



# Trials and Tribulations: Securing Industrial Control Systems

Alessandro Erba, Anne Müller, Nils Ole Tippenhauer (CISPA)

KIM ZETTER SECURITY 11.03.14 6:30 AM

# AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON





TECHNOLOGY NEWS | Thu Dec 31, 2015 | 12:28pm EST

## Ukraine to probe suspected Russian cyber attack on grid



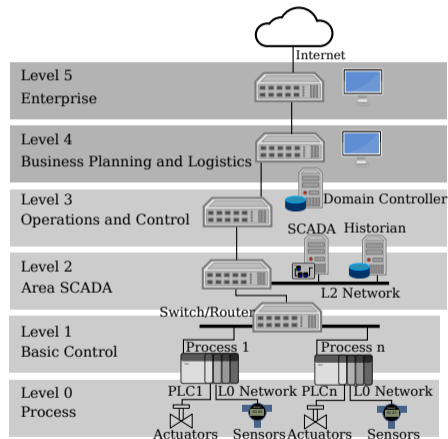


The screenshot shows a Reuters news article. At the top left is the Reuters logo. A navigation bar contains links for World, Business, Markets, Breakingviews, Technology, Investigations, Lifestyle, and Gra. The article is dated May 9, 2021, at 10:00 AM CEST. The category is Technology. The headline is 'Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed'. Below the headline, it says '5 minute read' and 'Christopher Bing, Stephanie Kelly'. There are four social media icons: Facebook, Twitter, a link icon, and an email icon. The bottom of the article features a large image of a pipeline stretching across a landscape under a blue sky.

8,850 km pipeline shut down due to randomware attack. Source: Reuters, May 2021

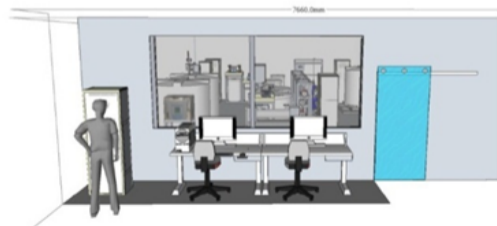
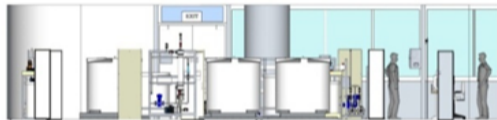
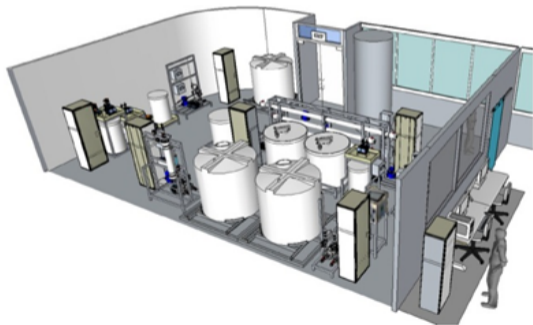
# Challenges for ICS Security

- No security for existing protocols/devices
- Great diversity in platforms and protocols
  - ▶ Which makes concerted research efforts hard
  - ▶ Platforms are generally proprietary
  - ▶ Uncooperative system operators
- Reliability must not be impacted
  - ▶ Hard computation deadlines
  - ▶ Control sensitive to time variations
- Sensor data can lead system to unsafe state
  - ▶ Actuating and sensing cannot be authenticated



# Our Applied Research in Singapore

- How to facilitate research on ICS? Own testbeds reproducing industrial setups
- SWaT, WaDI, EPIC testbeds designed for security research & education
- Full systems with physical process, control, SCADA. First opened 2015
- Overall system cost: > 500k EUR x3 (Water treatment, distribution, power)

