

# Nozomi Networks

**OT and IoT Security  
for Global Leader**



## Leadership in Key Industries



Oil & Gas  
6 of Top 20



Pharmaceuticals  
5 of Top 10



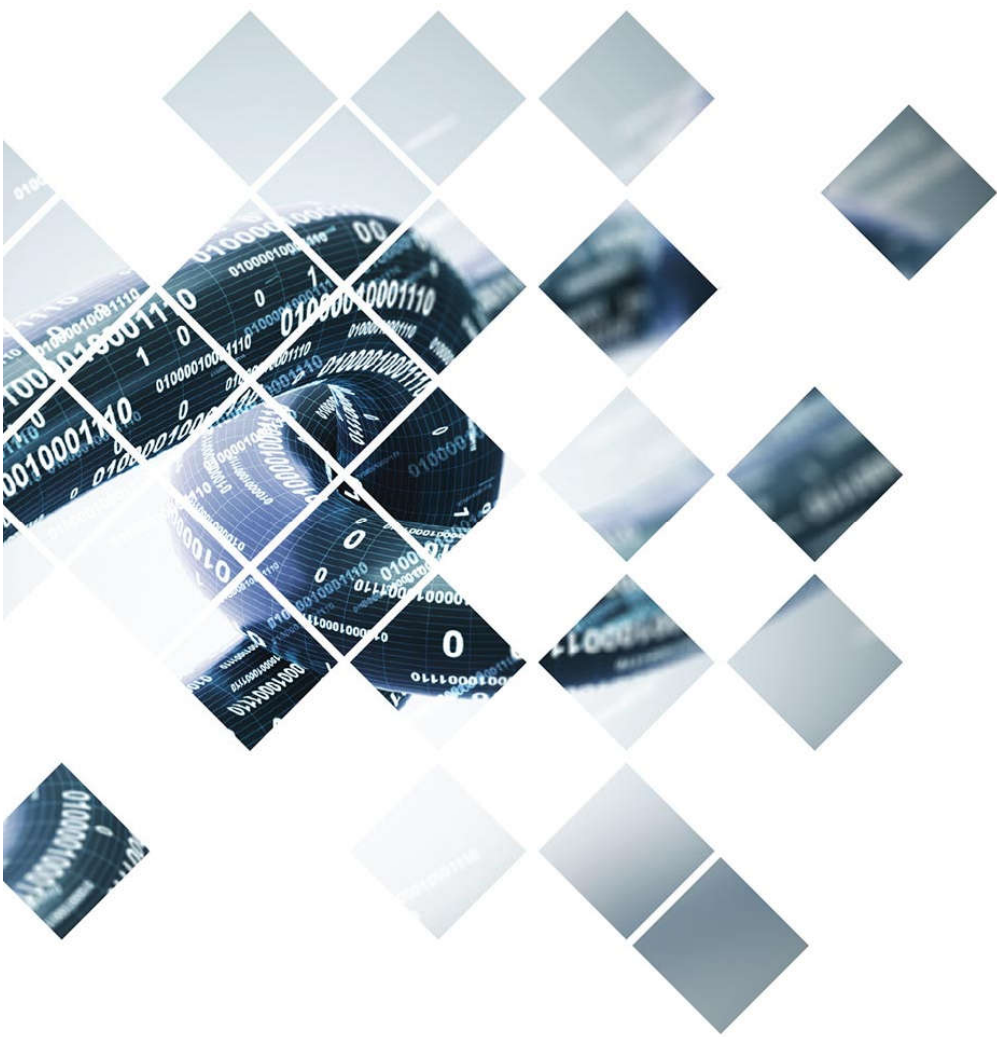
Utilities  
4 of Top 10



Mining  
4 of Top 10

# Key Takeaways

- Encryption for OT/IoT networks is not the norm today but **will be increasingly used in the future**
- It's possible to attack systems, even when they're encrypted
- Monitoring systems need to detect encryption-related attacks
- Nozomi Networks products are ready today



# Future Threat Detection Landscape

**Alerts** Page 1 of 1, 1 entries

 Export 

 Group by incident 

 Live  
 

RISK	TIME	NAME	DESCRIPTION
<div> <div>9</div> </div>	11:40:22.882	<div> <div>✓</div> <div>✗ RTU - Invalid CA certificate</div> </div>	An unknown CA certificate was detected in the RTU. This could indicate a misconfiguration of the certificates, or a malicious act to establish encrypted and authenticated communication with threat actors.

- ▾

⏮ ⏪ ⏩ ⏭



## RTU - Invalid CA certificate

 11:40:22.882 | **Status:** open

An unknown CA certificate was detected in the RTU. This could indicate a misconfiguration of the certificates, or a malicious act to establish encrypted and authenticated communication with threat actors.

	Source
Is security	false
Protocol	unknown

This alert has been triggered by an assertion that has failed.

[Open details >](#)

## Alerts

Page 1 of 1, 0 entries

 Export 

 Group by incident ☒ 

 Live ☒ 


RISK	TIME	NAME	DESCRIPTION
------	------	------	-------------

<div> <div>-</div> <div>▼</div> </div>	<div> <div>⏮</div> <div>⏪</div> <div>⏩</div> <div>⏭</div> </div>	<input type="text"/>	<input type="text"/>
--	--	----------------------	----------------------

