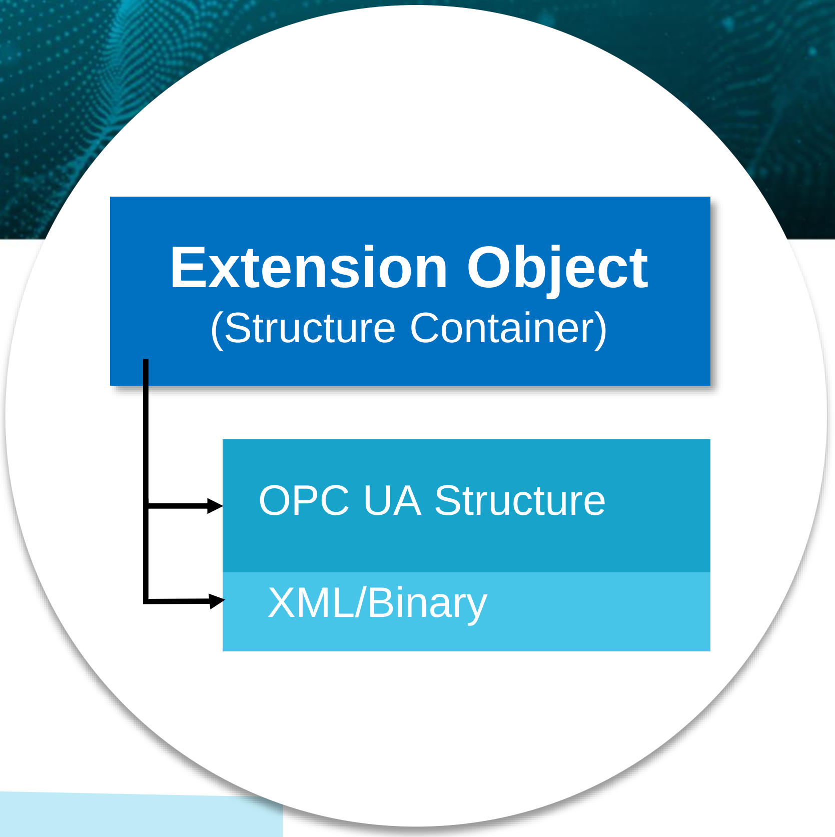
```csharp
public object ReadVariantContents(out TypeInfo typeInfo)
        {
            //...
                //...
                    //...
                        //...
                        case "Matrix":
                        {
                            Matrix matrix = ReadMatrix(typeName);
                            typeInfo = matrix.TypeInfo;
                            return matrix;
                        }
        }
```

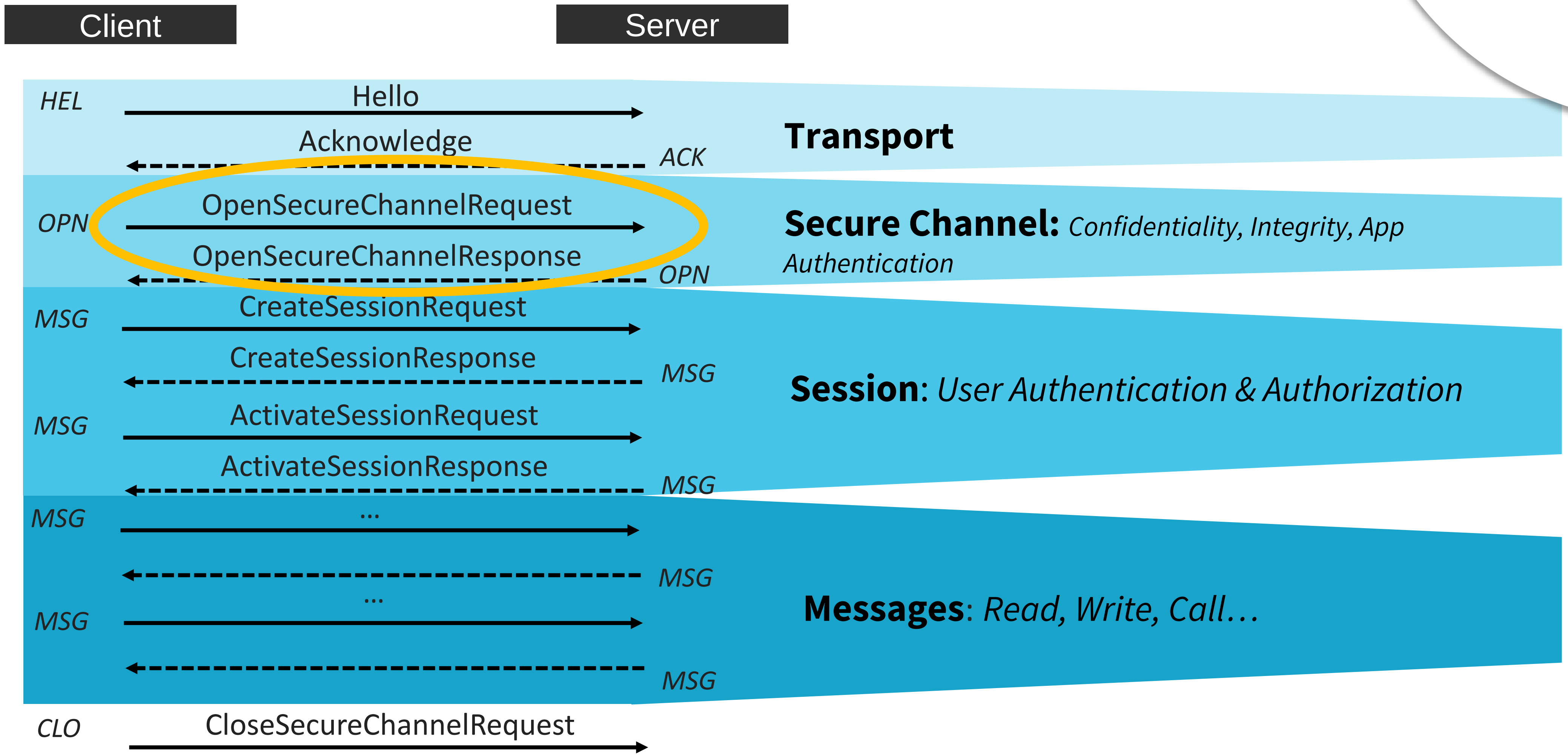


```csharp
private Matrix ReadMatrix(string fieldName)
{
    Array elements = null;
    Int32Collection dimensions = null;
    TypeInfo typeInfo = null;

    if (BeginField(fieldName, true))
    {
        PushNamespace(Namespaces.OpcUaXsd);

        if (BeginField("Elements", true))
        {
            object contents = ReadVariantContents(out typeInfo);
            elements = contents as Array;
            EndField("Elements");
        }
```

Nested Structures

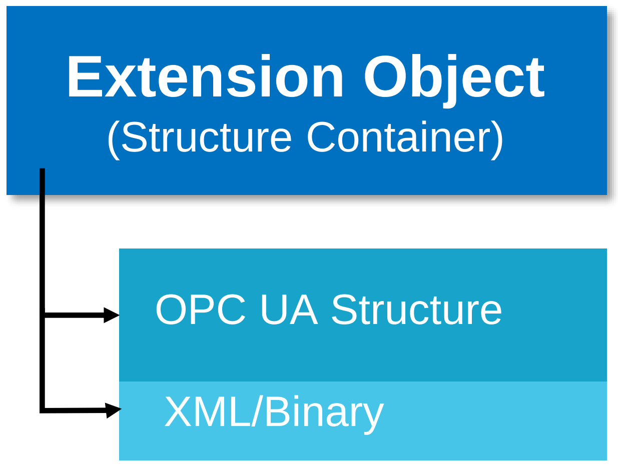
- **Extension Objects!**
- VERY useful for pivoting our way to vulnerable parts of the stacks
- Used in messages **before** channel or session **security** (in both directions)

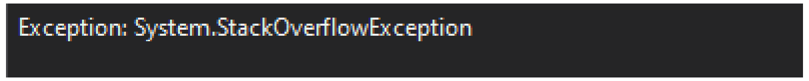




black hat USA 2021

Nested Structures



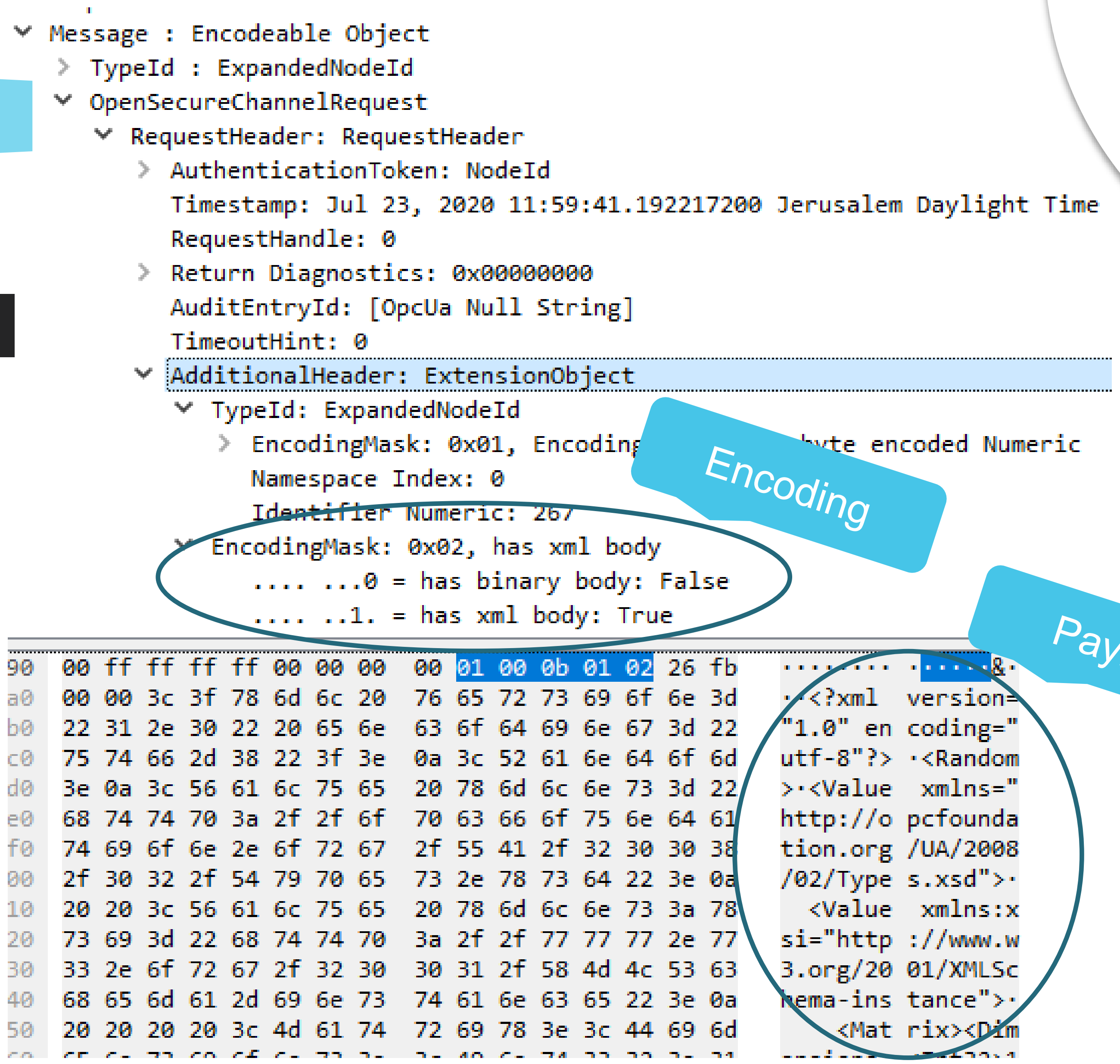


```
Exception: System.StackOverflowException
```

```
ReceiveBufferSize: 65536
SendBufferSize: 65536
```

```
ReceiveBufferSize: 8192
SendBufferSize: 8192
```

```
ReceiveBufferSize: 65535
SendBufferSize: 65535
```



```
Message : Encodeable Object
  TypeId : ExpandedNodeId
  OpenSecureChannelRequest
    RequestHeader: RequestHeader
      AuthenticationToken: NodeId
      Timestamp: Jul 23, 2020 11:59:41.192217200 Jerusalem Daylight Time
      RequestHandle: 0
      Return Diagnostics: 0x00000000
      AuditEntryId: [OpcUa Null String]
      TimeoutHint: 0
      AdditionalHeader: ExtensionObject
        TypeId: ExpandedNodeId
          EncodingMask: 0x01, Encoding           byte encoded Numeric
          Namespace Index: 0
          Identifier Numeric: 267
        EncodingMask: 0x02, has xml body
          .... ...0 = has binary body: False
          .... ..1. = has xml body: True
```

```
90  00 ff ff ff ff 00 00 00  00 01 00 0b 01 02 26 fb   ........ ......&·
a0  00 00 3c 3f 78 6d 6c 20  76 65 72 73 69 6f 6e 3d   ··<?xml  version=
b0  22 31 2e 30 22 20 65 6e  63 6f 64 69 6e 67 3d 22   "1.0" en coding="
c0  75 74 66 2d 38 22 3f 3e  0a 3c 52 61 6e 64 6f 6d   utf-8"?> ·<Random
d0  3e 0a 3c 56 61 6c 75 65  20 78 6d 6c 6e 73 3d 22   >·<Value  xmlns="
e0  68 74 74 70 3a 2f 2f 6f  70 63 66 6f 75 6e 64 61   http://o pcfounda
f0  74 69 6f 6e 2e 6f 72 67  2f 55 41 2f 32 30 30 38   tion.org /UA/2008
00  2f 30 32 2f 54 79 70 65  73 2e 78 73 64 22 3e 0a   /02/Type s.xsd">·
10  20 20 3c 56 61 6c 75 65  20 78 6d 6c 6e 73 3a 78     <Value  xmlns:x
20  73 69 3d 22 68 74 74 70  3a 2f 2f 77 77 77 2e 77   si="http ://www.w
30  33 2e 6f 72 67 2f 32 30  30 31 2f 58 4d 4c 53 63   3.org/20 01/XMLSc
40  68 65 6d 61 2d 69 6e 73  74 61 6e 63 65 22 3e 0a   hema-ins tance">·
50  20 20 20 20 3c 4d 61 74  72 69 78 3e 3c 44 69 6d       <Mat rix><Dim
```

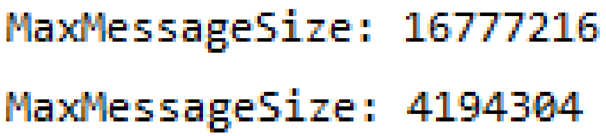
Encoding

Payload

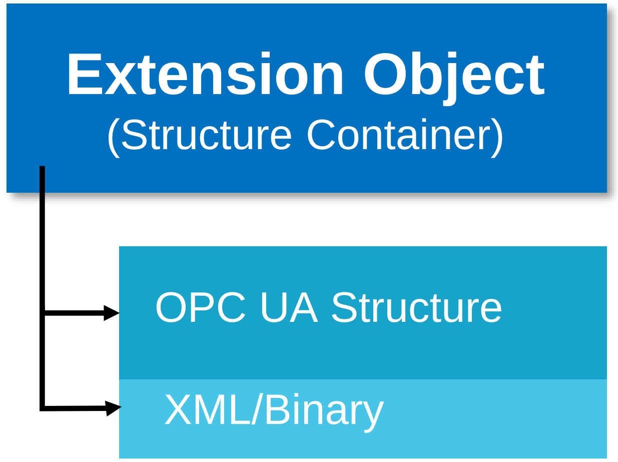
#BHUSA @BlackHatEvents

Nested Structures

- Chunks.



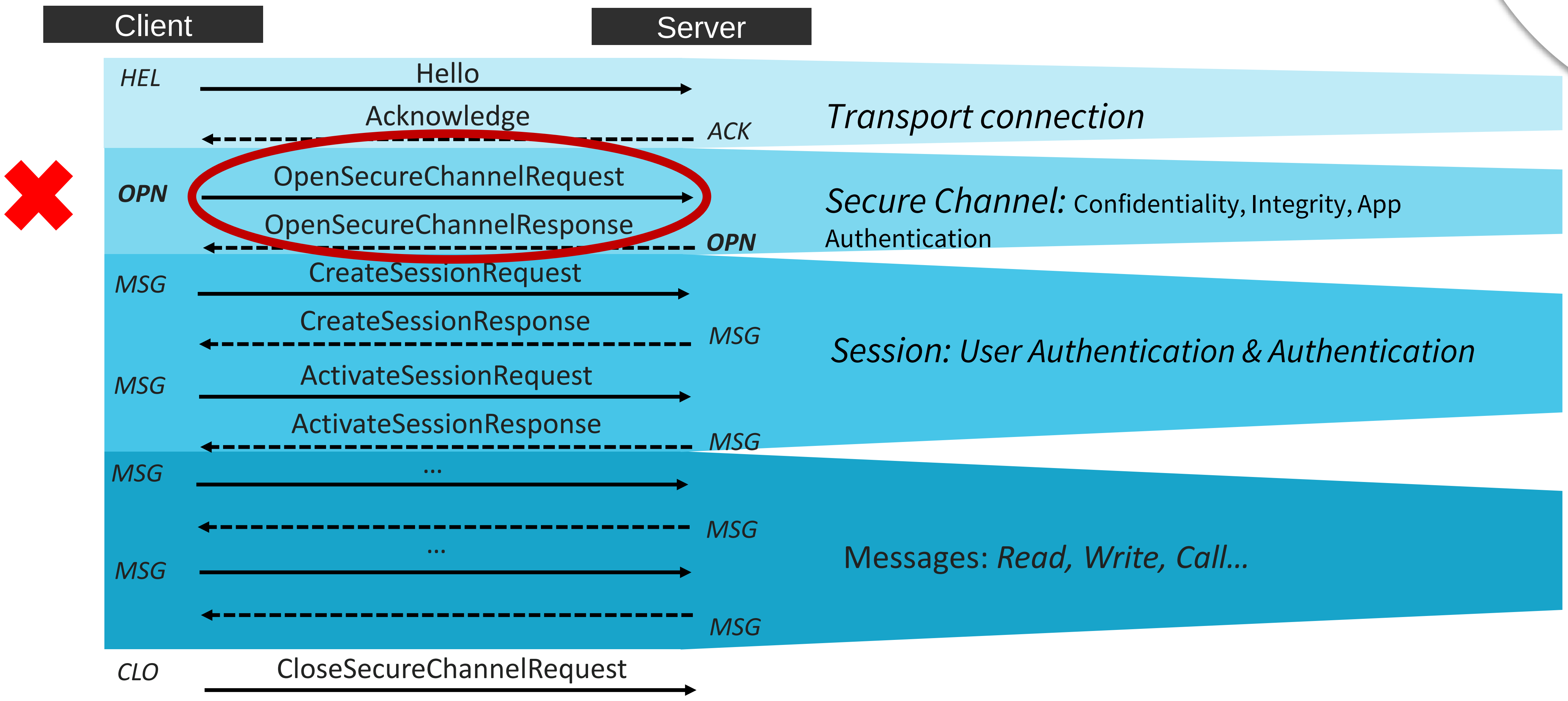
```
MaxMessageSize: 16777216

MaxMessageSize: 4194304
```