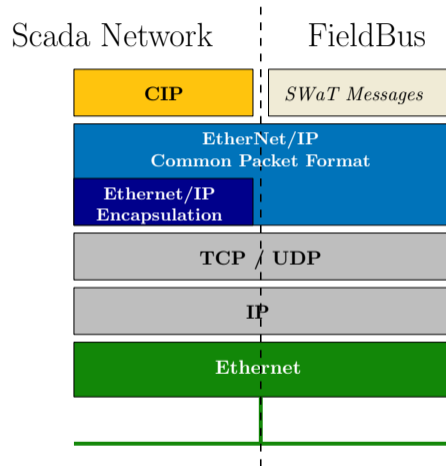


SWaT, planning stage rendering. Source: iTrust

# Related CPS/ICS Work from my Group

- Understand processes and attacks better
  - ▶ Datasets (CPSIoTSEC'20)
  - ▶ Real-world attacks (SG-CRC'16, CCS'16)
  - ▶ Simulation+Honeypot environments (CPS-SPC'15+'16, IoTPTS'17)
- Explore physical process-aware detection
  - ▶ Control-theory based (CCS'16)
  - ▶ Physics-based anomaly detection (CPS-SPC'16)
  - ▶ State-Aware Detection (SAC'18)
  - ▶ Evasion attacks (ACSAC'20)
- Leverage constraints for attacker
  - ▶ Finite data transmission in Distance Bounding (Esorics'09+'11, WiSec'15)
  - ▶ Broadcasting nature of wireless for GPS spoofing detection (CCS'11, ACSAC'16)
- Formal modeling and assessment of systems
  - ▶ Attacker models (Esorics'16, ASIACCS'17)
  - ▶ Quantitative Assessments (NSPW'13, QEST'15, PRDC'14)

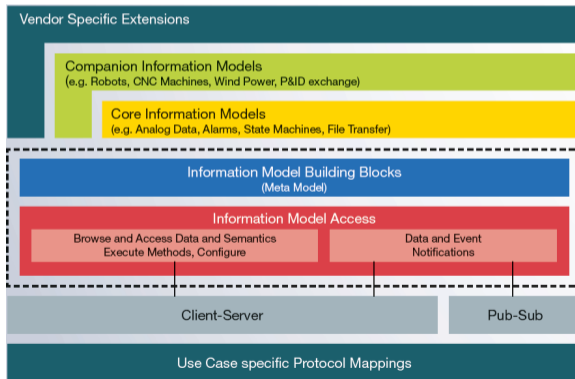
- In SWaT
  - ▶ Ethernet/IP (Rockwell): No security
  - ▶ HTTP/HTTPS no certs, no security
- In WADI
  - ▶ Modbus/TCP: No security
  - ▶ Some proprietary NI protocol (no security)
- In EPIC
  - ▶ GOOSE: No security
  - ▶ Modbus/TCP: No security
  - ▶ ...





# OPC Unified Architecture (UA)

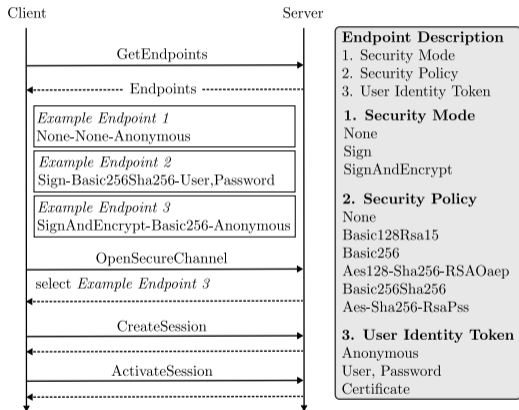
- Developed by OPC foundation, current version 1.04 released in 2018
- *Optional* security features
  - ▶ Authentication, encryption (different modes)
- German BSI reviewed OPC UA security and found no systematic errors
- Dahlmanns et al. (2020) found large numbers of insecure OPC UA systems online



Source: OPC foundation

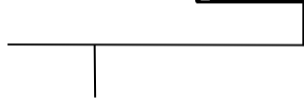
# Security Features of OPC UA (Client/Server)