There are no alerts

```
> p3 attack_script_CA.py
[2020-01-10 23:45:30,042] INFO : Starting...
[2020-01-10 23:45:31,045] INFO : Generating new rogue CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIID4DCCAsGCCQD1aITI4WlgRzANBgkqhkiG9w0BAQsFADCBsTELMakGA1UEBhMC
amsxFDASBgNVBAGMC05vIG1hbiBsYW5kMRMwEQYDVQQHDApDYW5keSBjaXR5MRUw
EwYDVQQKDAxUaGUgZGFyayBvbmUxZjAUBG9NVBAsMDURhcm9uZGhpc3dhc2x1Z210
BgNVBAMMAm9uZGhpc3dhc2x1Z210BgNVBAsMDURhcm9uZGhpc3dhc2x1Z210
aW1hdGVdQWNlcnRAZG1kbR1LmNvbTAeFw0yMDAxMTAxMTA1MjZaFw0yNTAxMDgx
MTA1MjZaMIGxMQswCQYDVQQGEWJqazEUMBIGA1UECAwLTm8gbW9uZGhpc3dhc2x1Z210
BgNVBACMCkNhbmR5IG9uZGhpc3dhc2x1Z210BgNVBAsMDFRoZSBkYXJrIG9uZTEWMBQGA1UE
CwwNRGFyayBkaXZpc2lvdjELMAkGA1UEAwwCamsxOzA5BgkqhkiG9w0BCQEWLHlv
dXR0b3VnaHR0aGlzd2FzbGVnaXRpbW9uZGhpc3dhc2x1Z210BgNVBAsMDFRoZSBkYXJrIG9uZTEWMBQGA1UE
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyMiH/ebZjx1Fy7B7xsHwVuhcJvSe
CKUFkulaQ09G+I5+q13LSX1bGTJidxhvQSCGV5oKhunlwJoQBYe75cRcbfNZaFtB
CZC6KyuXQS9x4rf/IKjpWxyzTIC3MqDHqFoso8IA32puQLssq4ne06F11P/4Sxv8
7jfkuhc8kEhGL8Tb0tXYoiLn+DSFYRDbk6x1uCJF62CL0LgaXpJeZh/fxoTjzqFT
Q/3V8jeNurWalHtfMvyX+ok1uxqrKyV+D1/2nd1du/nLYc6tfEdEVFT/Ej+SSmGA
B7HgRFxdLLdmOrjAbIPwy1PiVlu05iSxatgCQgX2Jj7IMuMtvmyFigN+fwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4IBAQAaml9udU5SRrEn3p3X3zC0aUZcV7f+4eS0+YQ
EvUzc/xlt+d612vvkfbAmplFMKghv06A0tCotzJPV0TbvZqtfr5G1kduv9Pjo8vX
xiGukd3qj2e90kbMs9gxxosLz4ZMV6ACx40ky4KeUE/OgG6RF114ZnX+1kHG/KiP
8w/iaYpSrZzZjVgCSmAL3AsNDnfAOR9/cQlGbbu37iL3RY011J74+rRLTCGlgBh1
mg2bbBUAgfIAS53o9m6Wi5+4nyCCRVcdOph9J2gM3QtpegCcs8uOKL14WdaVYvsU
kKk+8xBnkX1GPKsjAg13VKKGIwu1K2FtZZguqcdfDQy68gpR
```

```
-----END CERTIFICATE-----
```

```
[2020-01-10 23:45:36,047] INFO : Loading payload...
[2020-01-10 23:45:42,048] WARNING : Remote connection attempt to the RTU.
[2020-01-10 23:45:48,050] INFO : Status: Connected
[2020-01-10 23:45:48,050] WARNING : Uploading payload via FTP.
[2020-01-10 23:45:54,052] INFO : Status: Upload success
[2020-01-10 23:45:55,055] INFO : Exiting...
```




```
> p3 attack_script_CA.py
[2020-01-10 23:45:30,042] INFO : Starting...
[2020-01-10 23:45:31,045] INFO : Generating new rogue CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIID4DCCAsGCCQD1aITI4WlgRzANBgkqhkiG9w0BAQsFADCBsTElMAkGA1UEBhMC
amsxFDASBgNVBAGMC05vIGIhbiBsYW5kMkRMwEQYDVQQHDApDYW5keSBjaXR5MRUw
EwYDVQQKDAxUaGUgZGFyayBvbmUxZjAUBGNVBAsMDURhcmsGZG12aXNpb24xCzAJ
BgNVBAMMAMprMTswOQYJKoZIhvcNAQkBFix5b3V0aG91Z2h0dGhpc3dhc2xlZ2l0
aW1hdGVdQWNlcnRAZG1kbR1LmNvbTAeFw0yMDAxMTAxMTA1MjZaFw0yNTAxMDgx
MTA1MjZaMIGxMQswCQYDVQQGEWJqazEUMBIGA1UECAwLTm8gbWFWuIGxhbmQxEzAR
BgNVBACMcKNhbmR5IGNpdHkxFTATBgNVBAoMDFRoZSBkYXJrIG9uZTEWMBQGA1UE
CwwNRGFyayBkaXZpc2lvdjELMAkGA1UEAwwCamsxOzA5BgkqhkiG9w0BCQEWLHlv
dXRob3VnaHR0aGlzd2FzbGVnaXRpbWFW0ZUNBY2VydEBkaWRudHUuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYMiH/ebZjx1Fy7B7xsHwVuhcJvSe
CKUFkulaQO9G+I5+q13LSX1bGTJidxhvQSCGV5oKhunlwJoQBYe75cRcbfNZaFtB
CZC6KyuXQS9x4rf/IKjpWxyzTIC3MqDHqFoso8IA32puQLssq4ne06F1lP/4Sxv8
7jfkuhc8kEhGL8Tb0tXYoiLn+DSFYRDbk6x1uCJF62CLOLgaXpJeZh/fxoTjzqFT
Q/3V8jeNurWalHtfMvyX+ok1uxqrKyV+D1/2nd1du/nLYc6tfEdEVFT/Ej+SSmGA
B7HgRFxdLLdmOrjAbIPwy1PiVlu05iSxatgCQgX2Jj7IMuMtvmyFigN+fwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4IBAQAaml19udU5SRrEn3p3X3zC0aUZcV7f+4eS0+YQ
EvUzc/xlt+d612vvkfbAmplFMKghv06A0tCotzJPV0TbvZqtfr5G1kduv9Pjo8vX
xiGukd3qj2e90kbMs9gxxosLz4ZMV6ACx40ky4KeUE/OgG6RF114ZnX+1kHG/KiP
8w/iaYpSrZzZjVgCSmAL3AsNDnfAOR9/cQlGbbu37iL3RY011J74+rRLTCGlgbh1
mg2bbBUAgfIAS53o9m6Wi5+4nyCCRvcdOph9J2gM3QtpegCcs8u0KL14WDaVYvsU
kKk+8xBnkX1GPKsjAg13VKKGiwu1K2FtZZguqcdfDQy68gpR
```

```
-----END CERTIFICATE-----
```

```
[2020-01-10 23:45:36,047] INFO : Loading payload...
```