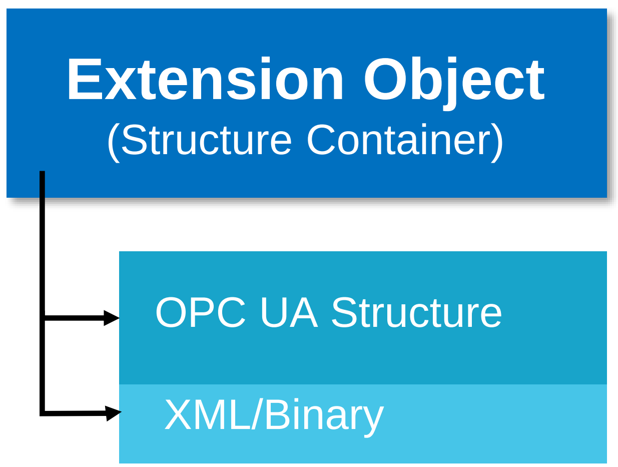


Extension Object (Structure Container)

OPC UA Structure

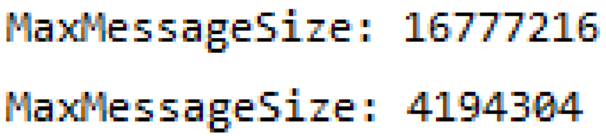
XML/Binary



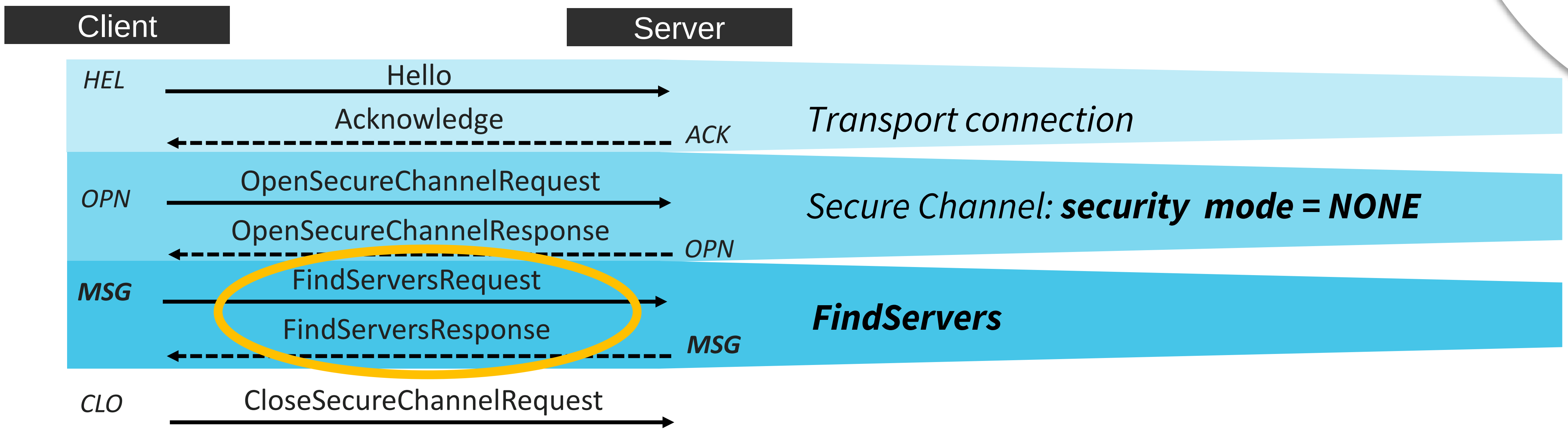


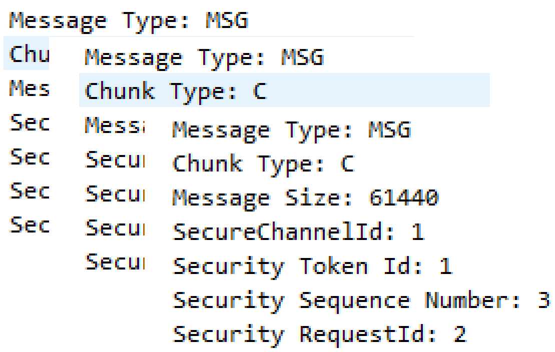
Nested Structures

- Chunks.

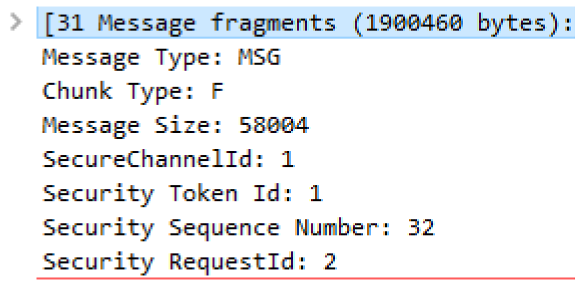


```
MaxMessageSize: 16777216

MaxMessageSize: 4194304
```

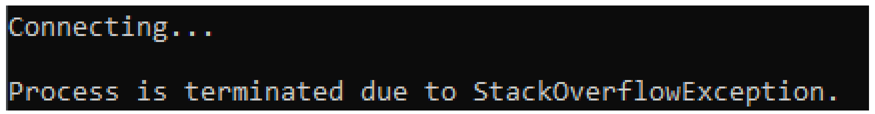




```
Message Type: MSG
Chu  Message Type: MSG
Mes  Chunk Type: C
Sec  Messi Message Type: MSG
Sec  Secui Chunk Type: C
Sec  Secui Message Size: 61440
Sec  Secui SecureChannelId: 1
     Secui Security Token Id: 1
           Security Sequence Number: 3
           Security RequestId: 2
```



```
> [31 Message fragments (1900460 bytes):
  Message Type: MSG
  Chunk Type: F
  Message Size: 58004
  SecureChannelId: 1
  Security Token Id: 1
  Security Sequence Number: 32
  Security RequestId: 2
```



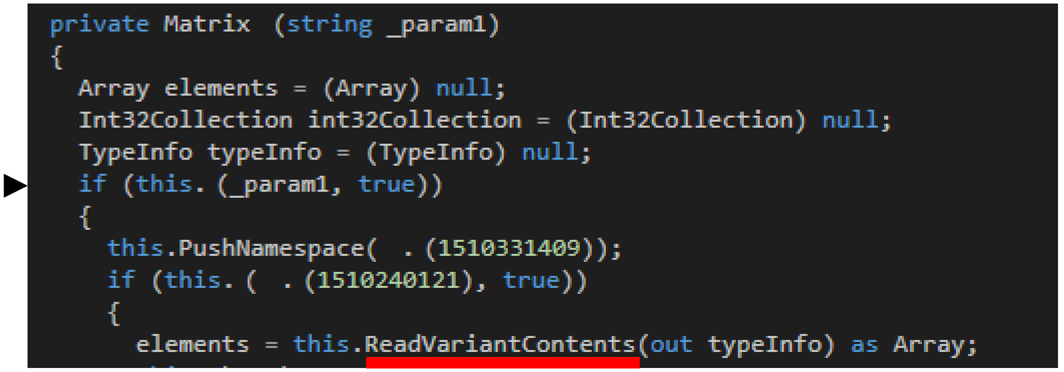
```
Connecting...

Process is terminated due to StackOverflowException.
```

.NET Stack Vulnerability

6 years old 0 day

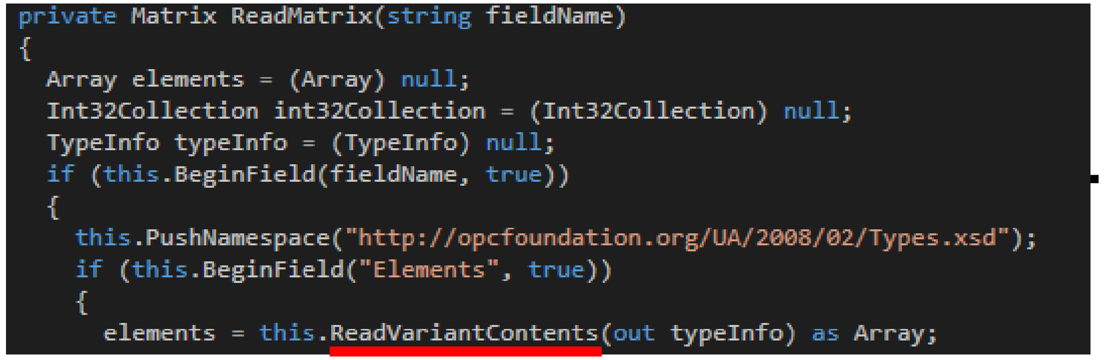
CVE-2021-27432

optimize! softing



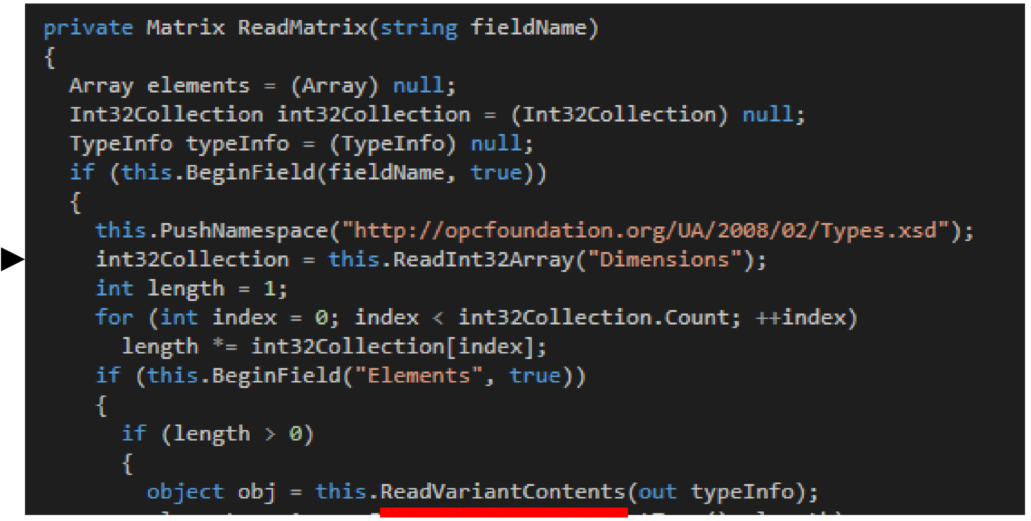
```
private Matrix  (string _param1)
{
  Array elements = (Array) null;
  Int32Collection int32Collection = (Int32Collection) null;
  TypeInfo typeInfo = (TypeInfo) null;
  if (this. (_param1, true))
  {
    this.PushNamespace(  . (1510331409));
    if (this. (  . (1510240121), true))
    {
      elements = this.ReadVariantContents(out typeInfo) as Array;
```

OPC FOUNDATION



```
private Matrix ReadMatrix(string fieldName)
{
  Array elements = (Array) null;
  Int32Collection int32Collection = (Int32Collection) null;
  TypeInfo typeInfo = (TypeInfo) null;
  if (this.BeginField(fieldName, true))
  {
    this.PushNamespace("http://opcfoundation.org/UA/2008/02/Types.xsd");
    if (this.BeginField("Elements", true))
    {
      elements = this.ReadVariantContents(out typeInfo) as Array;
```

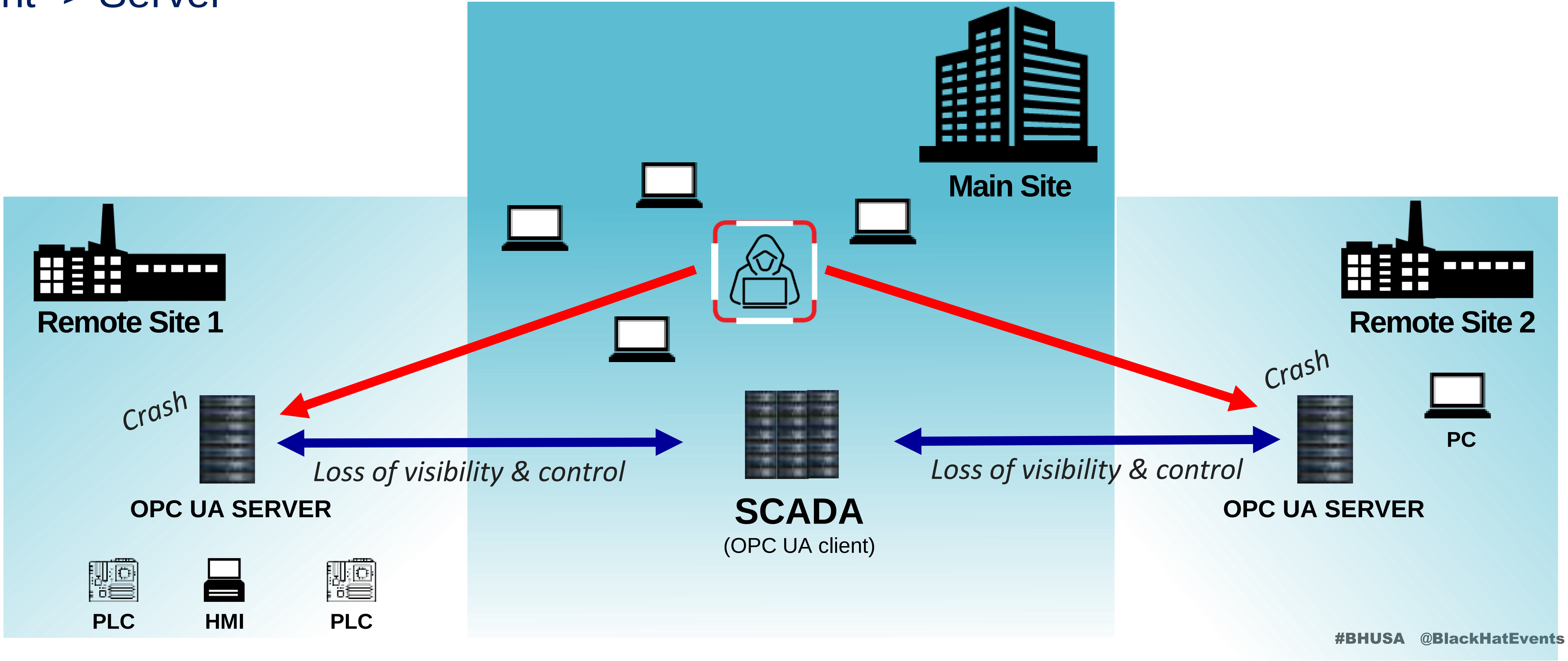
Unified Automation



```
private Matrix ReadMatrix(string fieldName)
{
  Array elements = (Array) null;
  Int32Collection int32Collection = (Int32Collection) null;
  TypeInfo typeInfo = (TypeInfo) null;
  if (this.BeginField(fieldName, true))
  {
    this.PushNamespace("http://opcfoundation.org/UA/2008/02/Types.xsd");
    int32Collection = this.ReadInt32Array("Dimensions");
    int length = 1;
    for (int index = 0; index < int32Collection.Count; ++index)
      length *= int32Collection[index];
    if (this.BeginField("Elements", true))
    {
      if (length > 0)
      {
        object obj = this.ReadVariantContents(out typeInfo);
```