- Servers offer endpoints
- Each endpoint can have own *security mode, security policy, and user identity*
- Security modes
  - ▶ *None, Sign, SignAndEncrypt*
- Security policies
  - ▶ Concrete scheme, e.g., *Basic256Sha256*
- Cert-based User identity
  - ▶ Apps can have *Certificate Trustlist*
  - ▶ *Global Discovery Server* can also act as CA

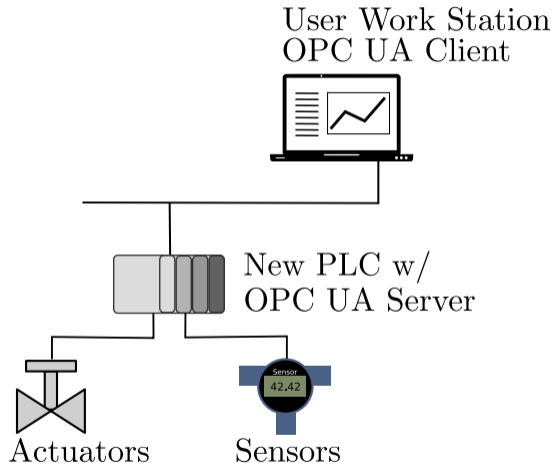


# Example Addition of New Device

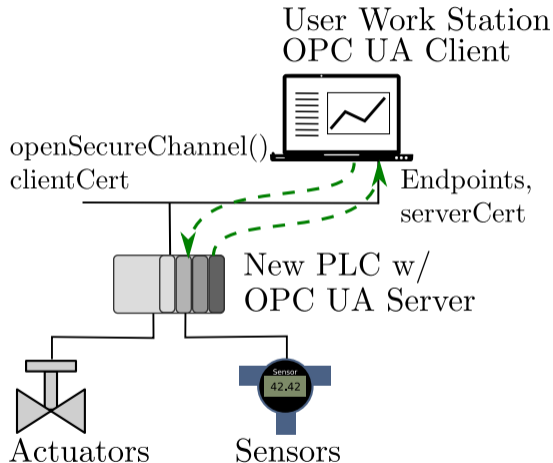
User Work Station  
OPC UA Client



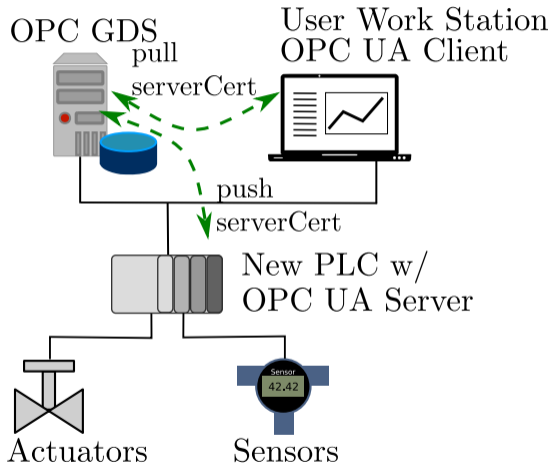
# Example Addition of New Device



# Example Addition of New Device



# Example Addition of New Device



# How is the Trust Bootstrapped?

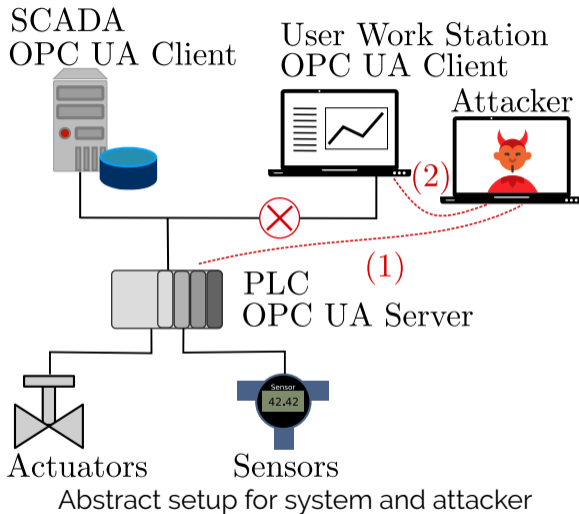
- How does the new device get the trust root (e.g., cert of GDS)?
- On Internet, root CAs have their certs shipped in clients
  - ▶ Not possible for ICS setting (self-signed certs, no Internet)
- *How is this solved in practise?*
- *What are challenges to set up OPC UA security?*
- How do libraries and OPC products
  - ▶ Recommend security configurations?
  - ▶ Address this trust root issue?