**Alerts** Page 1 of 1, 0 entriesExport Group by incident ☒  Live ☒ 

RISK	TIME	NAME	DESCRIPTION
------	------	------	-------------

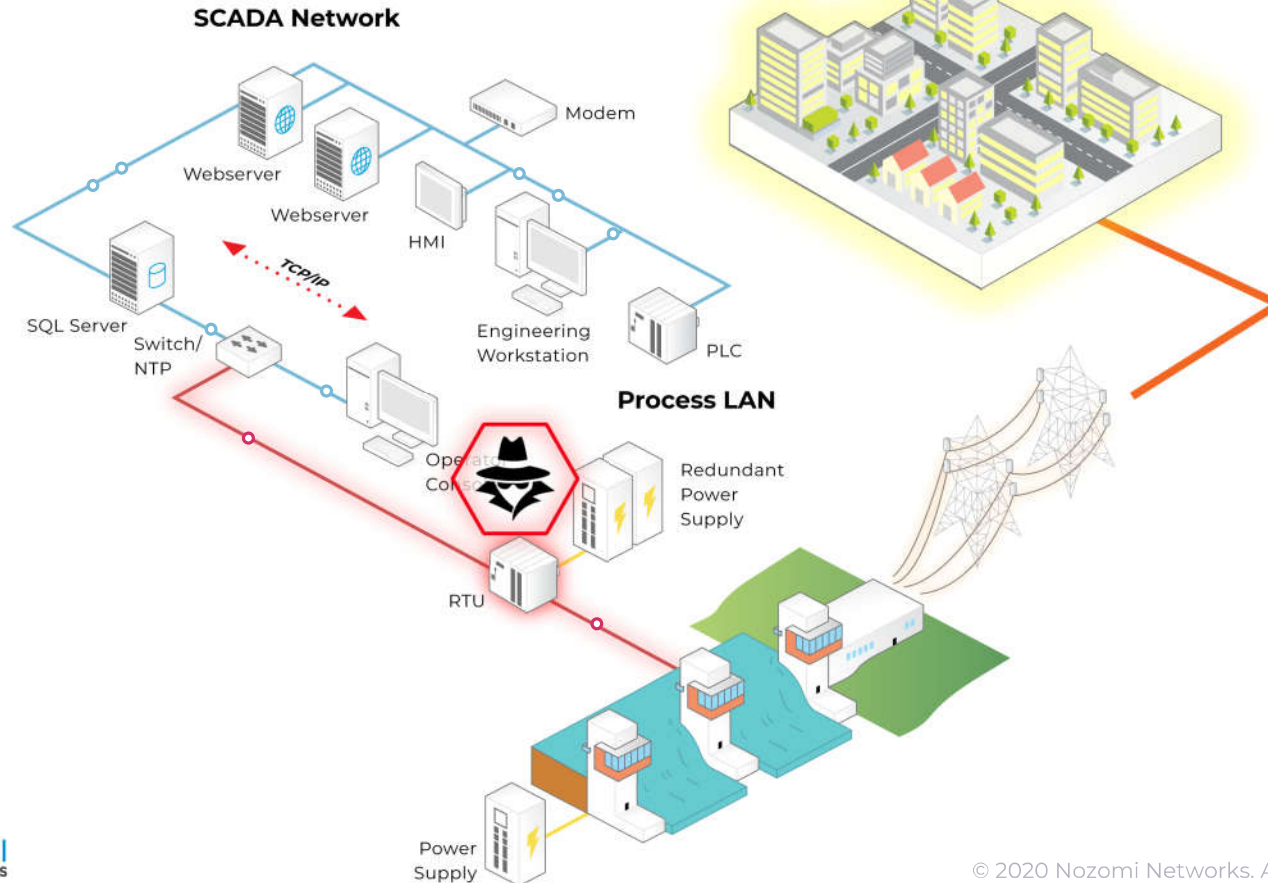
<div>- ▾</div>	<div>⏮ ⏪ ⏩ ⏭</div>	<div></div>	<div></div>
----------------	--------------------	-------------	-------------

There are no alerts



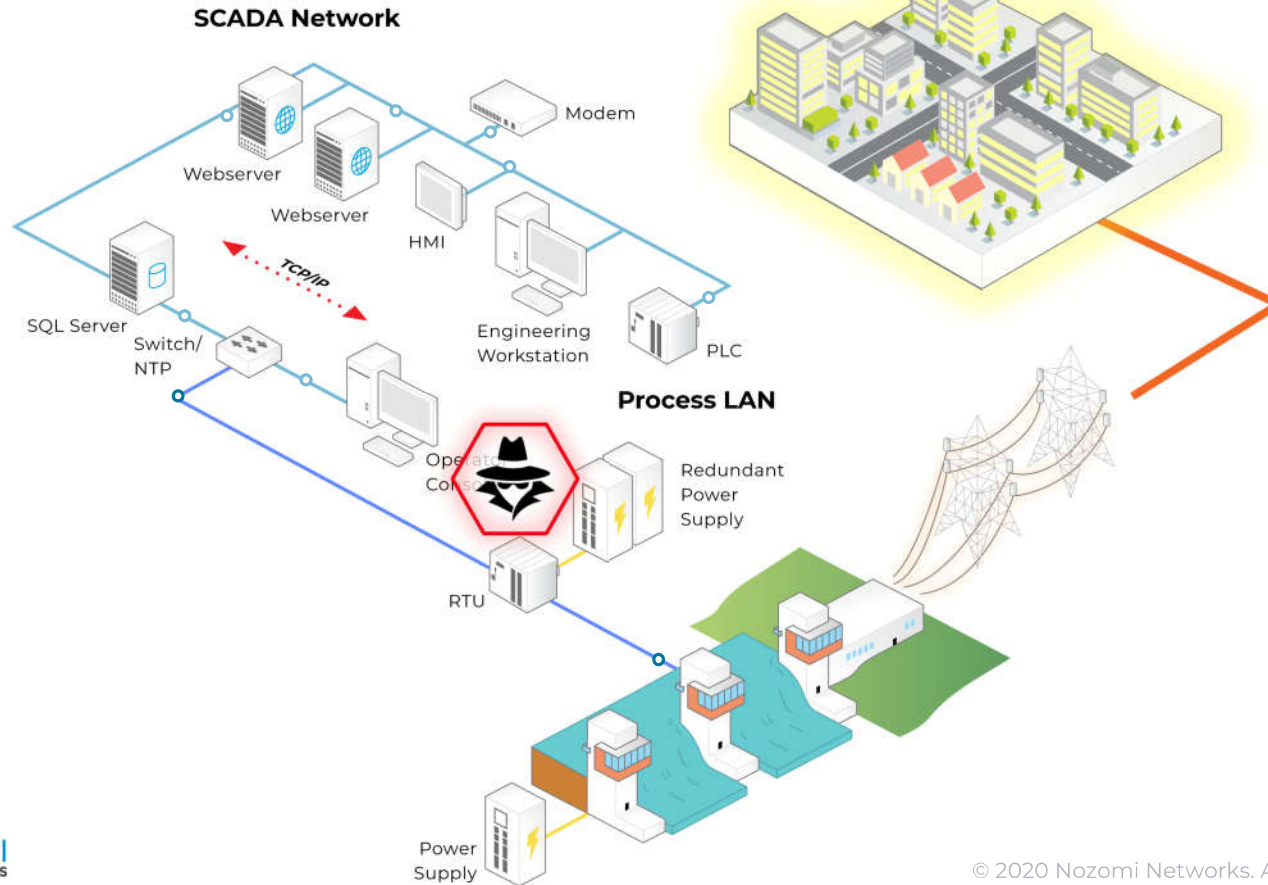
# Attack Scenario 2:

## Rogue CA Certificate



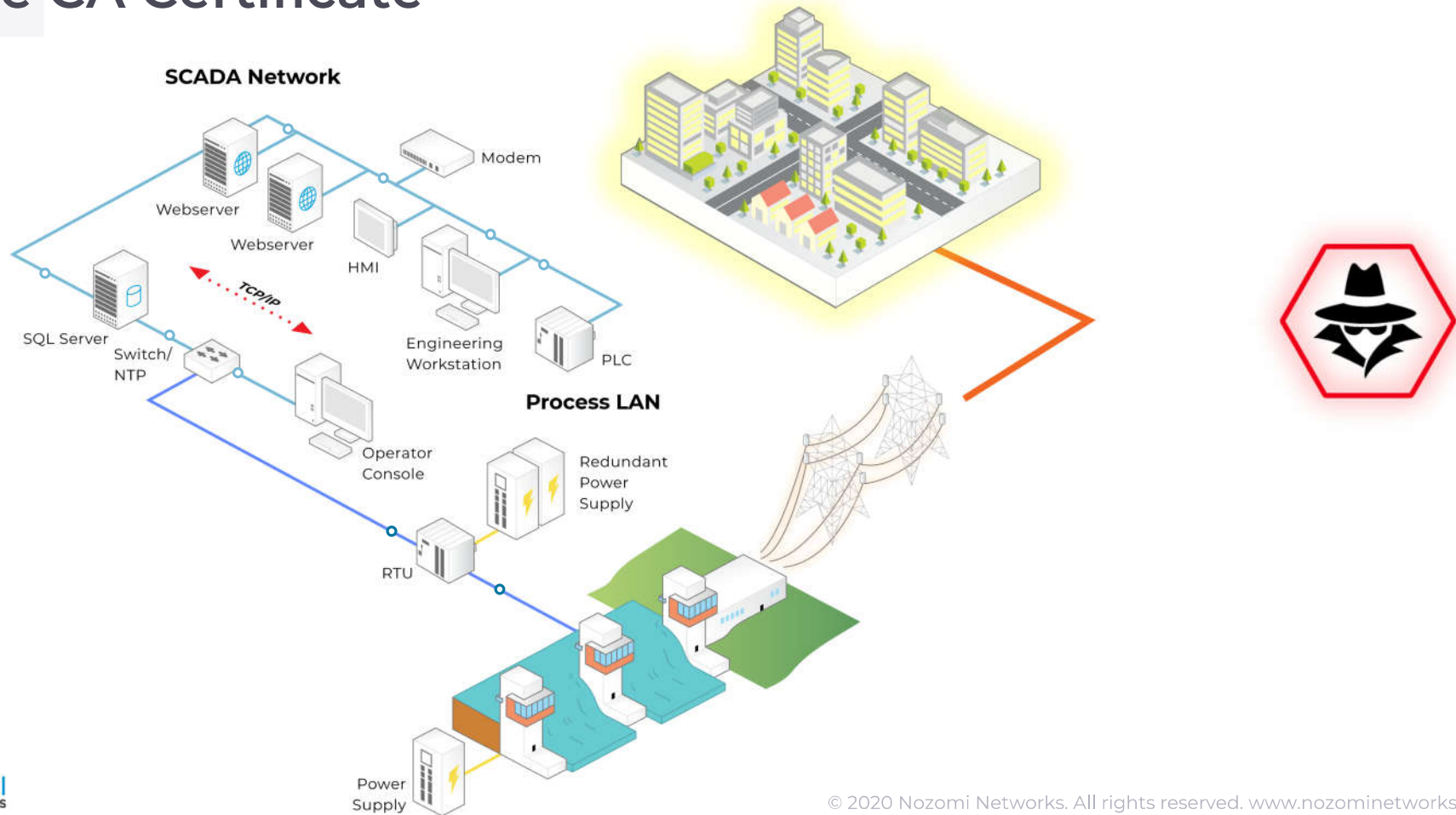
# Attack Scenario 2:

## Rogue CA Certificate



# Attack Scenario 2:







## Rogue CA Certificate



## Alerts Page 1 of 1, 2 entries

[Export](#) 
[Group by incident](#) 

[Live](#)  
 

RISK	TIME	NAME	DESCRIPTION
	11:51:43.834	  RTU - Clock Tampering	Clock tampering was detected in the RTU. The time drift is more than 30 days and could impact the operational process, or invalidate the TLS certificate if an expiration date is set.
	11:51:28.503	  Clock async	A significant time delta was detected between Guardian and a node. Clock asynchronization can create DoS states, hinder the operation process and invalidate digital certificates.



## RTU - Clock Tampering

11:51:43.834 | **Status:** open

Clock tampering was detected in the RTU. The time drift is more than 30 days and could impact the operational process, or invalidate the TLS certificate if an expiration date is set.

	Source
Is security	false
Protocol	unknown

This alert has been triggered by an assertion that has failed.

[Open details >](#)

## Alerts Page 1 of 1,1 entries

Export 

Group by incident ☐



Live ☒



RISK

- ▾

TIME



NAME

DESCRIPTION



11:51:28.503

⋮  
x Clock async

A significant time delta was detected between Guardian and a node. Clock asynchronization can create DoS states, hinder the operation process and invalidate digital certificates.



## Clock async

11:51:28.503 | **Status:** open

A significant time delta was detected between Guardian and a node. Clock asynchronization can create DoS states, hinder the operation process and invalidate digital certificates.

Source

Is security

false

Protocol

unknown

This alert has been triggered by an assertion that has failed.