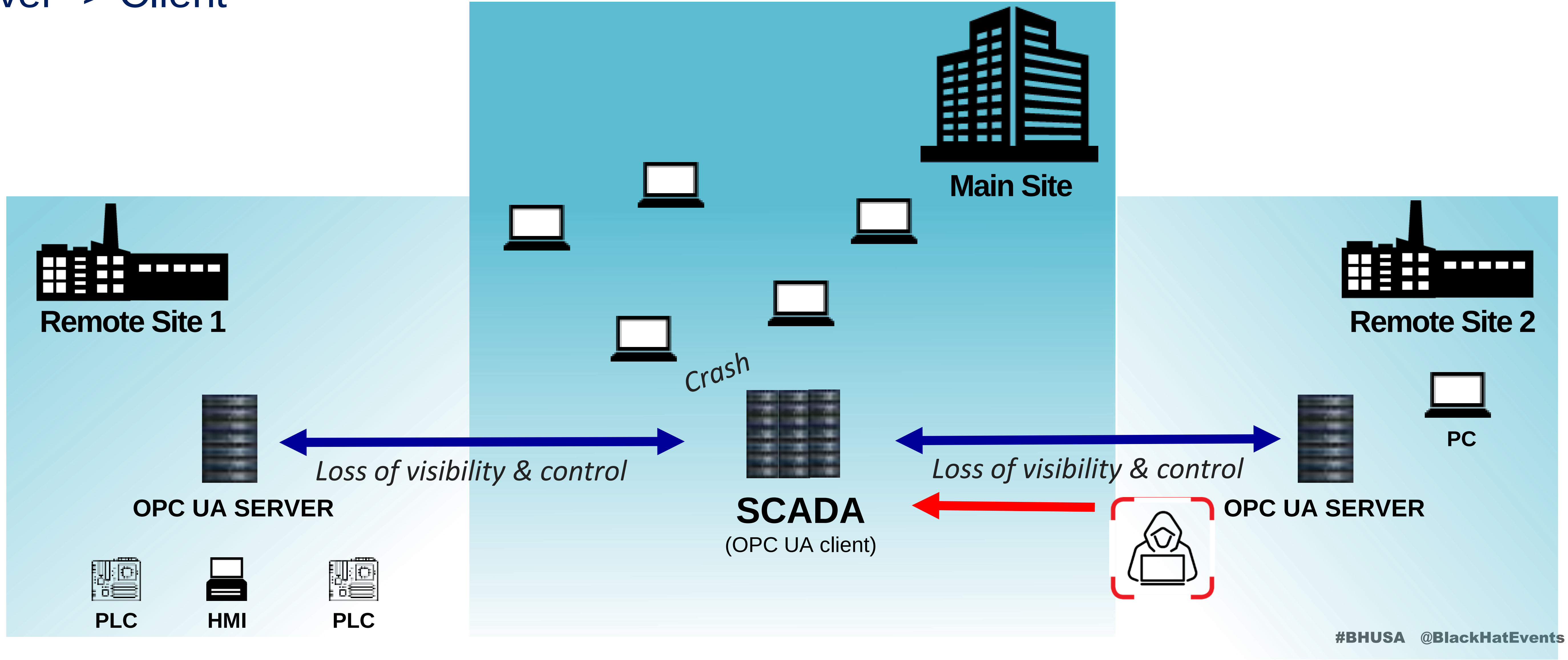
.NET Stack Vulnerability

Client -> Server



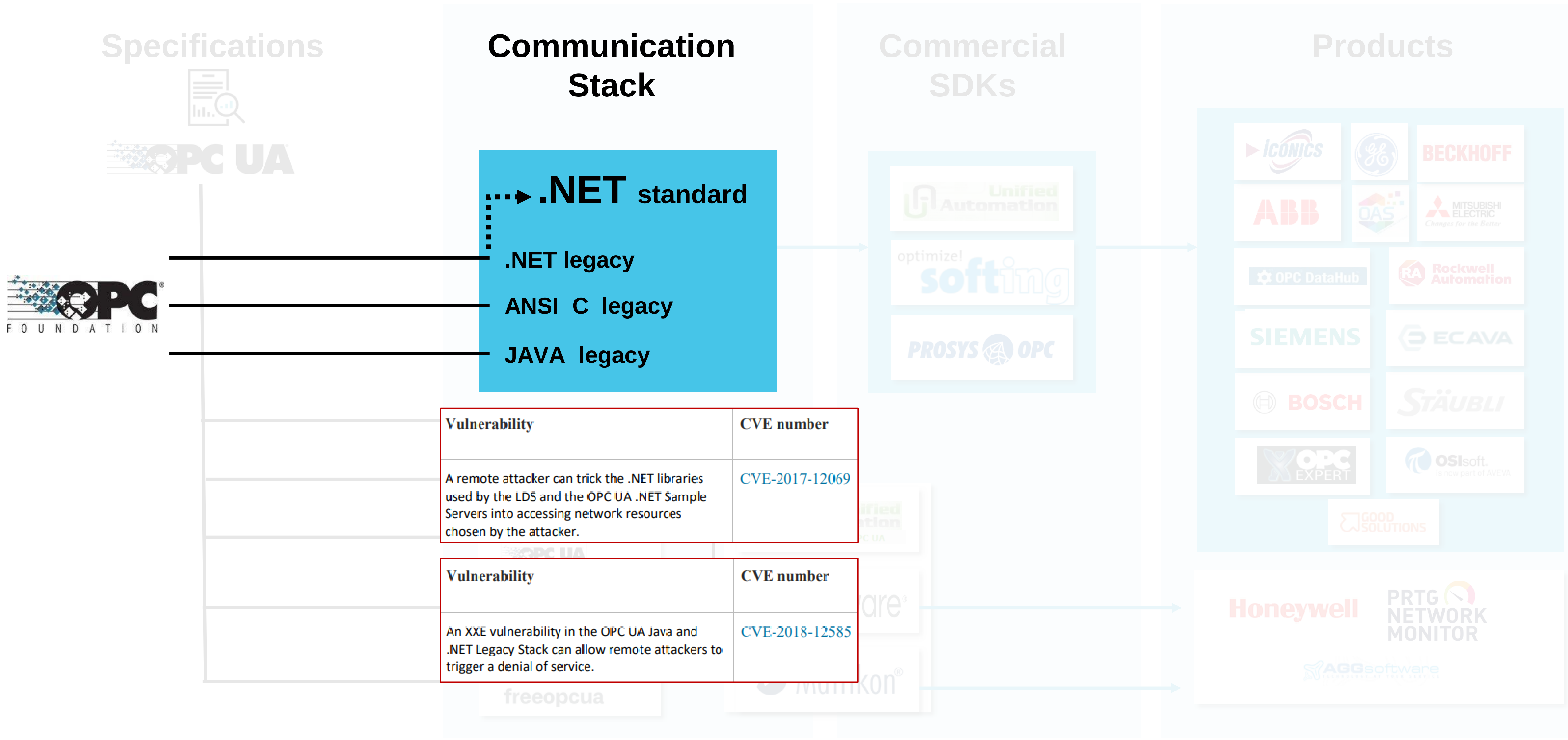
.NET Stack Vulnerability

Server -> Client



Unified Automation .NET SDK

<xml />



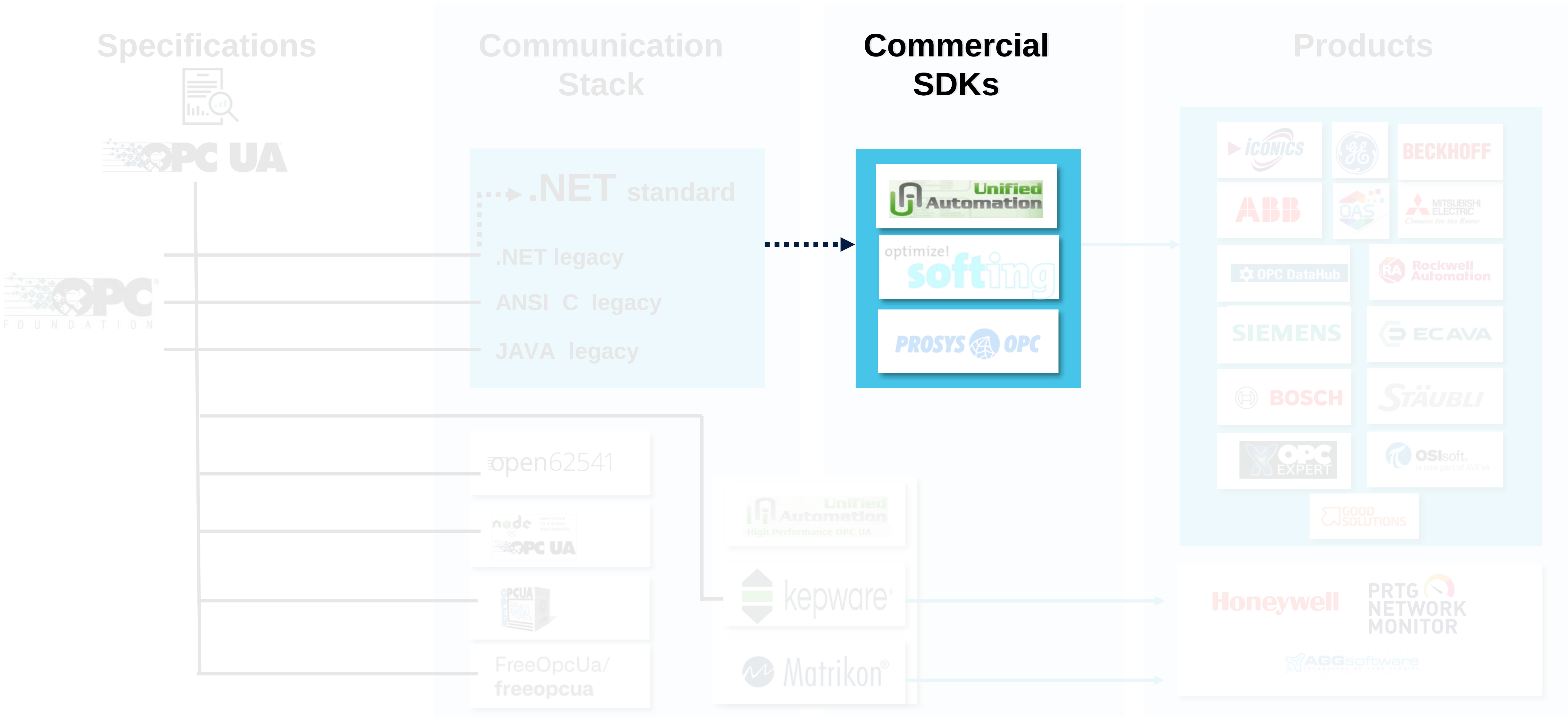
Vulnerability	CVE number
A remote attacker can trick the .NET libraries used by the LDS and the OPC UA .NET Sample Servers into accessing network resources chosen by the attacker.	CVE-2017-12069

Vulnerability	CVE number
An XXE vulnerability in the OPC UA Java and .NET Legacy Stack can allow remote attackers to trigger a denial of service.	CVE-2018-12585

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Unified Automation .NET SDK

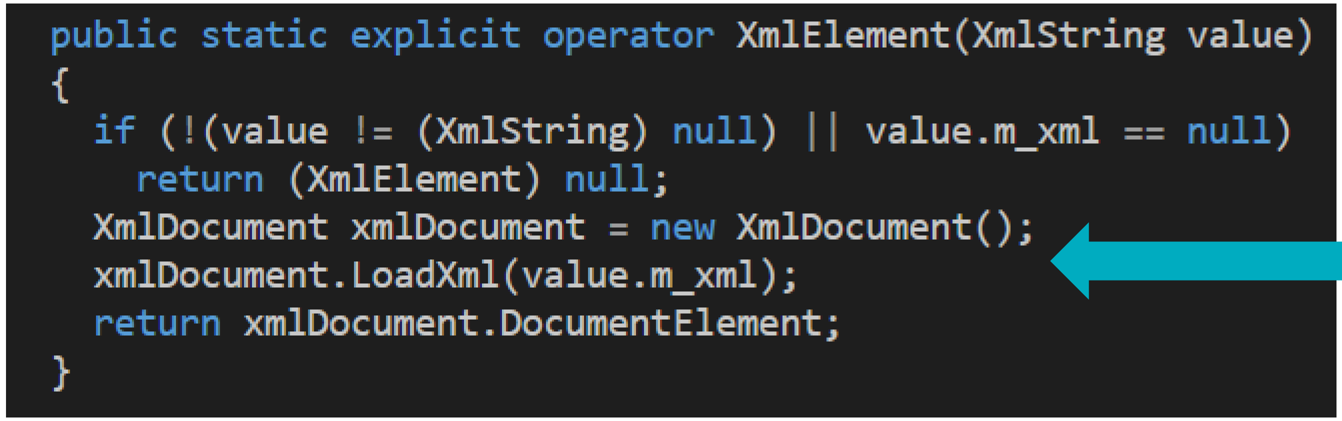
<xml />



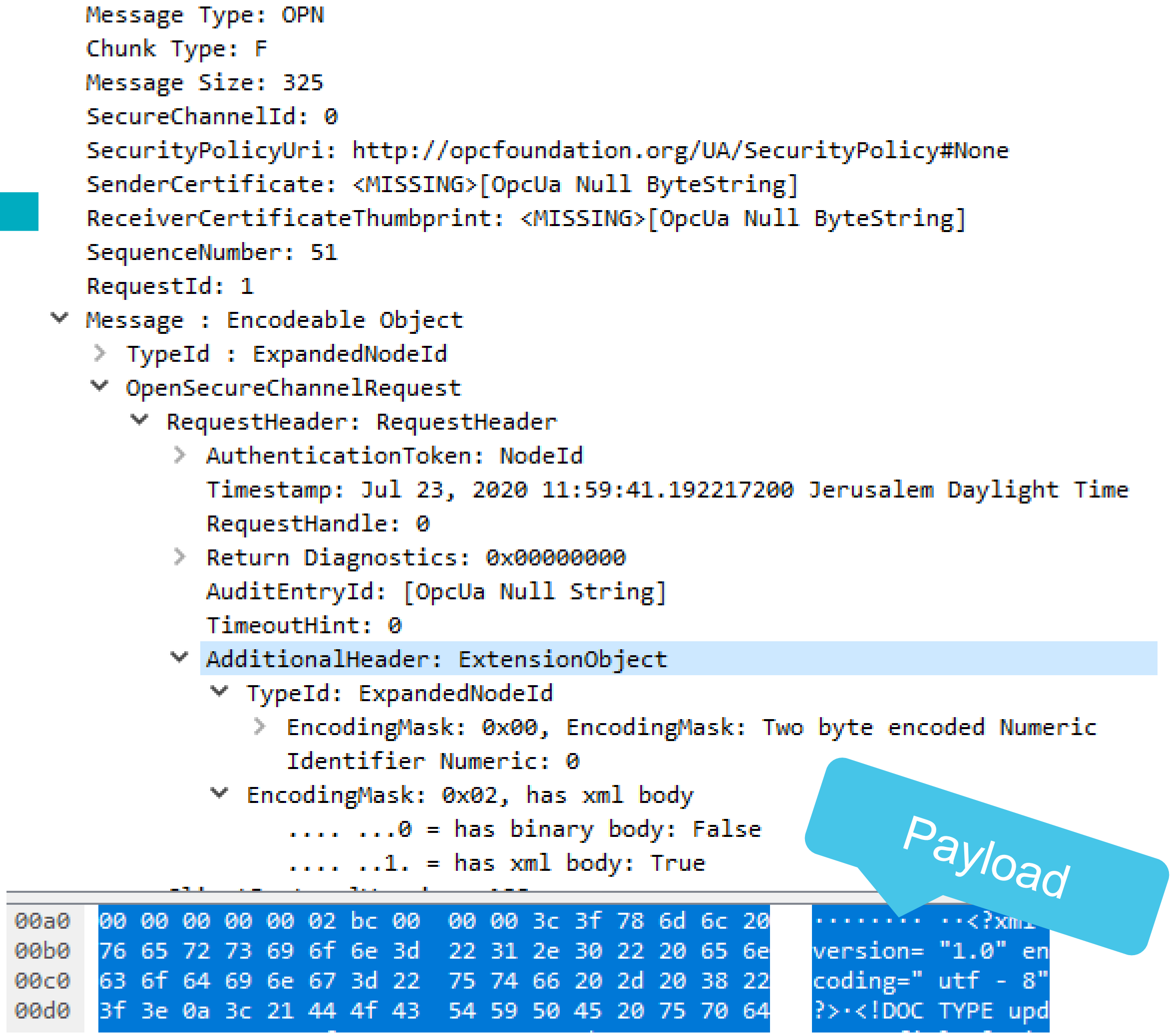
** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

XXE. Again.

CVE-2021-27434



```
public static explicit operator XmlElement(XmlString value)
{
  if (!(value != (XmlString) null) || value.m_xml == null)
    return (XmlElement) null;
  XmlDocument xmlDocument = new XmlDocument();
  xmlDocument.LoadXml(value.m_xml);
  return xmlDocument.DocumentElement;
}
```



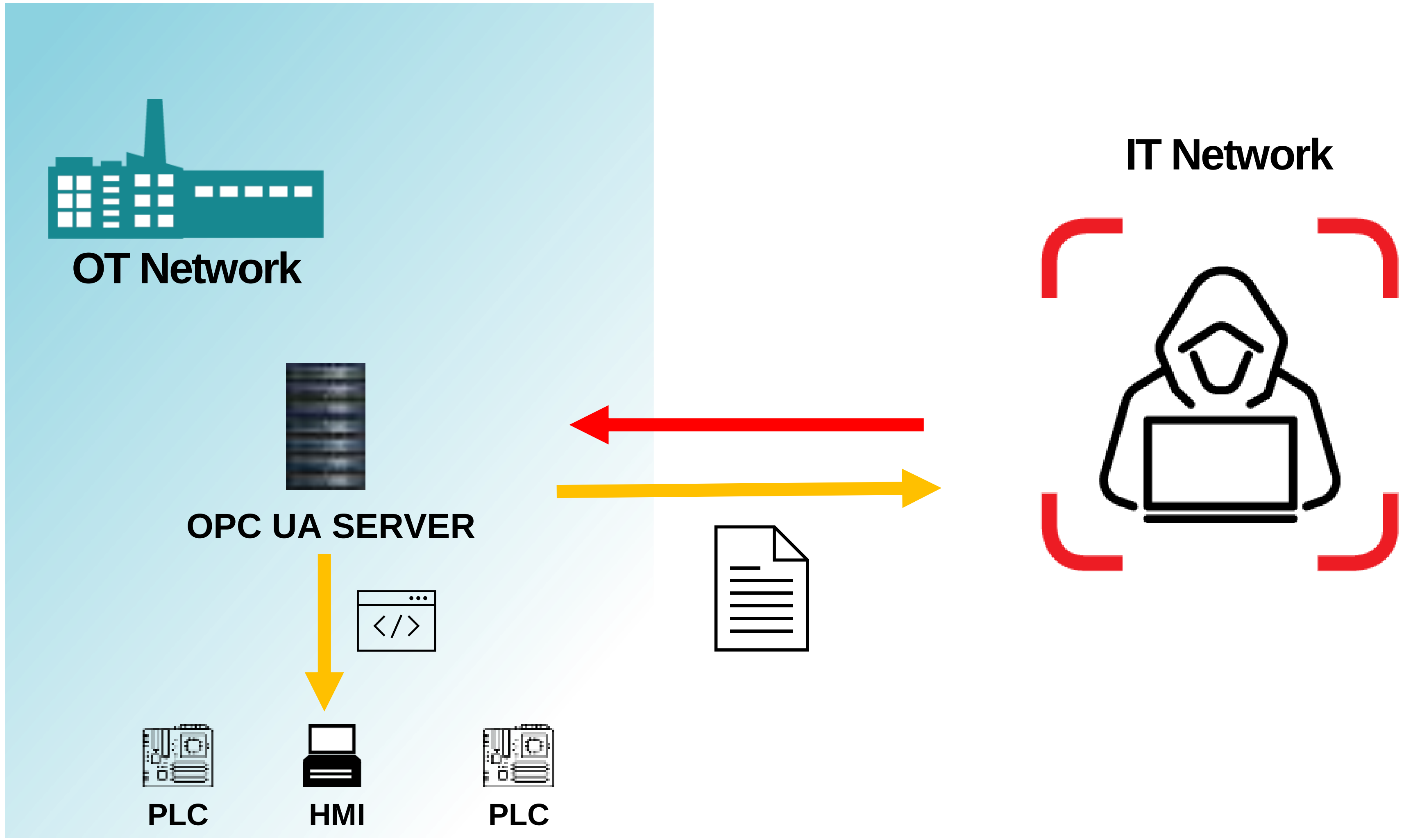
```
Message Type: OPN
Chunk Type: F
Message Size: 325
SecureChannelId: 0
SecurityPolicyUri: http://opcfoundation.org/UA/SecurityPolicy#None
SenderCertificate: <MISSING>[OpcUa Null ByteString]
ReceiverCertificateThumbprint: <MISSING>[OpcUa Null ByteString]
SequenceNumber: 51
RequestId: 1
Message : Encodeable Object
  TypeId : ExpandedNodeId
  OpenSecureChannelRequest
    RequestHeader: RequestHeader
      AuthenticationToken: NodeId
      Timestamp: Jul 23, 2020 11:59:41.192217200 Jerusalem Daylight Time
      RequestHandle: 0
      Return Diagnostics: 0x00000000
      AuditEntryId: [OpcUa Null String]
      TimeoutHint: 0
      AdditionalHeader: ExtensionObject
        TypeId: ExpandedNodeId
          EncodingMask: 0x00, EncodingMask: Two byte encoded Numeric
          Identifier Numeric: 0
        EncodingMask: 0x02, has xml body
          .... ...0 = has binary body: False
          .... ..1. = has xml body: True

00a0  00 00 00 00 00 02 bc 00  00 00 3c 3f 78 6d 6c 20   ········ ··<?xm
00b0  76 65 72 73 69 6f 6e 3d  22 31 2e 30 22 20 65 6e   version= "1.0" en
00c0  63 6f 64 69 6e 67 3d 22  75 74 66 20 2d 20 38 22   coding=" utf - 8"
00d0  3f 3e 0a 3c 21 44 4f 43  54 59 50 45 20 75 70 64   ?>·<!DOC TYPE upd
```