For our academic paper, we formulated to the following research questions:

- R1. What are practical challenges for the correct use of security features?
- R2. Are security features correctly implemented by the vendors and products?
- R3. What are the consequences of breaking security features?

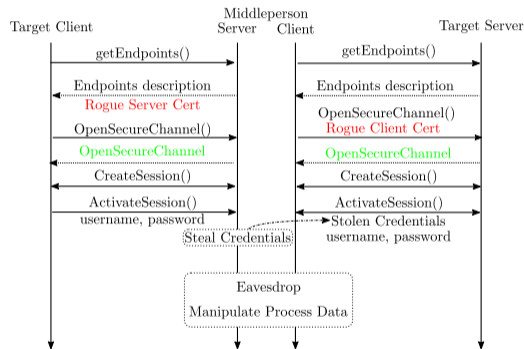


# Attacker Model



# Assessing OPC UA Artifacts

- To find practical challenges (R1), we survey proprietary and open source OPC UA enabled products
- To verify correct implementation (R2), we built a testing framework and applied it to artifacts
- To show consequences of security flaws (R3), we design a PoC that obtains authentication data, allowing to manipulate the process
- We assessed 48 *artifacts* (products+libraries)



Flow of middleperson attack

# Findings for Products

**Table 1.** Adoption of features OPC UA in proprietary products. ● denotes that the feature is supported by the product. ○ denotes that the feature is not supported by the product. ◐ denotes that the feature is supported but there are problems with its configuration that make industrial deployments insecure

Vendor	Platform	OPC Cert.	Pub-Sub	GDS	Security Trustlist	Recommended Policy
B&R	ADI OPC UA [7]	◐	○	○	● ●	Not specified
Bachmann	OPC UA Client and Server [3]	○	○	○	◐ ◐	Not specified
Beckhoff	TC3 OPC UA [4]	○	○	○	◐ ◐	Deprecated protocols
Beijer	iX Developer [5]	○	○	○	○ ○	None
Bosch Rexroth	ctrlX CORE [6]	○	○	○	● ●	None not supported
General Electric	iFIX [19]	○	○	compatible	●	Basic256Sha256
Honeywell	ControlEdge Builder [22]	○ <sup>+</sup>	○	○	○ ○	None
Lenze	Easy Starter [28]	○	○	○	◐ ◐	Deprecated protocols
Mitsubishi	MX Configurator-R [31]	●	○	○	● ●	None
National Instruments	InsightCM [33]	○	○	○	● ●	None
Omron	SYSMAC-SE2 [36]	●	○	○	● ●	Not specified
Panasonic	HMWIN Studio [44]	○	○	compatible	● ◐	Not specified
Rockwell	Factory talk linx [46]	○	○	○	● ●	Not specified
Schneider	Control Expert [15]	◐	○	○	● ●	Basic256Sha256
Siemens	STEP 7 [49]	●	○	compatible	● ◐	Not specified
Weidmüller	u-create studio [52]	○	○	○	● ●	Basic256Sha256
Yokogawa	SMARTDAC+ [53]	○	○	○	○ ○	None
Codesys based platforms						
Codesys	Codesys V3.5 [9]	○	●	○	● ◐	Not specified
ABB	Automation Builder [1]	○	○	○	● ◐	Basic256Sha256
Eaton	XSOFT-CODESYS [13]	○	○	○	● ◐	Not specified
Hitachi	HX Codesys [21]	○	○	○	● ◐	Not specified
Wago	e cockpit [51]	●	○	compatible	● ◐	Not specified

<sup>+</sup> We report the state of the documentation consulted during the investigation. After a pre-print of this manuscript was published online, the documentation related to this product was updated, now it supports security features and it is certified by OPC Foundation.