[Open details >](#)



## Alerts Page 1 of 1, 0 entries

Export Group by incident Live  

RISK	TIME	NAME	DESCRIPTION
------	------	------	-------------

<div>- ▼</div>	<div>⏮ ⏪ ⏩ ⏭</div>	<div></div>	<div></div>
----------------	--------------------	-------------	-------------

There are no alerts

```
► p3 attack_script_ntp.py
[2020-01-10 11:50:56,782] INFO : Starting...
[2020-01-10 11:50:57,784] INFO : RTU time: 10/01/2020 - 11:50:57
[2020-01-10 11:51:00,787] INFO : Attempting to tamper with the RTU clock.
[2020-01-10 11:51:04,789] WARNING : Setting ntp time to current time plus 4 years.
[2020-01-10 11:51:06,791] INFO : Waiting for RTU time response...
[2020-01-10 11:51:16,794] INFO : RTU time: 10/01/2024 - 11:51:16
[2020-01-10 11:51:19,796] INFO : Status: Clock tampering successful
[2020-01-10 11:51:20,799] INFO : Exiting...
```

```
research/s4x20/scripts
```


```
► █
```

```
► p3 attack_script_ntp.py
[2020-01-10 11:50:56,782] INFO : Starting...
[2020-01-10 11:50:57,784] INFO : RTU time: 10/01/2020 - 11:50:57
[2020-01-10 11:51:00,787] INFO : Attempting to tamper with the RTU clock.
[2020-01-10 11:51:04,789] WARNING : Setting ntp time to current time plus 4 years.
[2020-01-10 11:51:06,791] INFO : Waiting for RTU time response...
```