- Code refactoring reintroduced the vulnerability
- Exploitable over Extension Object decoding

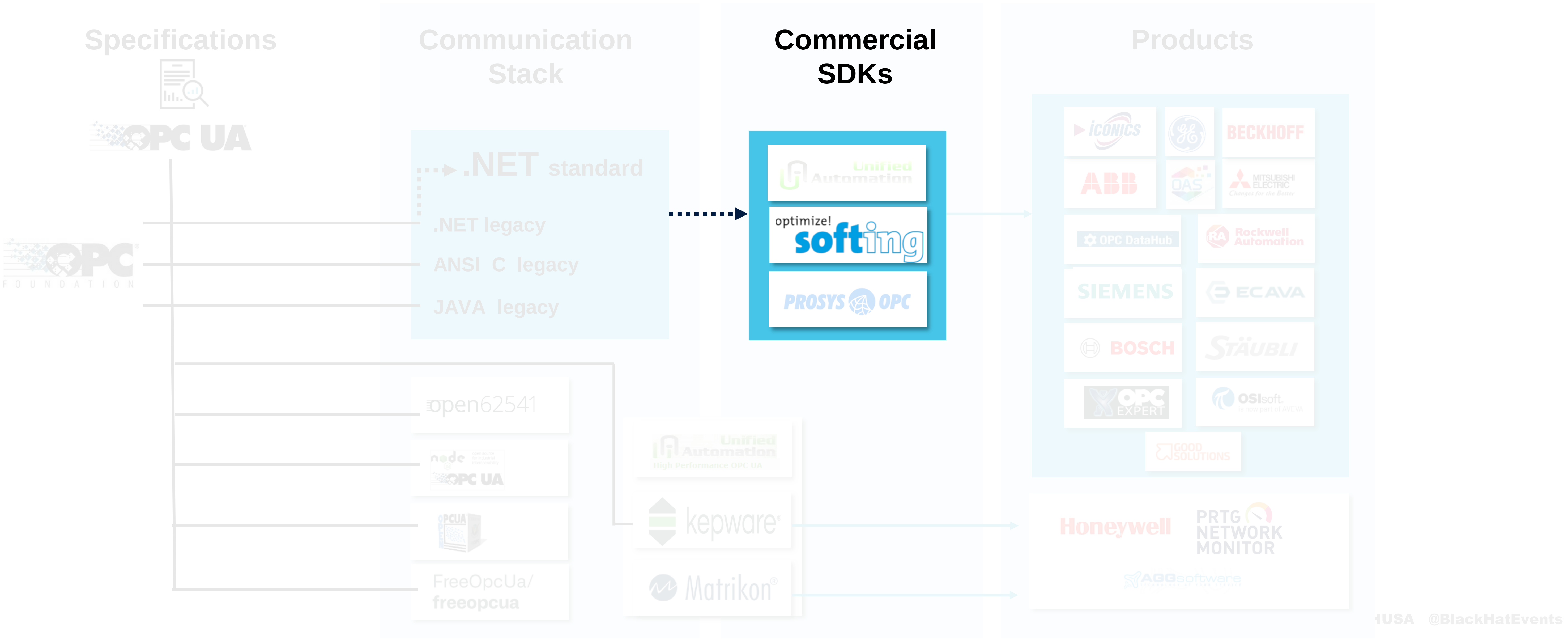
*XXE = XML External Entity

SDK XXE Vulnerability Impact

Client -> Server



Softing C++ OPC UA SDK



Specifications

Communication Stack

Commercial SDKs

Products

.NET standard

.NET legacy

ANSI C legacy

JAVA legacy

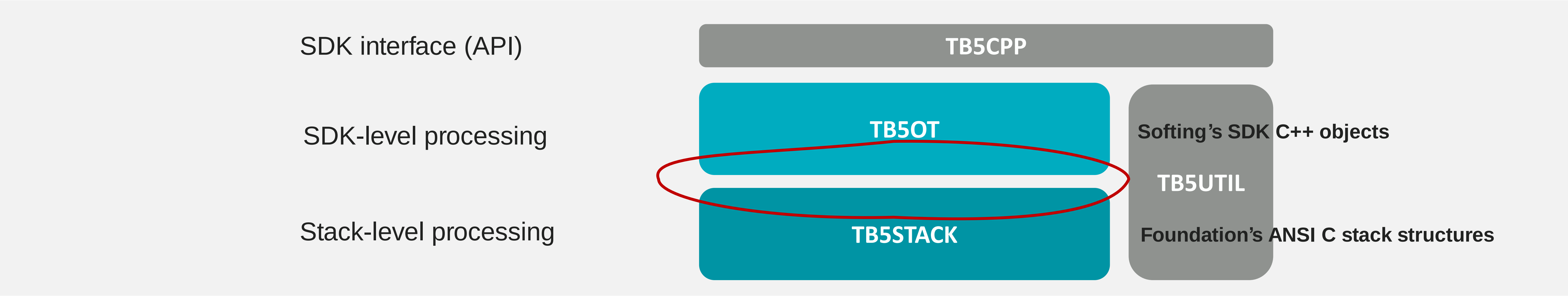
open62541

FreeOpcUa/ freeopcua

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Softing C++ OPC UA SDK

VxWorks



SDK interface (API)

SDK-level processing

Stack-level processing

TB5CPP

TB5OT

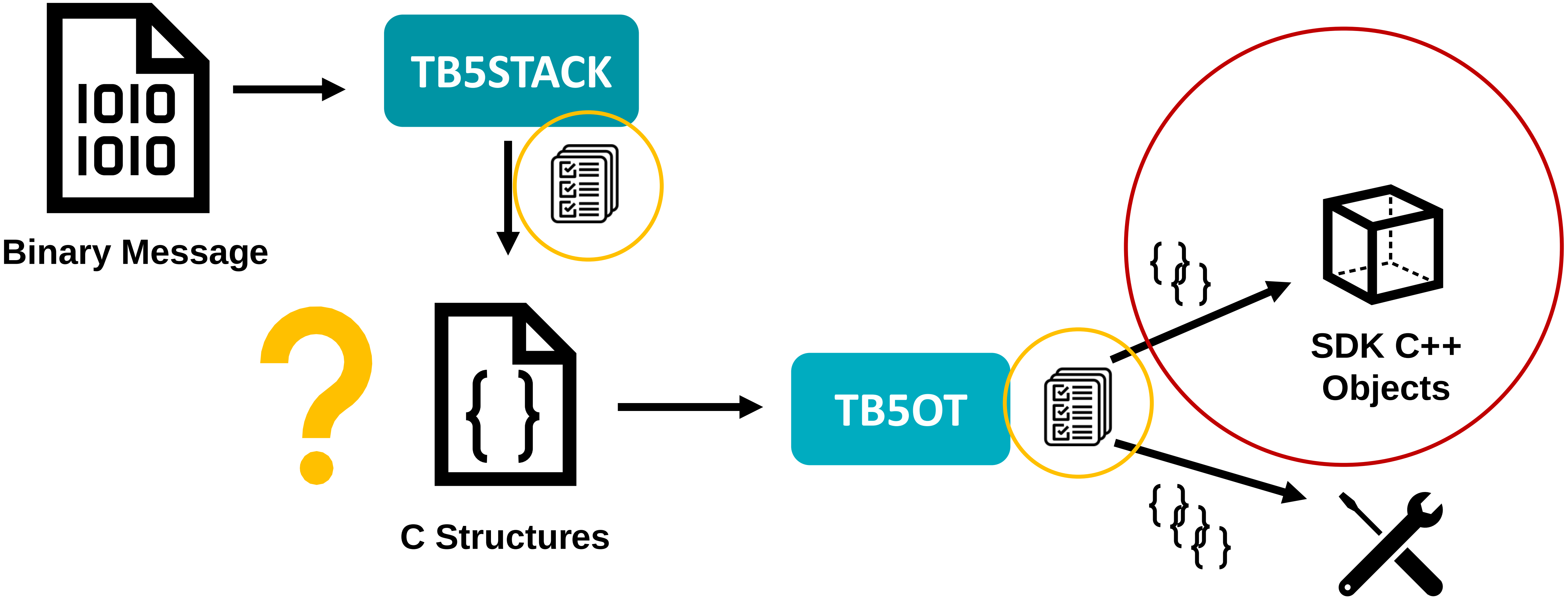
TB5STACK

TB5UTIL

Softing's SDK C++ objects

Foundation's ANSI C stack structures

From Binary to Objects

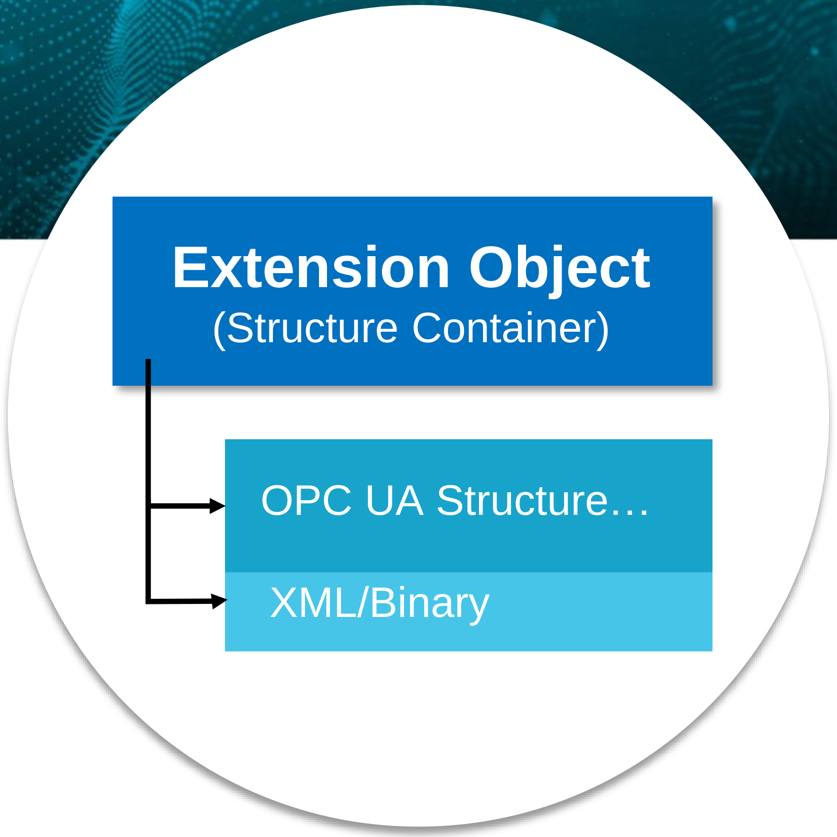


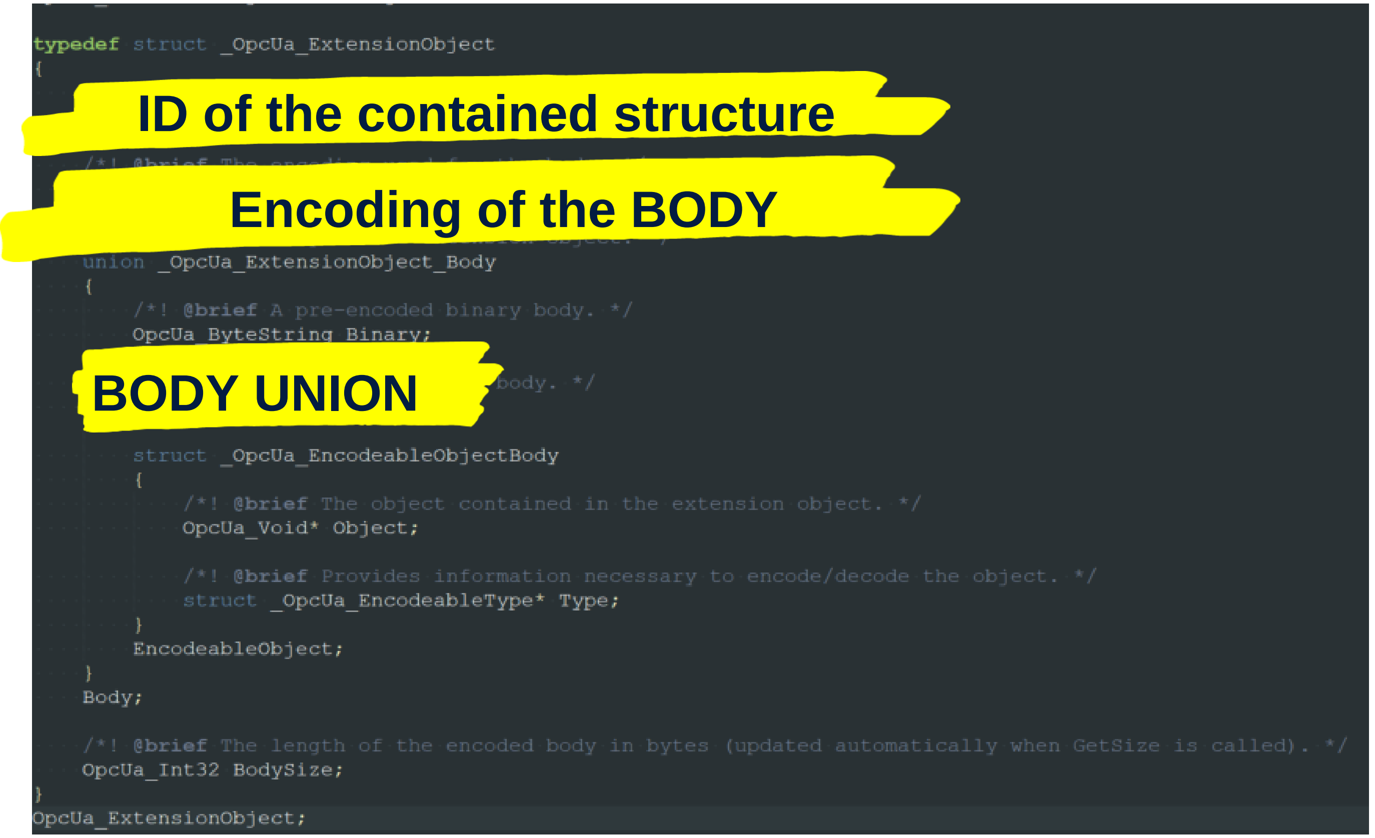
https://www.flaticon.com/free-icon/documents_160085

Foundation’s Extension Object

Looking at the Legacy ANCI C stack

decoded Extension Objects are stored in a specific structure

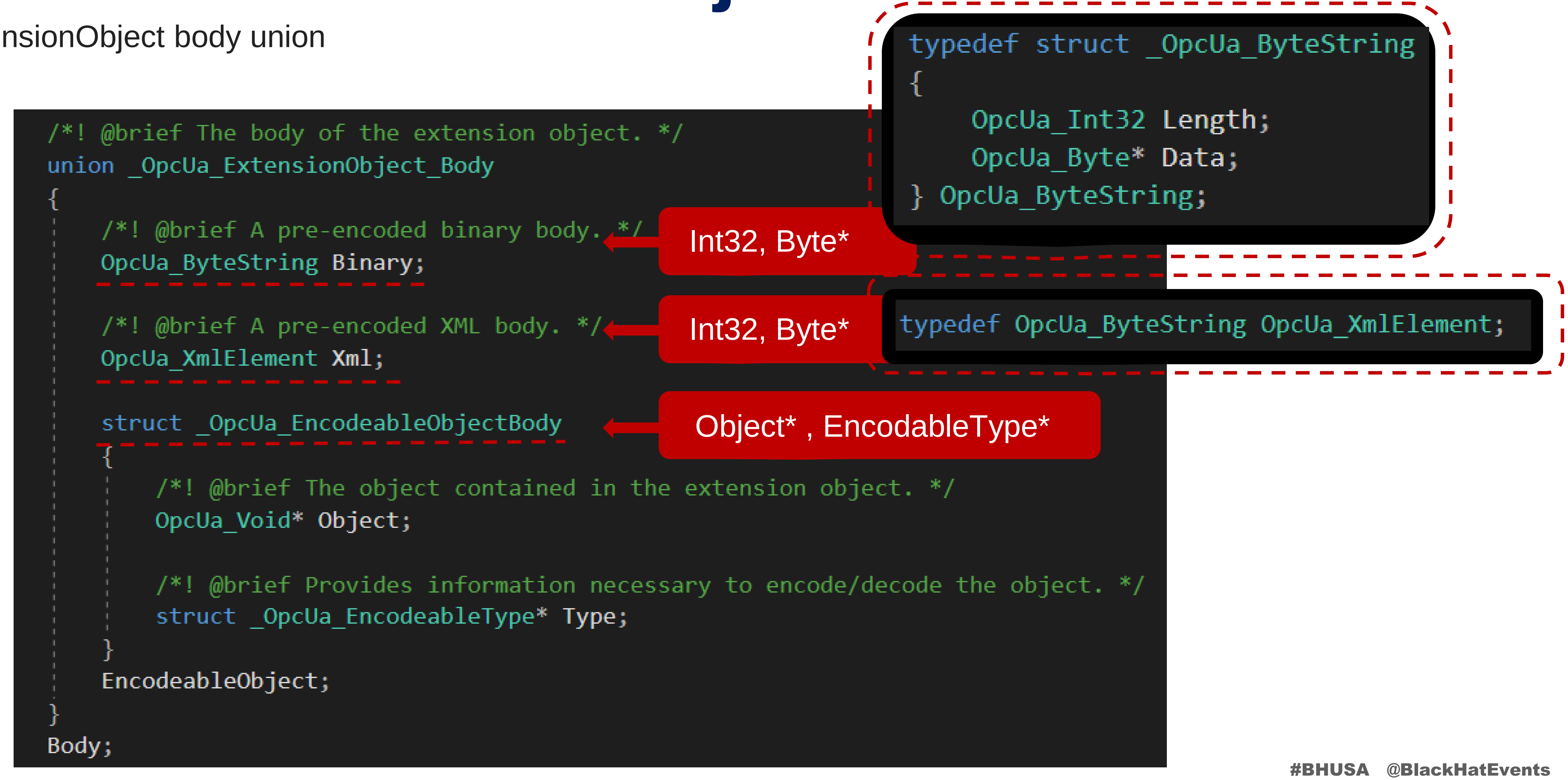




```
typedef struct _OpcUa_ExtensionObject
{
    union _OpcUa_ExtensionObject_Body
    {
        /*! @brief A pre-encoded binary body. */
        OpcUa_ByteString Binary;

                                  body. */

        struct _OpcUa_EncodeableObjectBody
        {
            /*! @brief The object contained in the extension object. */
            OpcUa_Void* Object;

            /*! @brief Provides information necessary to encode/decode the object. */
            struct _OpcUa_EncodeableType* Type;
        }
        EncodeableObject;
    }
    Body;

    /*! @brief The length of the encoded body in bytes (updated automatically when GetSize is called). */
    OpcUa_Int32 BodySize;
}
OpcUa_ExtensionObject;
```