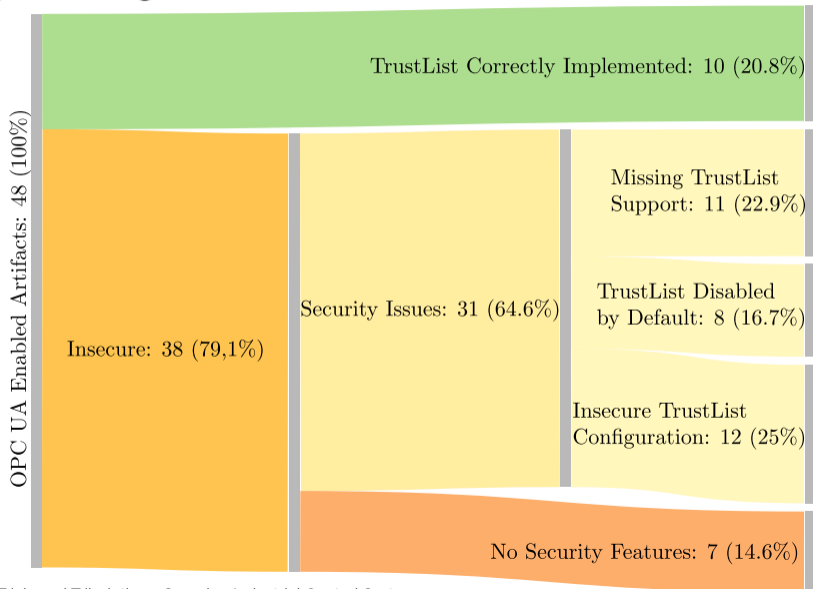
# Findings for Libraries

**Table 2.** Libraries with OPC UA implementation. ● denotes that the feature is supported by the product. ○ denotes that the feature is not supported by the product. ◐ denotes that the feature is supported but there are problems with its configuration. The column Security reports whether the library implements signing and encryption. The column Trustlist reports whether the library implements application authentication. The column Demo Behaviour reports whether a secure connection to the demo application is possible

Name	Lang.	OPC Cert.	Pub Sub	GDS	Server			Client		
					Security	Trustlist	Demo Behavior	Security	Trustlist	Demo Behavior
ASNeG [2]	C++	○	○*	○	●	○	-	○*	-	-
Eclipse Milo [14]	Java	○	○	○	●	●	●	●	◐	○
Free OpcUA [18]	C++	○	○	○	-	-	-	○	-	-
LibUA [29]	C#	○	○	○	●	○	○	●	○	○
node-opcua [35]	.js	○	○*	○	●	●	◐	●	○	○
opc-ua-client [11]	C#	○	○	-	-	-	-	●	●	◐
opcua [47]	Rust	○	○	○	●	●	◐	●	●	◐
opcua [20]	Golang	○	○	○	-	-	-	●	-	-
opcua [23]	TypeScript	○	○	-	-	-	-	○	-	-
opcua4j [41]	Java	○	○	○	○	-	-	-	-	-
open62541 [42]	C	◐*	●	○	●	●	◐	●	●	◐
OpenScada UA [43]	C++	○	○	○	●	○	○	●	○	○
Python-opcua [17]	Python	○	○	○	●	○	○	●	○	○
S2OPC [48]	C	◐*	●	○	●	●	●	●	◐	◐
UA.NET [40]	C#	●	○	●	●	●	●	●	●	◐
UAexpert [50]	C++	●	○	○	-	-	-	●	●	◐

\*Server certified, client not certified. ◐\*Denotes that the feature is going to be introduced in the next release