## Alerts

Page 1 of 1, 0 entries

 Export 

 Group by incident ☒ 

 Live ☒ 

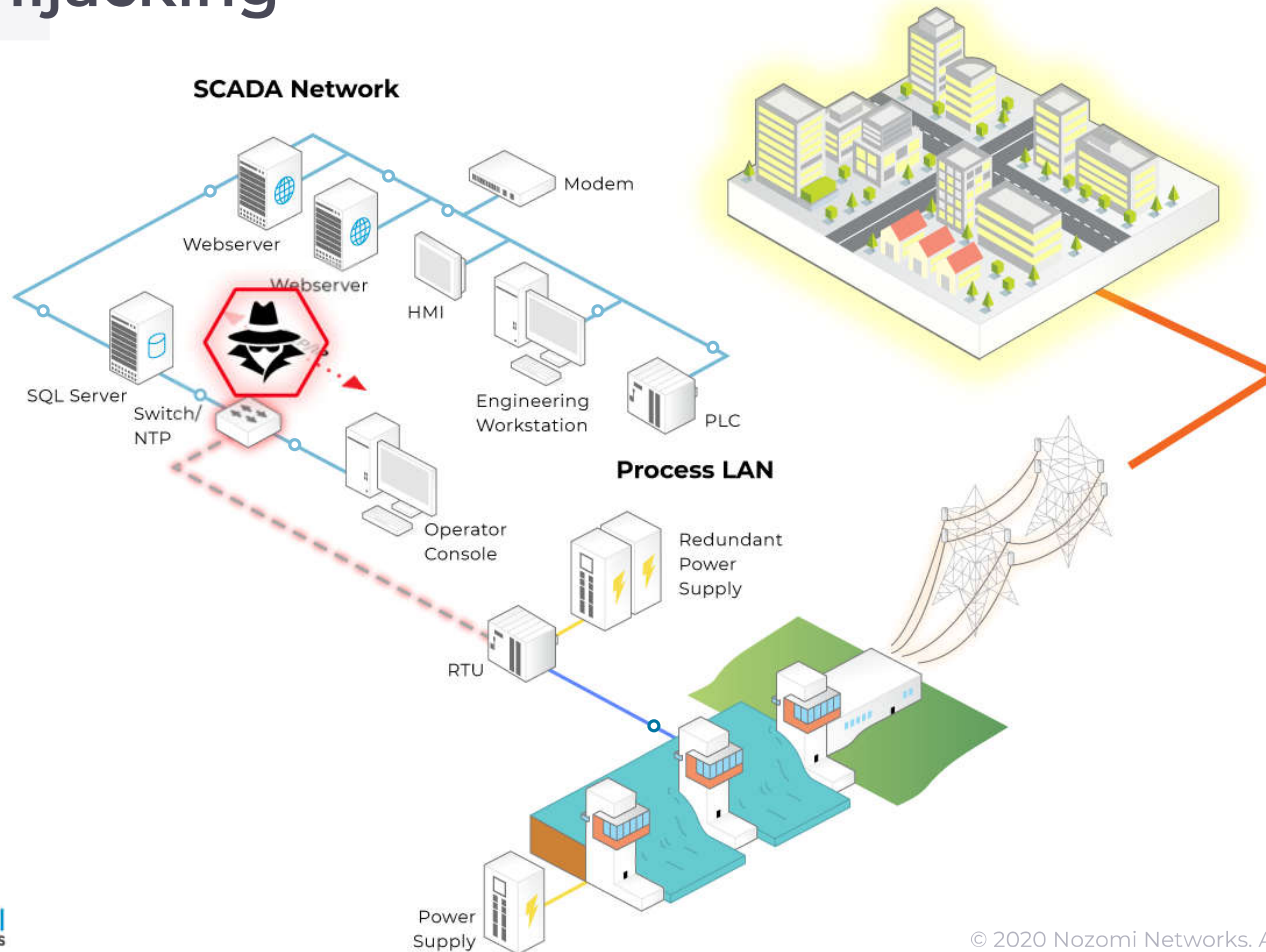

RISK	TIME	NAME	DESCRIPTION
------	------	------	-------------

- ▾	⏮ ⏪ ⏩ ⏭		
-----	---------	--	--

There are no alerts

# Attack Scenario 1:

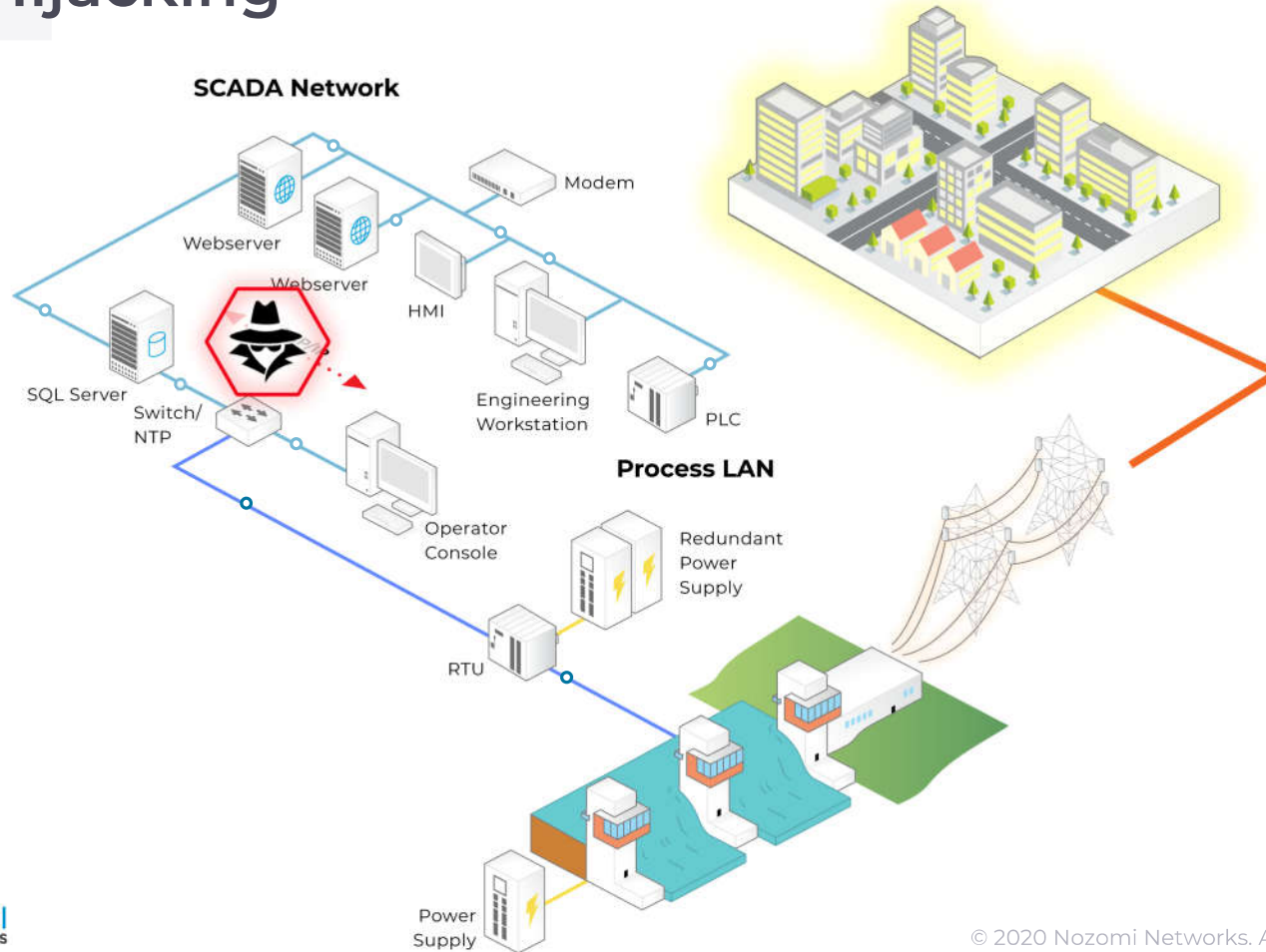
## NTP Hijacking





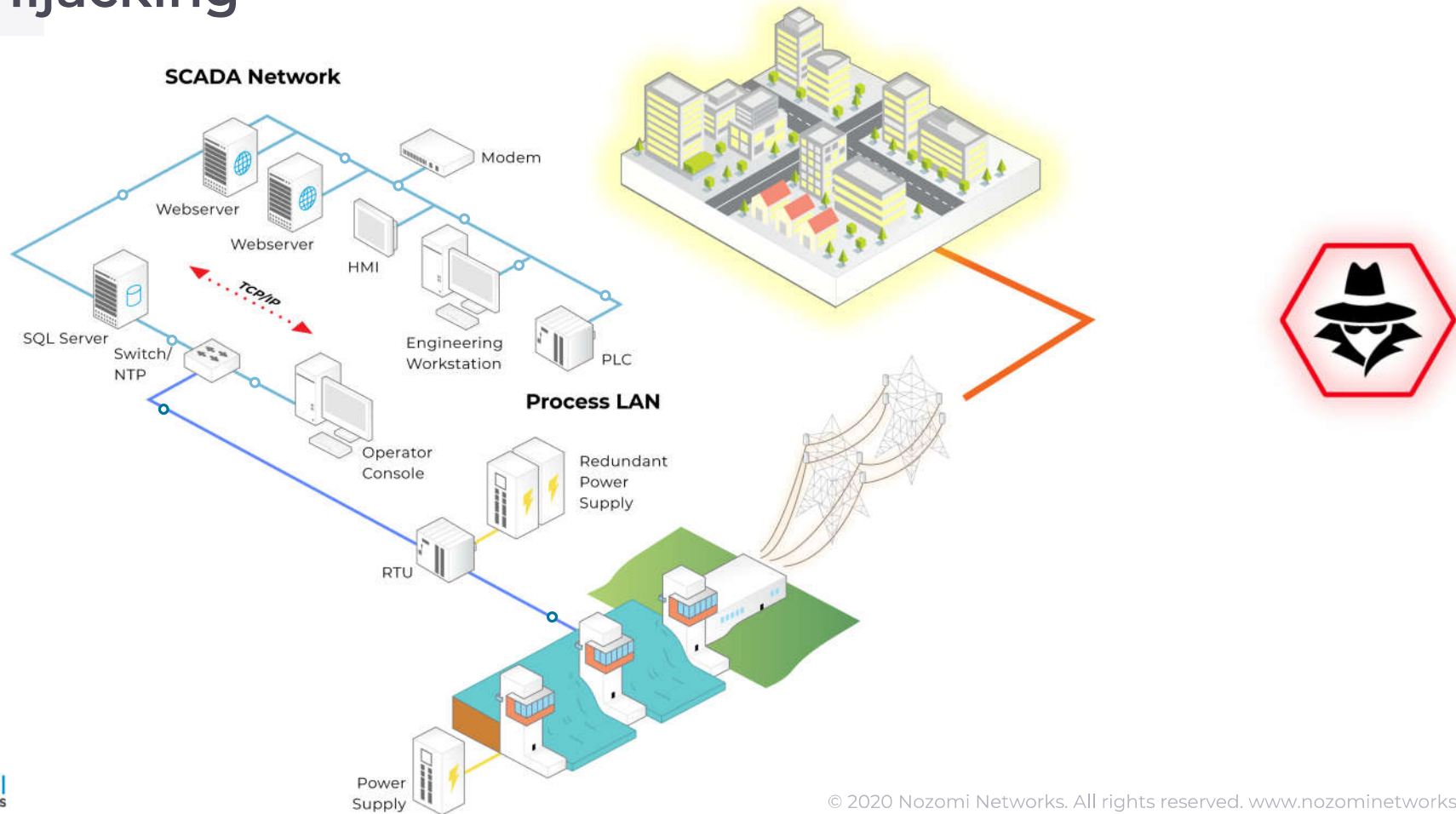
# Attack Scenario 1:

## NTP Hijacking



# Attack Scenario 1:

## NTP Hijacking

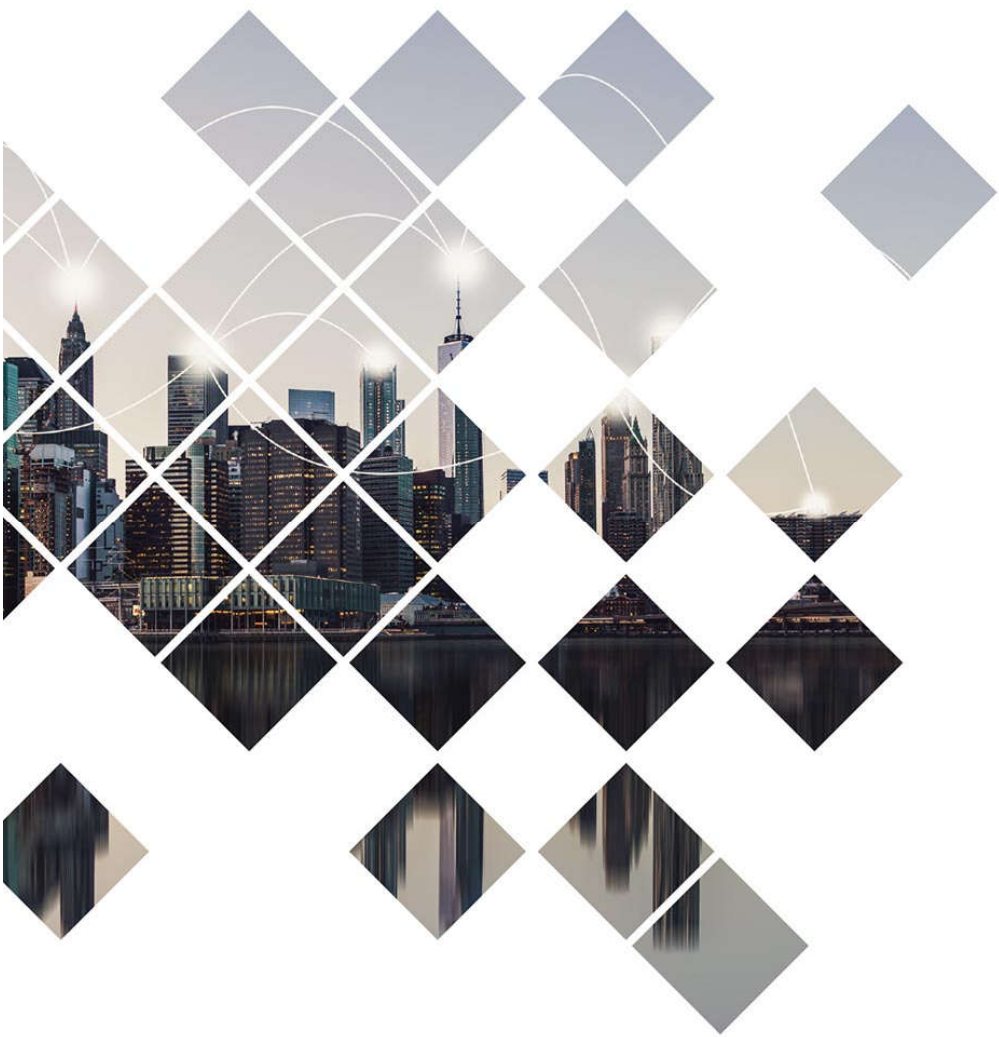




# Safeguarding Encryption in Action

## Test Cases

1. **Attack Scenario 1:**  
NTP Hijacking
2. **Attack Scenario 2:**  
Rogue CA Certificate



# Safeguarding Encryption in Action

## Test Cases

# (In)Secure Smart Grids: IEC 62351 - part 7

- Objects describing status of assets
- Several types of internal data (CPU, RAM, Certificates, ...)
- Improves threat and risk detection
- Real-world implementation
- Applies to worldwide Smart Grid technologies (SNMP, DNP3, IEC 61850, IEC 60870-5)





# (In)Secure Smart Grids: IEC 62351 - part 3

## Encryption and DPI

- DPI approach for encrypted communications
- Suggests implementations where the encrypted channels can be monitored
- These include:
  - Private Key Sharing
  - Proxy
  - Secure session-key sharing
  - And others



# (In)Secure Smart Grids: IEC 62351 - part 3

- Mandates the use of TLS encryption
- Establishes node and message authentication
- With IEC 62351-90-2, provides monitoring solutions for encrypted messages when Deep Packet Inspection (DPI) is required