Foundation’s ExtensionObject

Zooming into the ExtensionObject body union



```
/*! @brief The body of the extension object. */
union _OpcUa_ExtensionObject_Body
{
    /*! @brief A pre-encoded binary body. */
    OpcUa_ByteString Binary;

    /*! @brief A pre-encoded XML body. */
    OpcUa_XmlElement Xml;

    struct _OpcUa_EncodeableObjectBody
    {
        /*! @brief The object contained in the extension object. */
        OpcUa_Void* Object;

        /*! @brief Provides information necessary to encode/decode the object. */
        struct _OpcUa_EncodeableType* Type;
    }
    EncodeableObject;
}
Body;
```

Int32, Byte*

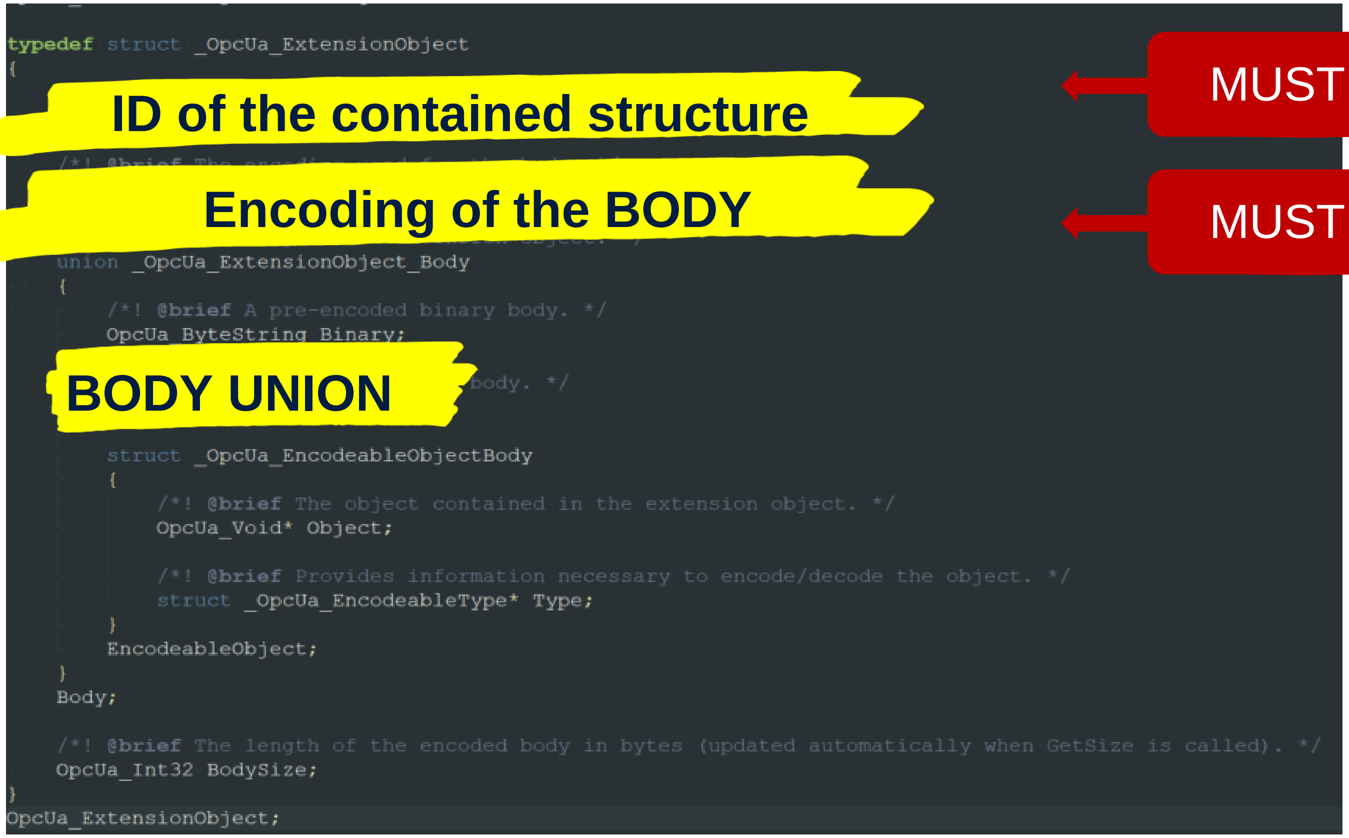
Int32, Byte*

Object* , EncodableType*

```
typedef struct _OpcUa_ByteString
{
    OpcUa_Int32 Length;
    OpcUa_Byte* Data;
} OpcUa_ByteString;
```

```
typedef OpcUa_ByteString OpcUa_XmlElement;
```

Foundation’s ExtensionObject



```
typedef struct _OpcUa_ExtensionObject
{
    union _OpcUa_ExtensionObject_Body
    {
        /*! @brief A pre-encoded binary body. */
        OpcUa_ByteString Binary;

                                body. */

        struct _OpcUa_EncodeableObjectBody
        {
            /*! @brief The object contained in the extension object. */
            OpcUa_Void* Object;

            /*! @brief Provides information necessary to encode/decode the object. */
            struct _OpcUa_EncodeableType* Type;
        }
        EncodeableObject;
    }
    Body;

    /*! @brief The length of the encoded body in bytes (updated automatically when GetSize is called). */
    OpcUa_Int32 BodySize;
}
OpcUa_ExtensionObject;
```

ID of the contained structure

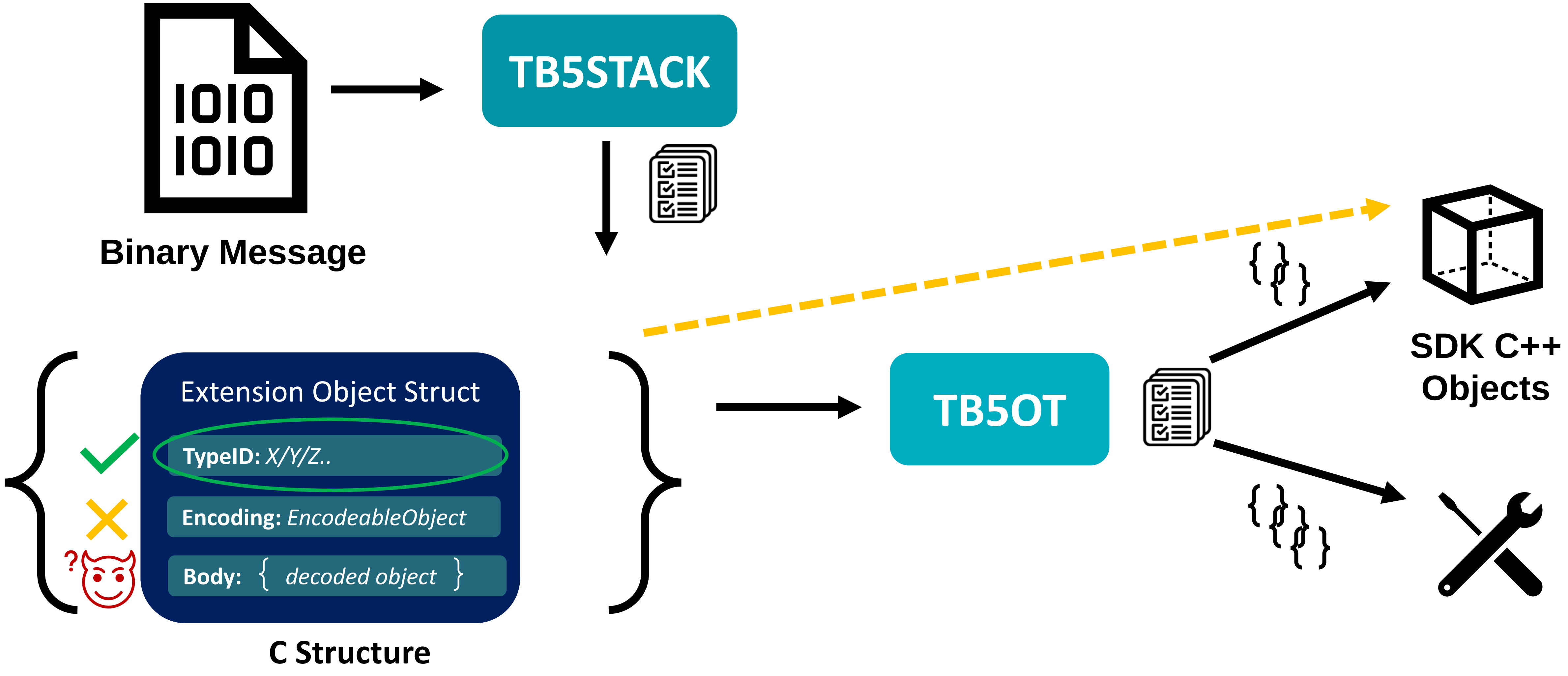
MUST be validated

Encoding of the BODY

MUST be validated

BODY UNION

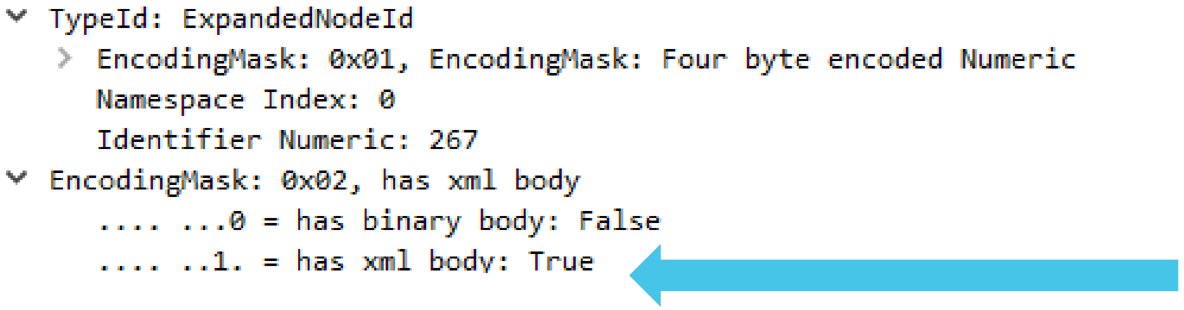
Setting C++ Objects



https://www.flaticon.com/free-icon/documents_160085

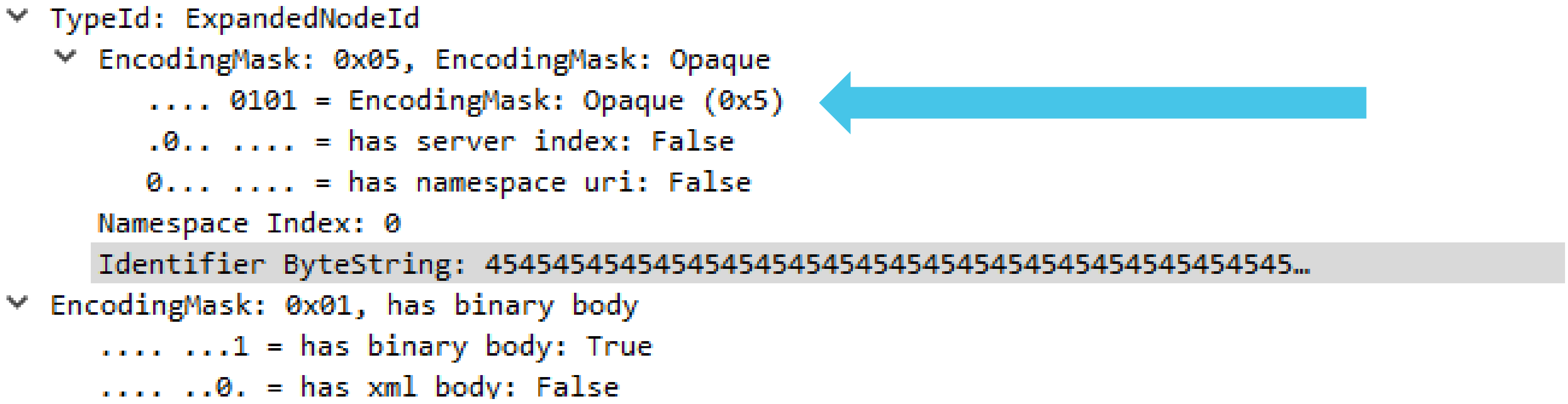
Skipping Internal Structure Decoding

1. XML..



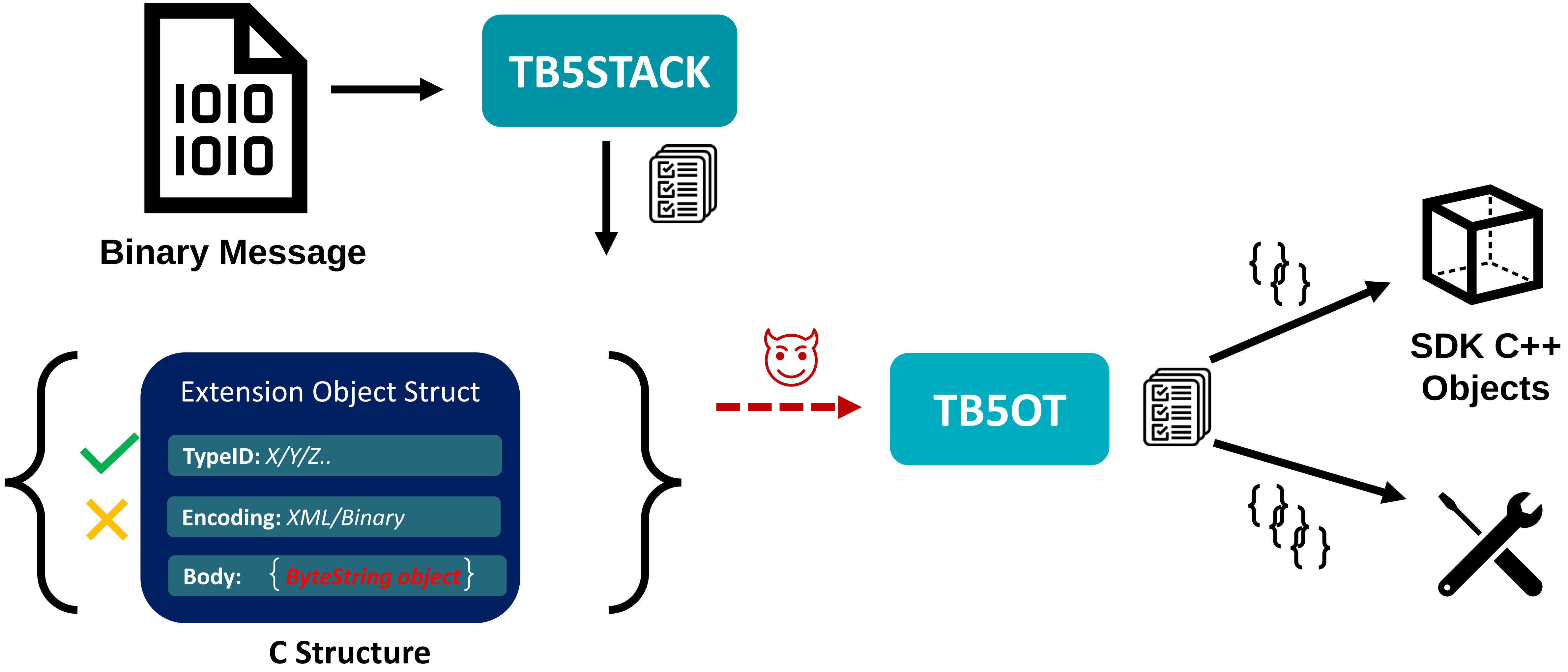
```
v TypeId: ExpandedNodeId
  > EncodingMask: 0x01, EncodingMask: Four byte encoded Numeric
    Namespace Index: 0
    Identifier Numeric: 267
v EncodingMask: 0x02, has xml body
    .... ...0 = has binary body: False
    .... ..1. = has xml body: True
```

2. Type-ID encoding



```
v TypeId: ExpandedNodeId
  v EncodingMask: 0x05, EncodingMask: Opaque
      .... 0101 = EncodingMask: Opaque (0x5)
      .0.. .... = has server index: False
      0... .... = has namespace uri: False
    Namespace Index: 0
    Identifier ByteString: 4545454545454545454545454545454545454545454545…
v EncodingMask: 0x01, has binary body
    .... ...1 = has binary body: True
    .... ..0. = has xml body: False
```