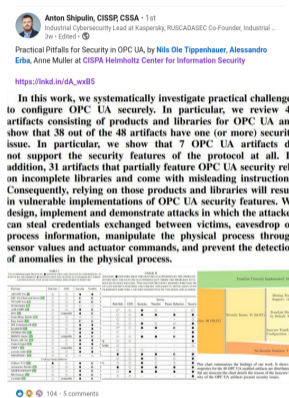
# Summary Findings



- How to fix issues?
- Certification by OPC is one way
  - ▶ Ensures that products at least comply to standard
- We suggest tighter requirements in standard
  - ▶ Disallow secure channels without Trustlist
  - ▶ Require secure / out-of-band channel for cert bootstrap
  - ▶ Don't just outsource cert verifications to humans
- Tutorials and manuals need to be very careful with dismissing security features
  - ▶ If everything is disabled in tutorial, unlikely to be used later
- Impact of insecure setups need to be discussed more clearly with users

# Impact of Findings

- Currently under submission at tier-2 security conference
- Preprint was quickly picked up by Anton Shipulin, industrial security lead at Kaspersky
  - ▶ 104 likes on linkedin, 28 likes on twitter
- Some suggested to submit to Blackhat etc.
- We didn't try for CVEs as no direct exploits
- We discussed study with BSI and OPC foundation
  - ▶ Likely impact in OPC UA standard and certification process
  - ▶ It appears optional security is still wanted trade-off
- We are currently looking into user studies with ICS operators



Anton Shipulin, CISSP, CSSA · 1st  
Industrial Cybersecurity Lead at Kaspersky, RUSCADASEC Co-Founder, Industrial ...  
3w · Edited · 🌐

Practical Pitfalls for Security in OPC UA, by Nils Ole Tippenhauer, Alessandro Erba, Anne Muller at CISPA Helmholtz Center for Information Security  
[https://lnkd.in/dA\\_wxBS](https://lnkd.in/dA_wxBS)

In this work, we systematically investigate practical challenge to configure OPC UA securely. In particular, we review 41 artifacts consisting of products and libraries for OPC UA and show that 38 out of the 48 artifacts have one (or more) security issue. In particular, we show that 7 OPC UA artifacts do not support the security features of the protocol at all. In addition, 31 artifacts that partially feature OPC UA security rely on incomplete libraries and come with misleading instructions. Consequently, relying on those products and libraries will result in vulnerable implementations of OPC UA security features. We design, implement and demonstrate attacks in which the attacker can steal credentials exchanged between victims, eavesdrop on process information, manipulate the physical process through sensor values and actuator commands, and prevent the detection of anomalies in the physical process.

Artifact	Product	Library	Security Issue	Severity	Impact
...	...	...	...	...	...

👍👎🗨️ 104 · 5 comments

LinkedIn post by Anton Shipulin

# Conclusions

- There are significant security shortcomings in industrial protocols, products, and legacy systems
- Reason is not (only) technical ignorance, but practical issues
  - ▶ Legacy compliance, long lifetime, lack of CA infrastructure, observability requirements, ...
- OPC UA one of the few solutions with security features, solid design
  - ▶ Challenges in implementations by third parties, endusers
- We identified 38 out of 48 reviewed artifacts have one (or more) security issue
- Impact: as reaction to our pre-print
  - ▶ Several libraries/vendors already updated documentation
  - ▶ OPC UA documentation will likely be updated
  - ▶ Certification process might also be reviewed
- Lots of promise in usable security for ICS, but difficult to do user studies
- Preprint out at <https://arxiv.org/abs/2104.06051>



# Conclusions

- There are significant security shortcomings in industrial protocols, products, and legacy systems
- Reason is not (only) technical ignorance, but practical issues
  - ▶ Legacy compliance, long lifetime, lack of CA infrastructure, observability requirements, ...
- OPC UA one of the few solutions with security features, solid design
  - ▶ Challenges in implementations by third parties, endusers
- We identified 38 out of 48 reviewed artifacts have one (or more) security issue
- Impact: as reaction to our pre-print
  - ▶ Several libraries/vendors already updated documentation
  - ▶ OPC UA documentation will likely be updated
  - ▶ Certification process might also be reviewed
- Lots of promise in usable security for ICS, but difficult to do user studies
- Preprint out at <https://arxiv.org/abs/2104.06051>

Thank you for your attention - Questions?