# (In)Secure Smart Grids: IEC 62351

## IEC TC57 Working Group 15

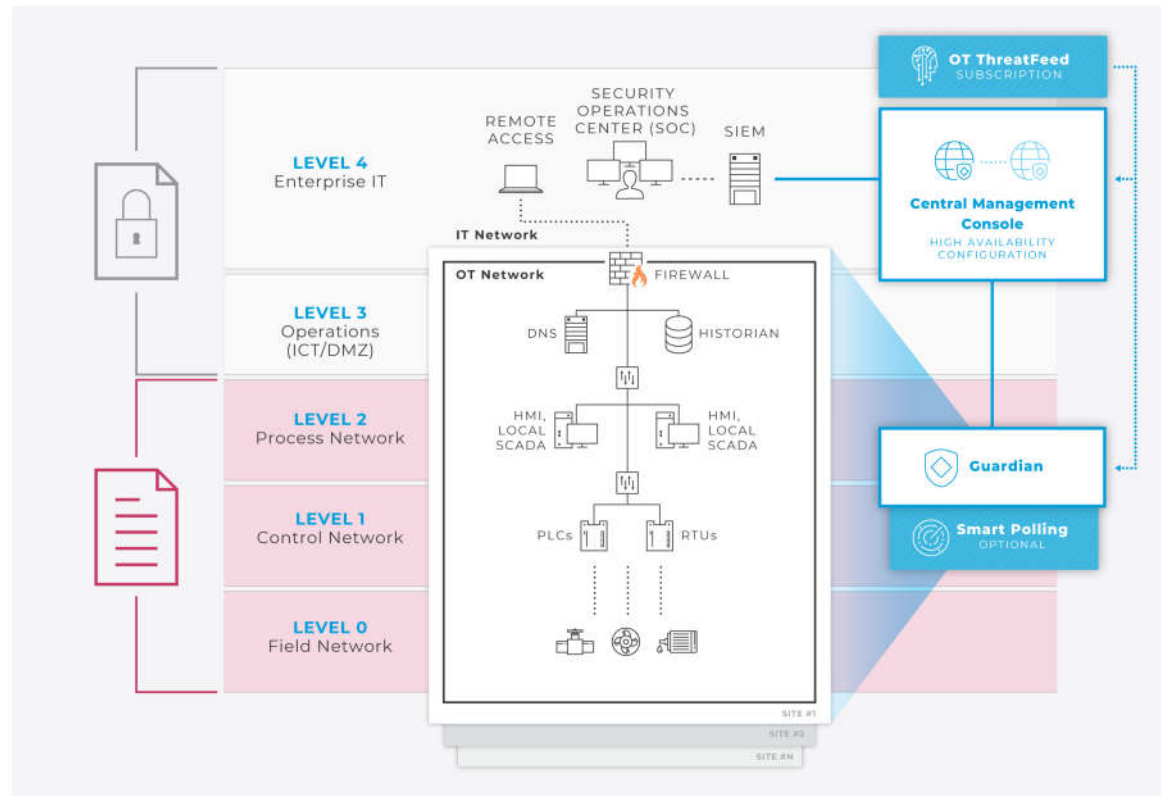
- Protocols have a critical role
- Advantages
- Improves security
- Introduces secure network channels
- Increases asset visibility



# Encryption in the OT World

## State of the art:

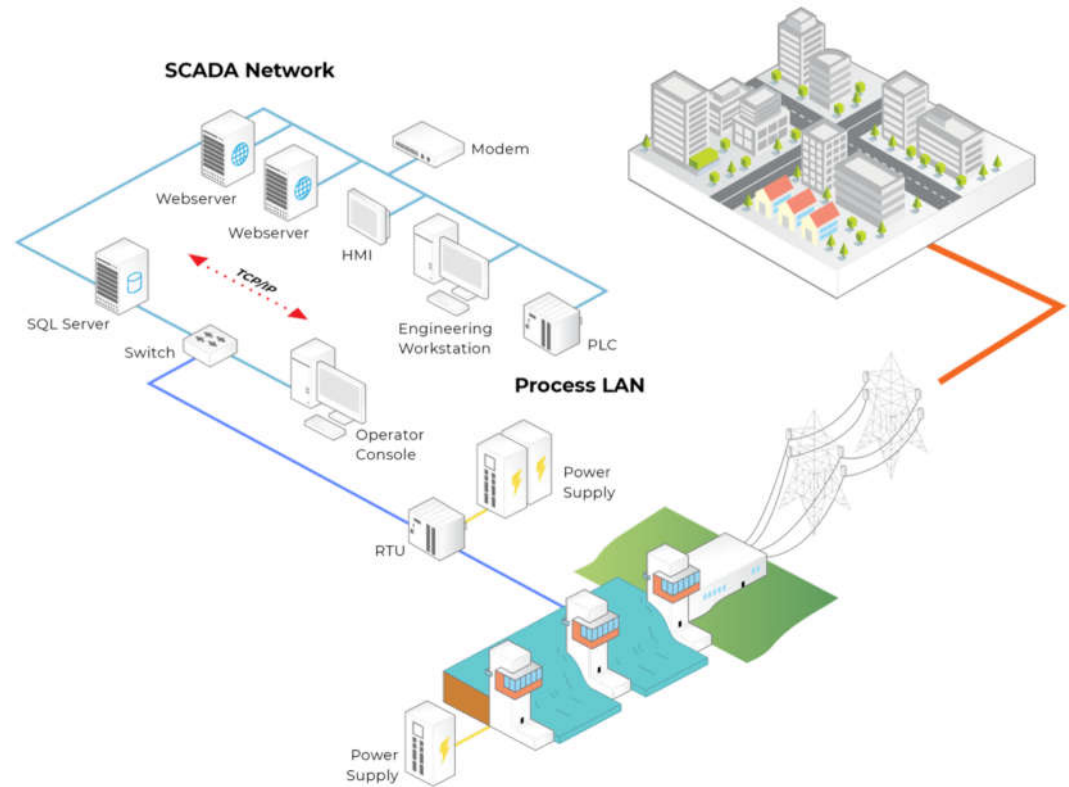
- Upper levels in Purdue already have encryption (OPC/UA, PI/OSIsoft)
  - Using classic TLS implementations
- Lower levels have almost no encryption at all. Some implementations include:
  - Secure ModBus (coming soon)
  - Step7CommPlus (Siemens)
  - IEC 62351 part 3



# Encryption Is Not the Norm

## Challenges:

- Additional operational overhead (e.g. protect the keys)
- OT protocol constraints (e.g. GOOSE, SV)
- Troubleshooting becomes more complex





# Agenda

## Line Up

- Encryption in the OT World
- IEC 62351- parts 3 and 7
- Attack Scenarios
  - Server NTP hijacking
  - Rogue CA certificate
- Future Threat Detection Landscape

# Nozomi Networks

**The Leading Solution  
for OT and IoT  
Security and Visibility**

## Industrial Strength OT and IoT Security and Visibility



Know what's on  
your network



Pinpoint cyber risks  
and threats



Unify security visibility  
across OT, IoT and IT

**REQUEST A DEMO**

# Who Are We?



Yiannis Stavrou

Security Researcher

[yiannis.stavrou@nozominetworks.com](mailto:yiannis.stavrou@nozominetworks.com)



Michael Dugent

Technical Operations Manager

[michael.dugent@nozominetworks.com](mailto:michael.dugent@nozominetworks.com)

- Cryptography, Malware Analysis
- ICS Reverse Engineering

- ICS Cyber Security – many years
- First-hand field experience - extensive



# Encryption in IT/OT/IoT Networks and How to Monitor Them

Yiannis Stavrou, Michael Dugent