Setting C++ Objects



Binary Message

TB5STACK

Extension Object Struct

TypeID: *X/Y/Z..*

Encoding: *XML/Binary*

Body: { *ByteString object* }

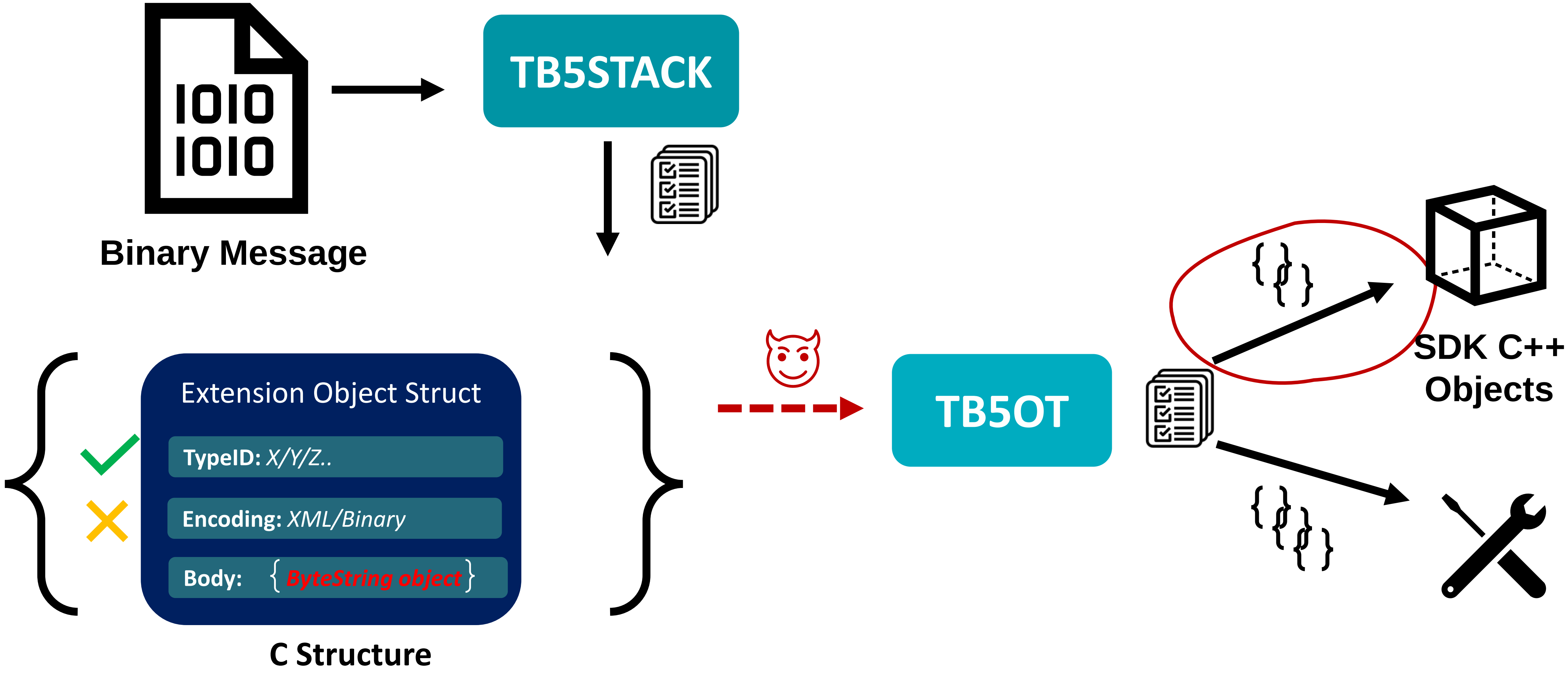
C Structure

TB5OT

SDK C++ Objects

https://www.flaticon.com/free-icon/documents_160085

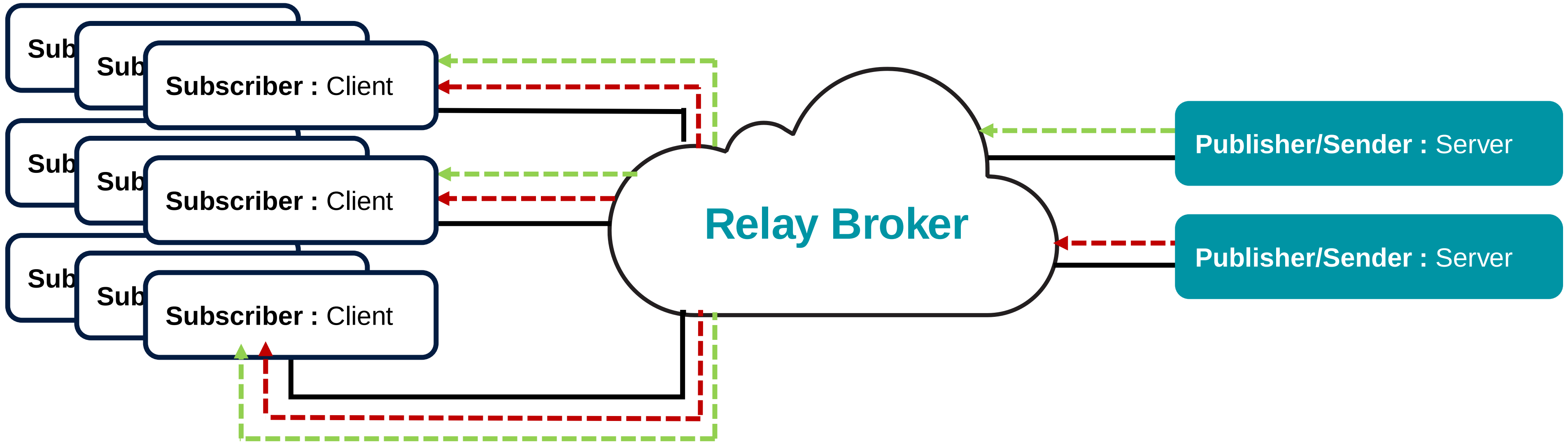
Setting C++ Objects



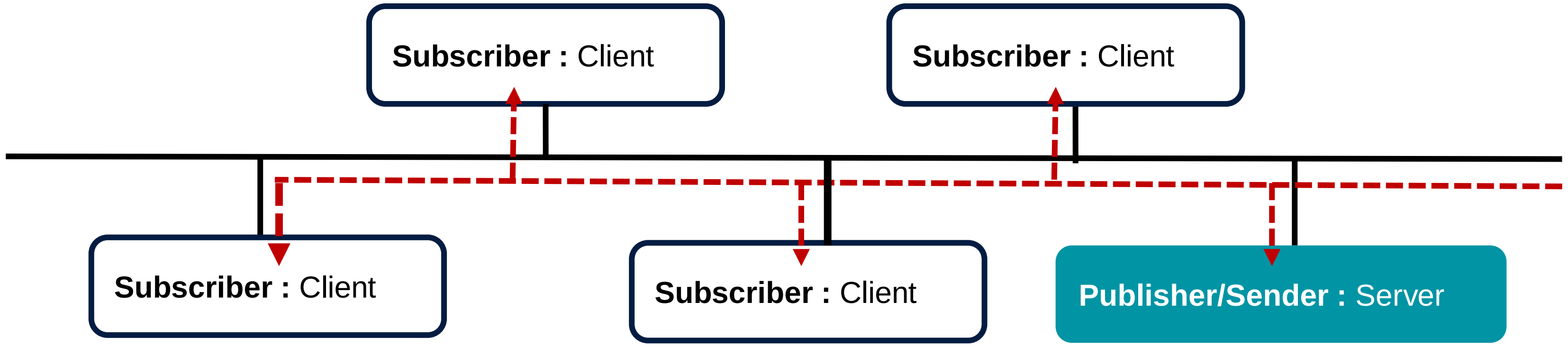
https://www.flaticon.com/free-icon/documents_160085

A word about PubSub

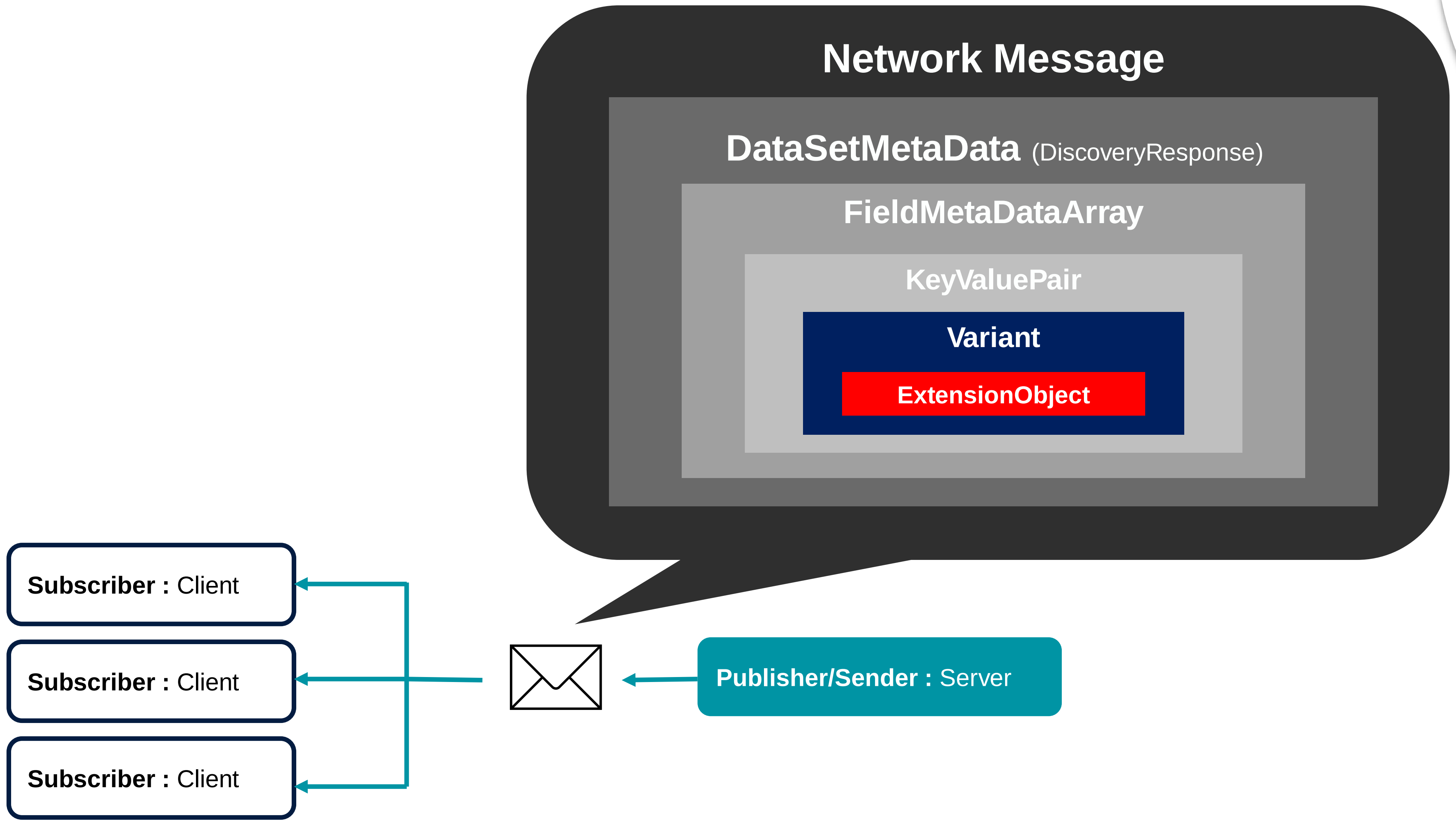
Option: Publish/Subscribe in the Cloud

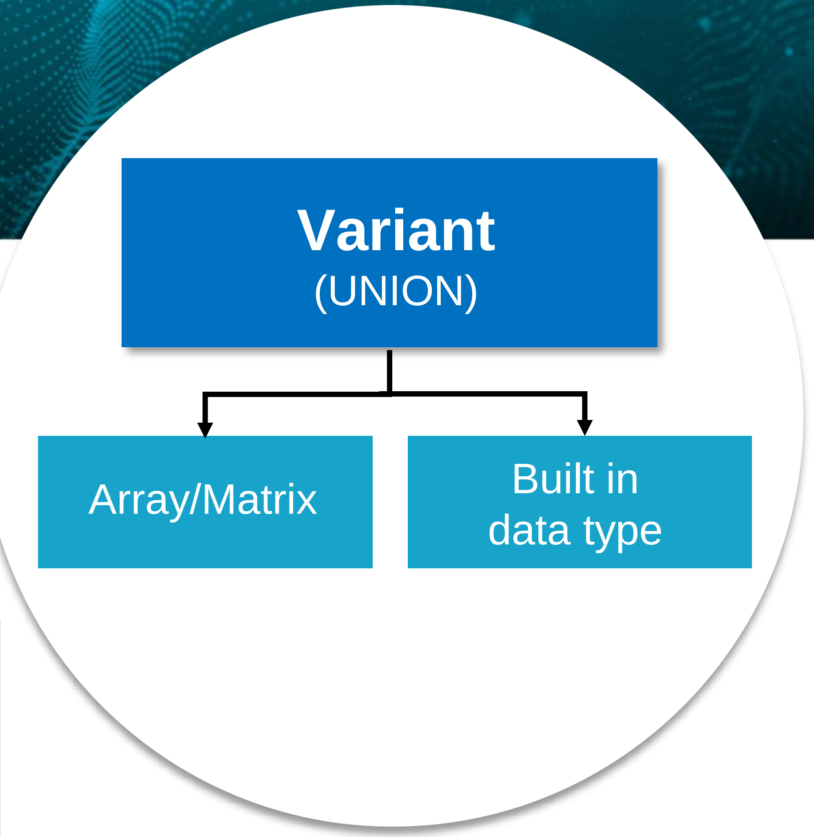


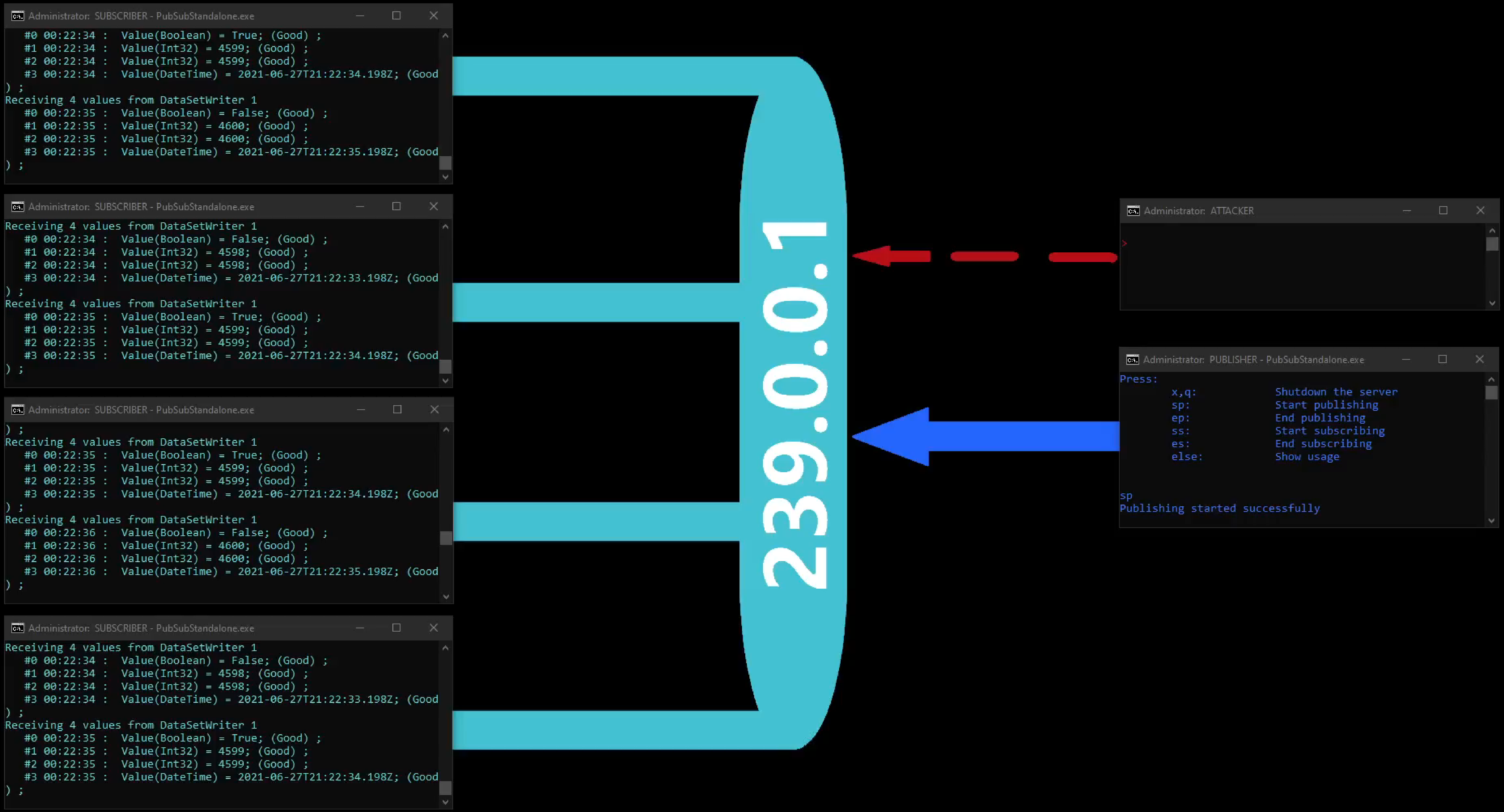
Option: Secure Multicast



Exploiting the Object Setters






Administrator: SUBSCRIBER - PubSubStandalone.exe
Administrator: SUBSCRIBER - PubSubStandalone.exe
Administrator: SUBSCRIBER - PubSubStandalone.exe
Administrator: SUBSCRIBER - PubSubStandalone.exe
239.0.0.1
Administrator: ATTACKER
Administrator: PUBLISHER - PubSubStandalone.exe

```
   #0 00:22:34 :  Value(Boolean) = True; (Good) ;
   #1 00:22:34 :  Value(Int32) = 4599; (Good) ;
   #2 00:22:34 :  Value(Int32) = 4599; (Good) ;
   #3 00:22:34 :  Value(DateTime) = 2021-06-27T21:22:34.198Z; (Good
) ;
Receiving 4 values from DataSetWriter 1
   #0 00:22:35 :  Value(Boolean) = False; (Good) ;
   #1 00:22:35 :  Value(Int32) = 4600; (Good) ;
   #2 00:22:35 :  Value(Int32) = 4600; (Good) ;
   #3 00:22:35 :  Value(DateTime) = 2021-06-27T21:22:35.198Z; (Good
) ;
```

```
Receiving 4 values from DataSetWriter 1
   #0 00:22:34 :  Value(Boolean) = False; (Good) ;
   #1 00:22:34 :  Value(Int32) = 4598; (Good) ;
   #2 00:22:34 :  Value(Int32) = 4598; (Good) ;
   #3 00:22:34 :  Value(DateTime) = 2021-06-27T21:22:33.198Z; (Good
) ;
Receiving 4 values from DataSetWriter 1
   #0 00:22:35 :  Value(Boolean) = True; (Good) ;
   #1 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #2 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #3 00:22:35 :  Value(DateTime) = 2021-06-27T21:22:34.198Z; (Good
) ;
```

```
) ;
Receiving 4 values from DataSetWriter 1
   #0 00:22:35 :  Value(Boolean) = True; (Good) ;
   #1 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #2 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #3 00:22:35 :  Value(DateTime) = 2021-06-27T21:22:34.198Z; (Good
) ;
Receiving 4 values from DataSetWriter 1
   #0 00:22:36 :  Value(Boolean) = False; (Good) ;
   #1 00:22:36 :  Value(Int32) = 4600; (Good) ;
   #2 00:22:36 :  Value(Int32) = 4600; (Good) ;
   #3 00:22:36 :  Value(DateTime) = 2021-06-27T21:22:35.198Z; (Good
) ;
```

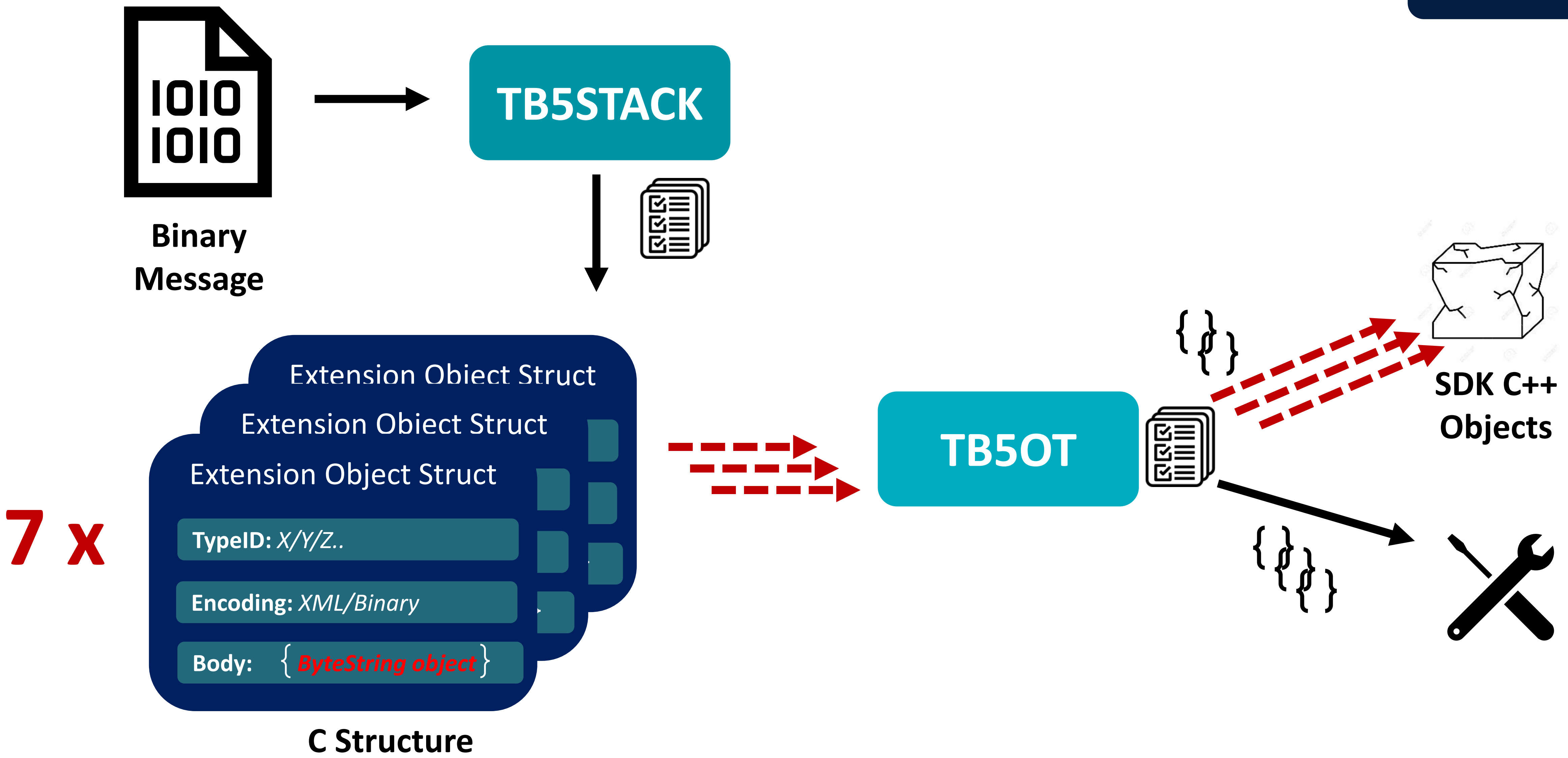
```
Receiving 4 values from DataSetWriter 1
   #0 00:22:34 :  Value(Boolean) = False; (Good) ;
   #1 00:22:34 :  Value(Int32) = 4598; (Good) ;
   #2 00:22:34 :  Value(Int32) = 4598; (Good) ;
   #3 00:22:34 :  Value(DateTime) = 2021-06-27T21:22:33.198Z; (Good
) ;
Receiving 4 values from DataSetWriter 1
   #0 00:22:35 :  Value(Boolean) = True; (Good) ;
   #1 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #2 00:22:35 :  Value(Int32) = 4599; (Good) ;
   #3 00:22:35 :  Value(DateTime) = 2021-06-27T21:22:34.198Z; (Good
) ;
```

```
>
```

```
Press:
        x,q:            Shutdown the server
        sp:             Start publishing
        ep:             End publishing
        ss:             Start subscribing
        es:             End subscribing
        else:           Show usage


sp
Publishing started successfully
```

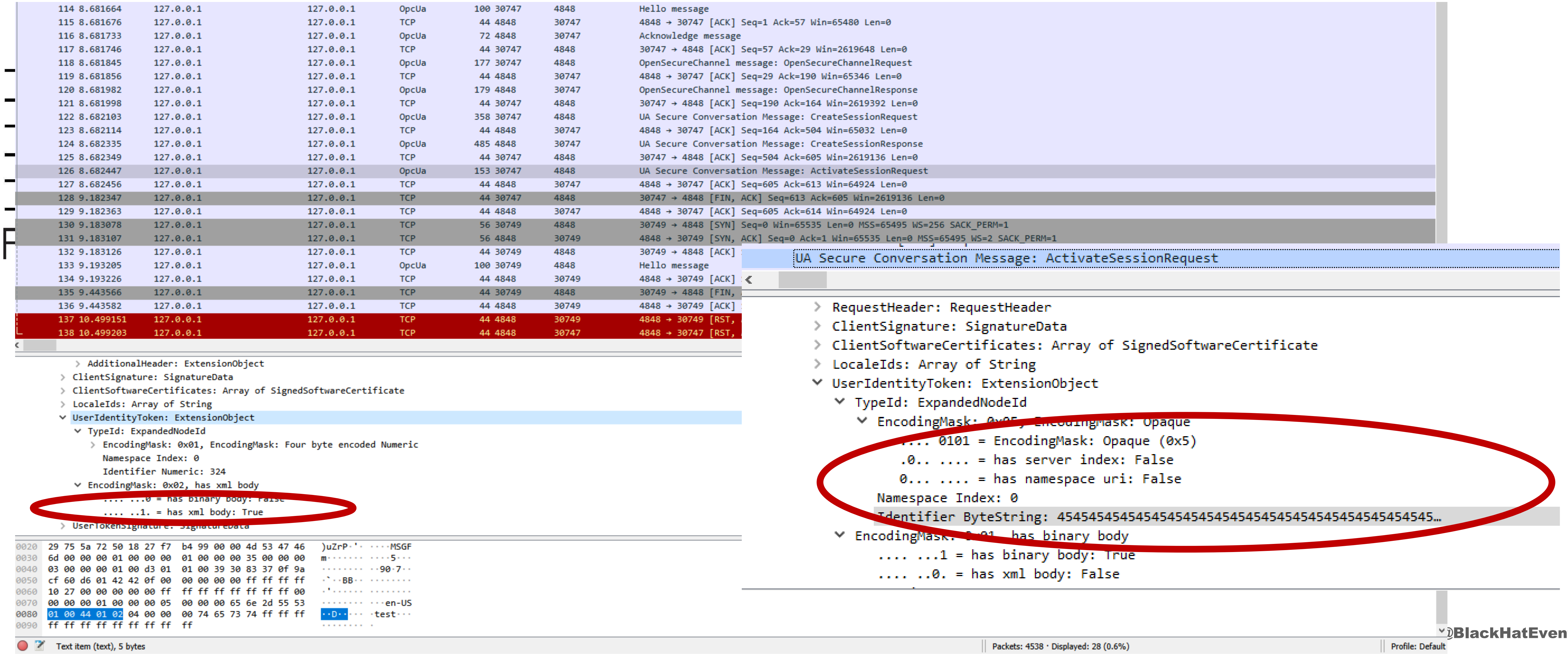
Setting C++ Objects

CVE-2021-32994



https://www.123rf.com/photo_141980838_stock-vector-crumpled-cube-box-icon-black-illustration-of-damage-breakage-pain-damnification-contour-isolated-vec.html

Not a one-time mistake…



```
114 8.681664   127.0.0.1   127.0.0.1   OpcUa  100 30747  4848   Hello message
115 8.681676   127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [ACK] Seq=1 Ack=57 Win=65480 Len=0
116 8.681733   127.0.0.1   127.0.0.1   OpcUa   72 4848   30747  Acknowledge message
117 8.681746   127.0.0.1   127.0.0.1   TCP     44 30747  4848   30747 → 4848 [ACK] Seq=57 Ack=29 Win=2619648 Len=0
118 8.681845   127.0.0.1   127.0.0.1   OpcUa  177 30747  4848   OpenSecureChannel message: OpenSecureChannelRequest
119 8.681856   127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [ACK] Seq=29 Ack=190 Win=65346 Len=0
120 8.681982   127.0.0.1   127.0.0.1   OpcUa  179 4848   30747  OpenSecureChannel message: OpenSecureChannelResponse
121 8.681998   127.0.0.1   127.0.0.1   TCP     44 30747  4848   30747 → 4848 [ACK] Seq=190 Ack=164 Win=2619392 Len=0
122 8.682103   127.0.0.1   127.0.0.1   OpcUa  358 30747  4848   UA Secure Conversation Message: CreateSessionRequest
123 8.682114   127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [ACK] Seq=164 Ack=504 Win=65032 Len=0
124 8.682335   127.0.0.1   127.0.0.1   OpcUa  485 4848   30747  UA Secure Conversation Message: CreateSessionResponse
125 8.682349   127.0.0.1   127.0.0.1   TCP     44 30747  4848   30747 → 4848 [ACK] Seq=504 Ack=605 Win=2619136 Len=0
126 8.682447   127.0.0.1   127.0.0.1   OpcUa  153 30747  4848   UA Secure Conversation Message: ActivateSessionRequest
127 8.682456   127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [ACK] Seq=605 Ack=613 Win=64924 Len=0
128 9.182347   127.0.0.1   127.0.0.1   TCP     44 30747  4848   30747 → 4848 [FIN, ACK] Seq=613 Ack=605 Win=2619136 Len=0
129 9.182363   127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [ACK] Seq=605 Ack=614 Win=64924 Len=0
130 9.183078   127.0.0.1   127.0.0.1   TCP     56 30749  4848   30749 → 4848 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
131 9.183107   127.0.0.1   127.0.0.1   TCP     56 4848   30749  4848 → 30749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=2 SACK_PERM=1
132 9.183126   127.0.0.1   127.0.0.1   TCP     44 30749  4848   30749 → 4848 [ACK]
133 9.193205   127.0.0.1   127.0.0.1   OpcUa  100 30749  4848   Hello message
134 9.193226   127.0.0.1   127.0.0.1   TCP     44 4848   30749  4848 → 30749 [ACK]
135 9.443566   127.0.0.1   127.0.0.1   TCP     44 30749  4848   30749 → 4848 [FIN,
136 9.443582   127.0.0.1   127.0.0.1   TCP     44 4848   30749  4848 → 30749 [ACK]
137 10.499151  127.0.0.1   127.0.0.1   TCP     44 4848   30749  4848 → 30749 [RST,
138 10.499203  127.0.0.1   127.0.0.1   TCP     44 4848   30747  4848 → 30747 [RST,
```

```
    > AdditionalHeader: ExtensionObject
  > ClientSignature: SignatureData
  > ClientSoftwareCertificates: Array of SignedSoftwareCertificate
  > LocaleIds: Array of String
  v UserIdentityToken: ExtensionObject
    v TypeId: ExpandedNodeId
      > EncodingMask: 0x01, EncodingMask: Four byte encoded Numeric
        Namespace Index: 0
        Identifier Numeric: 324
    v EncodingMask: 0x02, has xml body
        .... ...0 = has binary body: False
        .... ..1. = has xml body: True
  > UserTokenSignature: SignatureData
```

```
0020  29 75 5a 72 50 18 27 f7  b4 99 00 00 4d 53 47 46   )uZrP·'· ····MSGF
0030  6d 00 00 00 01 00 00 00  01 00 00 00 35 00 00 00   m······· ····5···
0040  03 00 00 00 01 00 d3 01  01 00 39 30 83 37 0f 9a   ········ ··90·7··
0050  cf 60 d6 01 42 42 0f 00  00 00 00 00 ff ff ff ff   ·`··BB·· ········
0060  10 27 00 00 00 00 00 ff  ff ff ff ff ff ff ff 00   ·'······ ········
0070  00 00 00 01 00 00 00 05  00 00 00 65 6e 2d 55 53   ········ ···en-US
0080  01 00 44 01 02 04 00 00  00 74 65 73 74 ff ff ff   ··D····· ·test···
0090  ff ff ff ff ff ff ff ff  ff                        ········ ·
```

Text item (text), 5 bytes

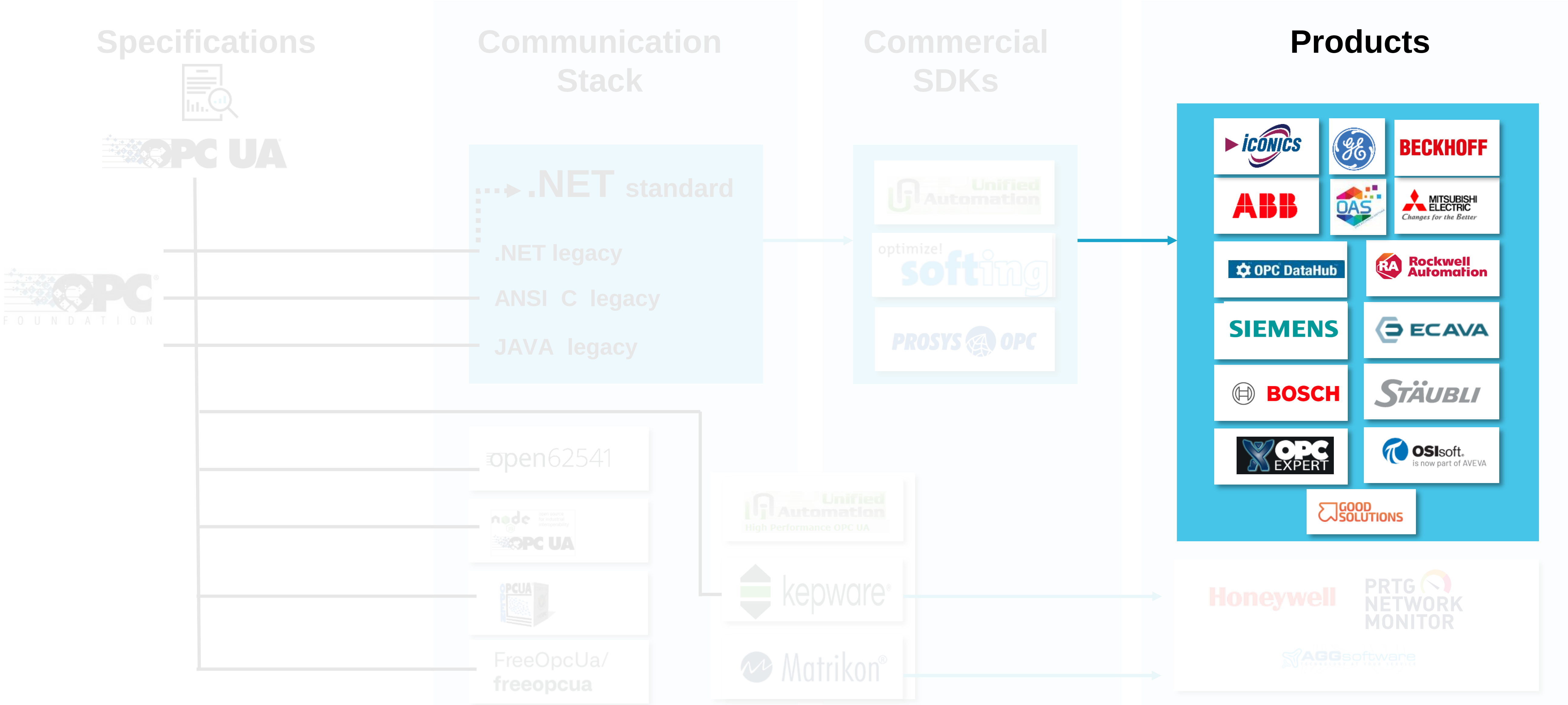
Packets: 4538 · Displayed: 28 (0.6%)

Profile: Default

UA Secure Conversation Message: ActivateSessionRequest

```
> RequestHeader: RequestHeader
> ClientSignature: SignatureData
> ClientSoftwareCertificates: Array of SignedSoftwareCertificate
> LocaleIds: Array of String
v UserIdentityToken: ExtensionObject
  v TypeId: ExpandedNodeId
    v EncodingMask: 0x05, EncodingMask: Opaque
        .... 0101 = EncodingMask: Opaque (0x5)
        .0.. .... = has server index: False
        0... .... = has namespace uri: False
      Namespace Index: 0
      Identifier ByteString: 4545454545454545454545454545454545454545454545…
  v EncodingMask: 0x01, has binary body
      .... ...1 = has binary body: True
      .... ..0. = has xml body: False
```

Products



Specifications

Communication Stack

Commercial SDKs

Products

.NET standard

.NET legacy

ANSI C legacy

JAVA legacy

open62541

FreeOpcUa/ freeopcua

** This mapping is based on our best effort & knowledge; some vendors or relations may be missing or inaccurate **

Products

Configurations

Integration
with OPC UA SDK/stack

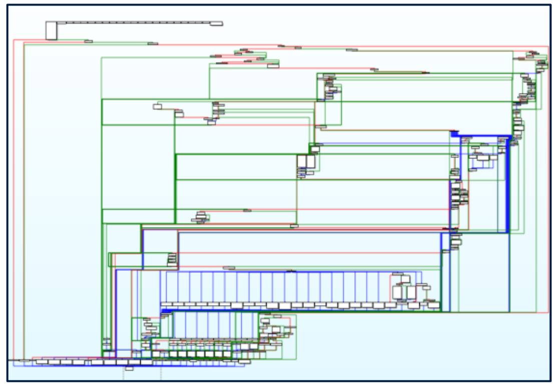
SDK Integration

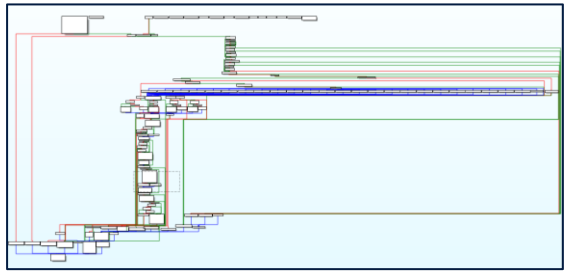
Required Interfaces

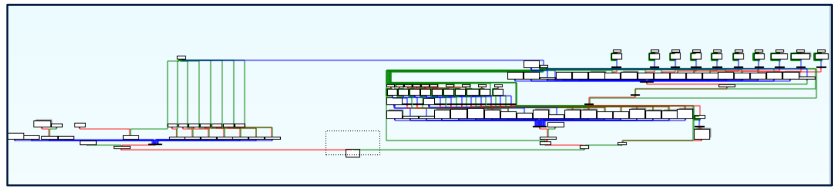
ServerConfig, NodeManager, **IOManager**

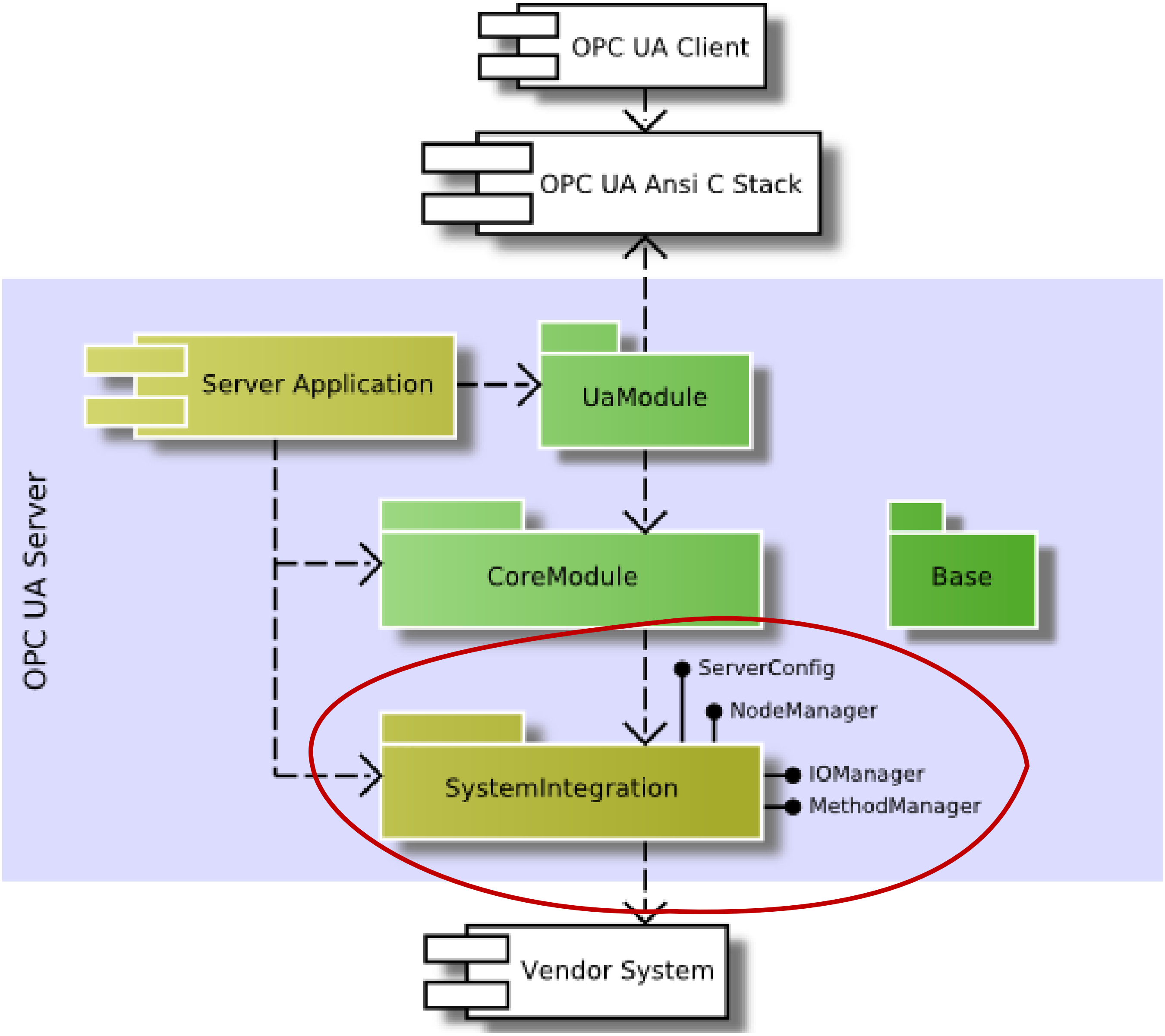
Optional Interfaces

MethodManager, EventManager, HistoryManager









http://documentation.unified-automation.com/uasdkcpp/1.4.2/html/L1ServerSdkIntroduction.html

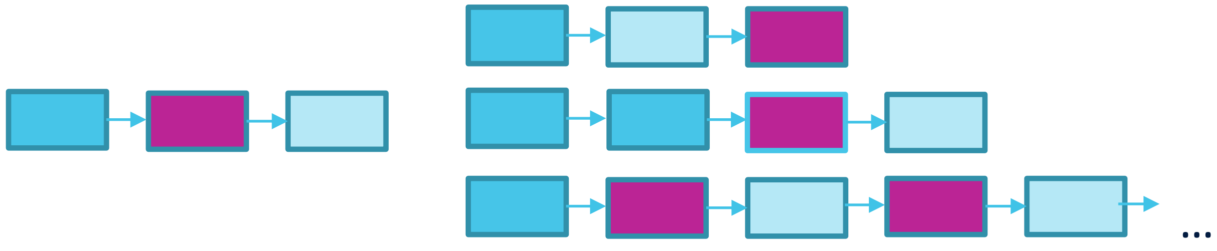
Fuzzing Products

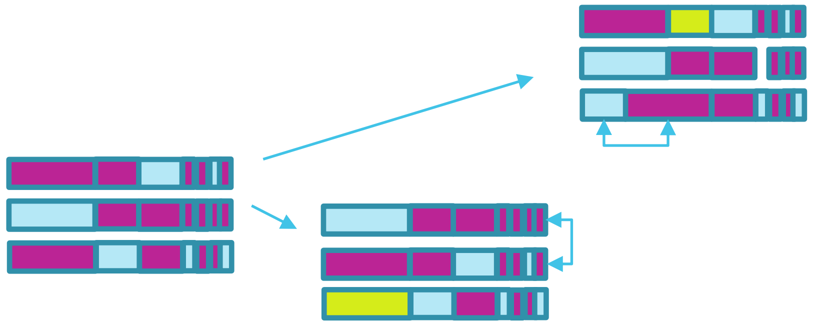
IOManager:

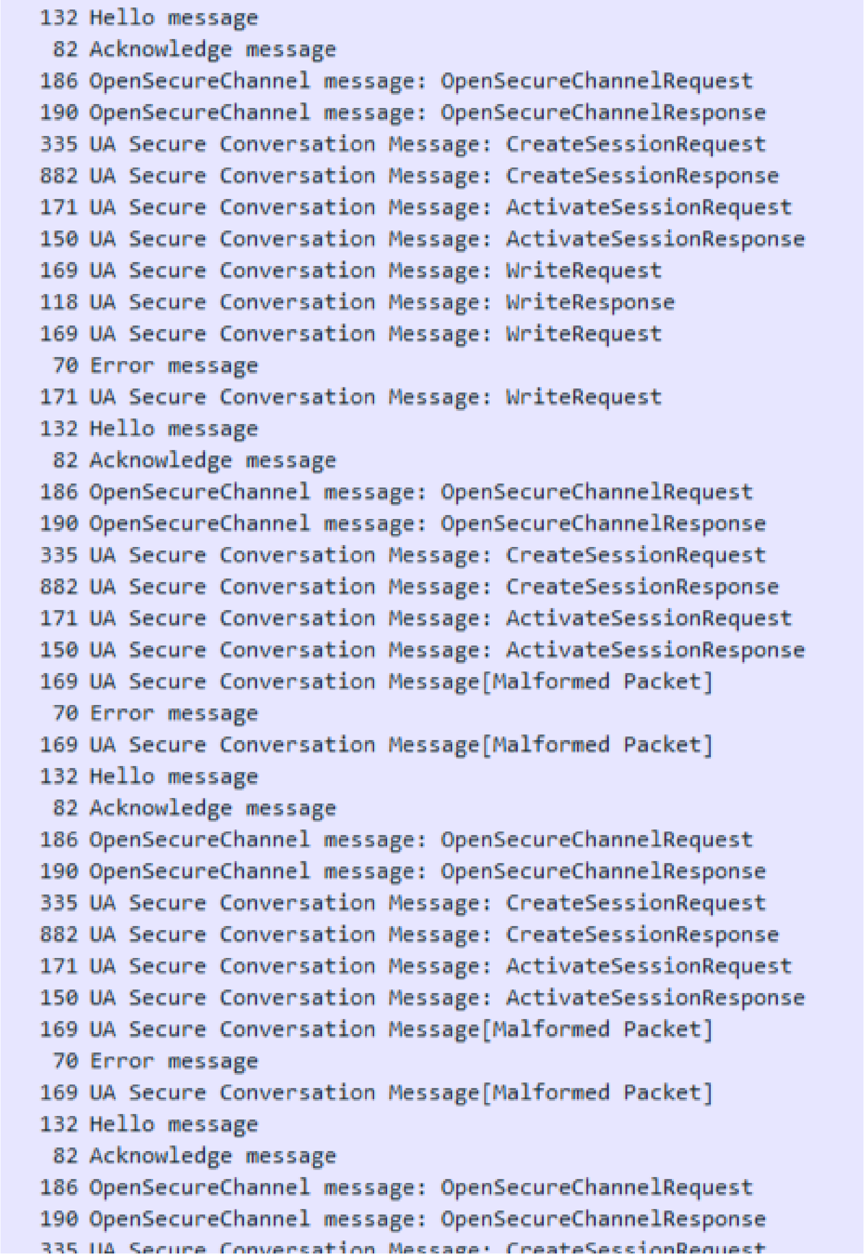
* Read

* Write

* Monitor Items

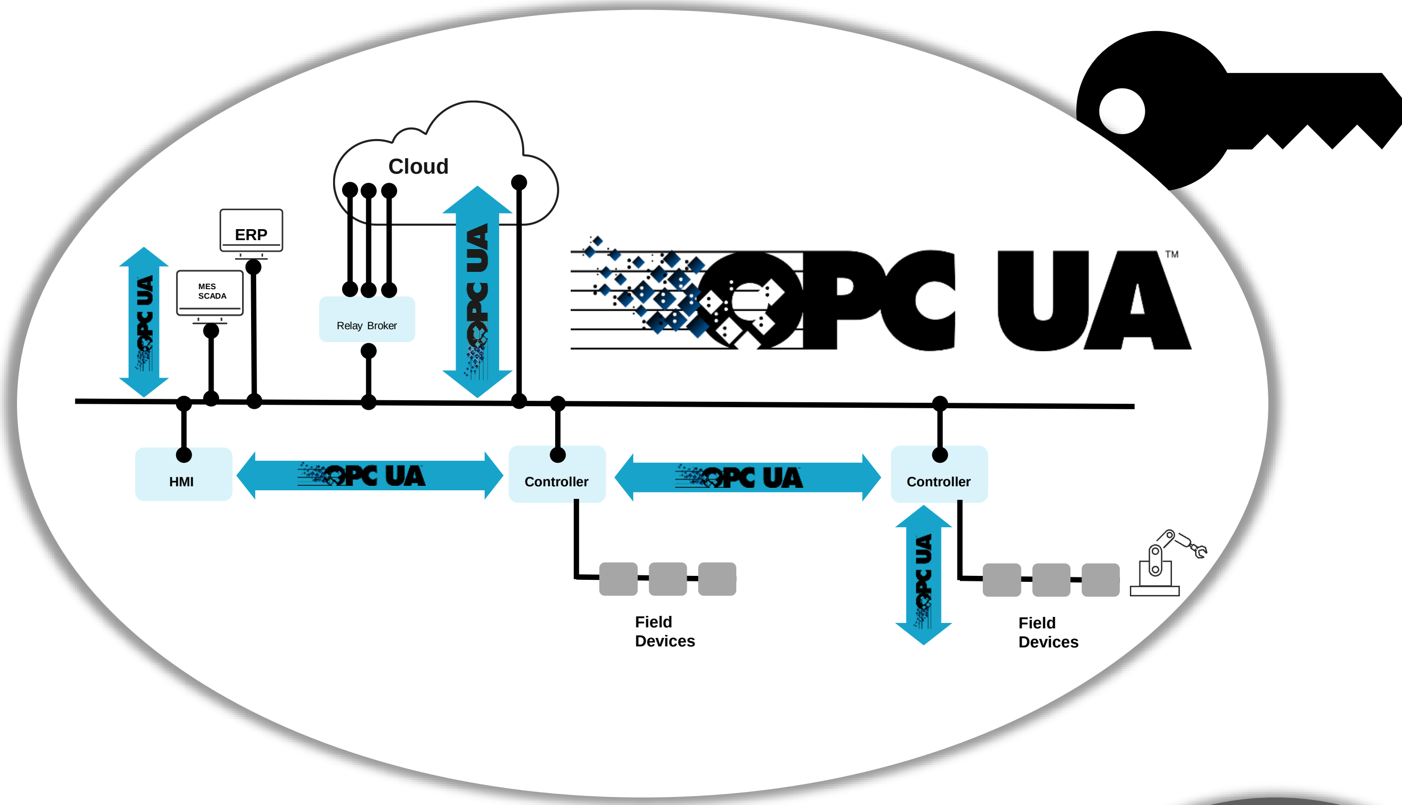


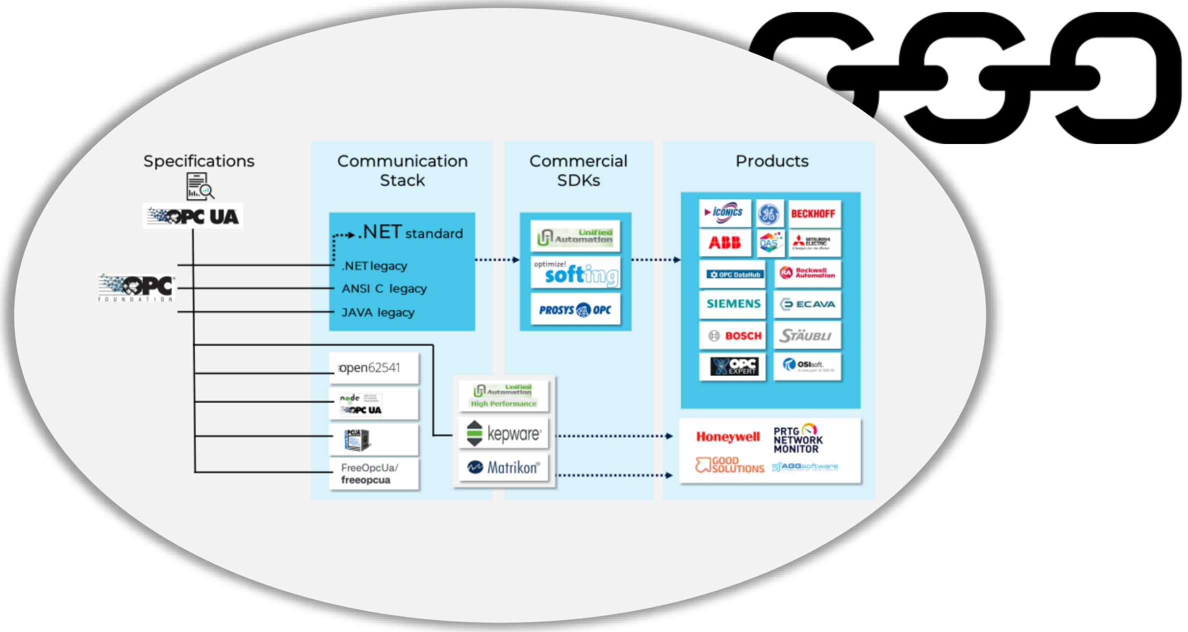


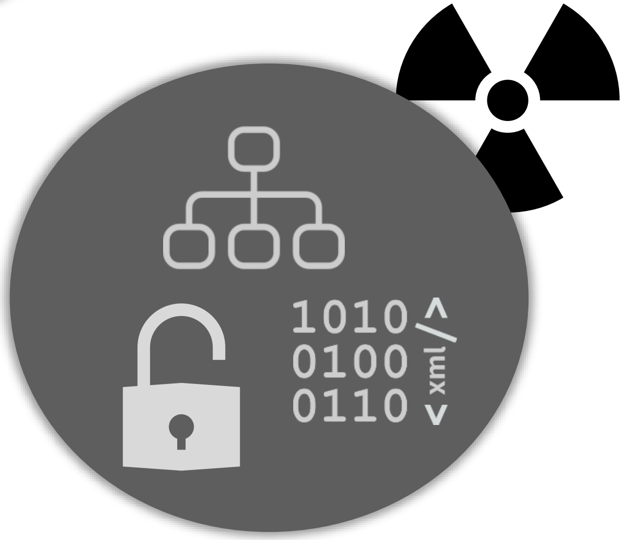


```
132 Hello message
 82 Acknowledge message
186 OpenSecureChannel message: OpenSecureChannelRequest
190 OpenSecureChannel message: OpenSecureChannelResponse
335 UA Secure Conversation Message: CreateSessionRequest
882 UA Secure Conversation Message: CreateSessionResponse
171 UA Secure Conversation Message: ActivateSessionRequest
150 UA Secure Conversation Message: ActivateSessionResponse
169 UA Secure Conversation Message: WriteRequest
118 UA Secure Conversation Message: WriteResponse
169 UA Secure Conversation Message: WriteRequest
 70 Error message
171 UA Secure Conversation Message: WriteRequest
132 Hello message
 82 Acknowledge message
186 OpenSecureChannel message: OpenSecureChannelRequest
190 OpenSecureChannel message: OpenSecureChannelResponse
335 UA Secure Conversation Message: CreateSessionRequest
882 UA Secure Conversation Message: CreateSessionResponse
171 UA Secure Conversation Message: ActivateSessionRequest
150 UA Secure Conversation Message: ActivateSessionResponse
169 UA Secure Conversation Message[Malformed Packet]
 70 Error message
169 UA Secure Conversation Message[Malformed Packet]
132 Hello message
 82 Acknowledge message
186 OpenSecureChannel message: OpenSecureChannelRequest
190 OpenSecureChannel message: OpenSecureChannelResponse
335 UA Secure Conversation Message: CreateSessionRequest
882 UA Secure Conversation Message: CreateSessionResponse
171 UA Secure Conversation Message: ActivateSessionRequest
150 UA Secure Conversation Message: ActivateSessionResponse
169 UA Secure Conversation Message[Malformed Packet]
 70 Error message
169 UA Secure Conversation Message[Malformed Packet]
132 Hello message
 82 Acknowledge message
186 OpenSecureChannel message: OpenSecureChannelRequest
190 OpenSecureChannel message: OpenSecureChannelResponse
335 UA Secure Conversation Message: CreateSessionRequest
```

Summary


Cloud
ERP
MES SCADA
Relay Broker
OPC UA
OPC UA
OPC UA™
HMI
OPC UA
Controller
OPC UA
Controller
OPC UA
Field Devices
Field Devices


Specifications
OPC UA
OPC FOUNDATION
Communication Stack
.NET standard
.NET legacy
ANSI C legacy
JAVA legacy
open62541
node OPC UA
FreeOpcUa/ freeopcua
Commercial SDKs
Unified Automation
optimize! softing
PROSYS OPC
Unified Automation High Performance
kepware
Matrikon
Products
ICONICS
BECKHOFF
ABB
QAS
MITSUBISHI ELECTRIC
OPC DataHub
Rockwell Automation
SIEMENS
ECAVA
BOSCH
STÄUBLI
OPC EXPERT
OSIsoft
Honeywell
PRTG NETWORK MONITOR
GOOD SOLUTIONS
AGGsoftware


1010
0100
0110
<xml/>

Stay Safe!

Eran Jacob
@EranJacob
linkedin.com/in/eranj

Special thanks to

Matan Dobrushin
@matan_dob

Roman Dvorkin
linkedin.com/in/roman-dvorkin

Alon Zini
linkedin.com/in/alon-zini-3b9698185

and the rest of the team