

Opportunities in Industrial Cyber Security

UWTSD - Guest Lecture 29/11/2022

Daniel Lewis

Founder & Executive Chair, Awen Collective



<https://www.awencollective.com/>

Presenter: Daniel Lewis

Founder & Executive Chair., Awen Collective (2017-Present)

- Strategy, Direction, Marketing, R&D, Internationalisation
- Market & Tech

Previously...

- Senior Research Fellow @ USW - InfoSec (2015-2017)
- PhD Research @ University of Bristol - Intelligent Systems
- Software Engineering & Knowledge Engineering
- BSc(hons) Intelligent Systems & Software Engineering - Oxford Brookes (2007)



<https://www.linkedin.com/in/danieljohnlewis/>

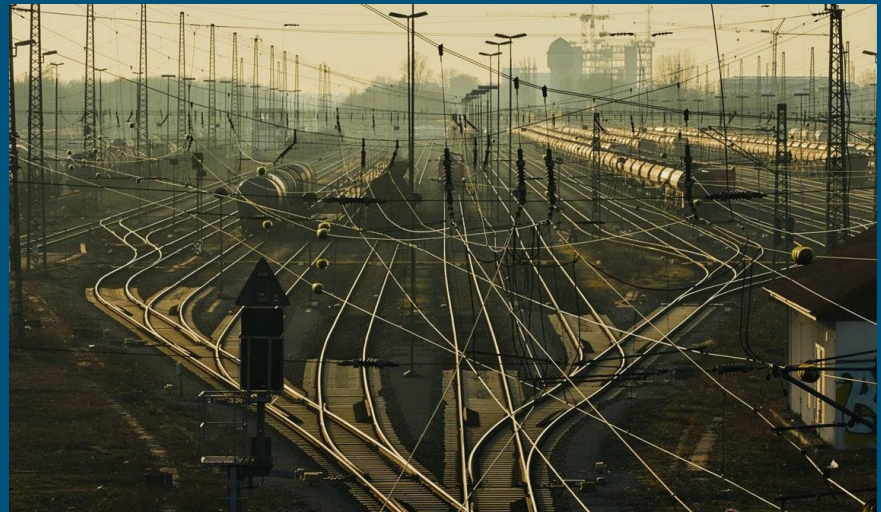
What makes
Operational
Technology a
target?

The Problem

Critical National Infrastructure (and manufacturing) is critical

Built on Operational Technologies (OT):

- Efficient
- Simple
- Engineering Managed
- Built to last
- Aging
- Vulnerable



<https://www.awencollective.com/>

What is Operational technology?

OT

OT, or Operational Technology, is any technology which provides “on-the-floor” operations. These are typically automation technologies, and includes:

SCADA

ICS / IACS / IPCS / DCS

IIoT

Industrial Robotics

<https://www.awencollective.com/kbase/item/ot-operational-technology>



Elmschrat, CC BY-SA 3.0, via Wikimedia Commons

OT Vendors



Logos are copyright their respective organisations, and are used without permission but with good intentions! Other brands are available.

Sectors

Critical National Infrastructure

- Energy:
 - Electricity
 - Oil & Gas
 - Civil Nuclear
- Transport:
 - Road
 - Rail
 - Aviation
- (Petro) Chemicals & Metals
- Defence
- Aerospace
- Healthcare
- Smart Cities

Manufacturing

- Automotive
- Pharmaceuticals
- Electrical, Electronics & Mechanical
- Food & Drink
- Pulp & Paper
- Clothing & Textiles
- Toys & Games
- Construction materials
- Packaging
- *and more*

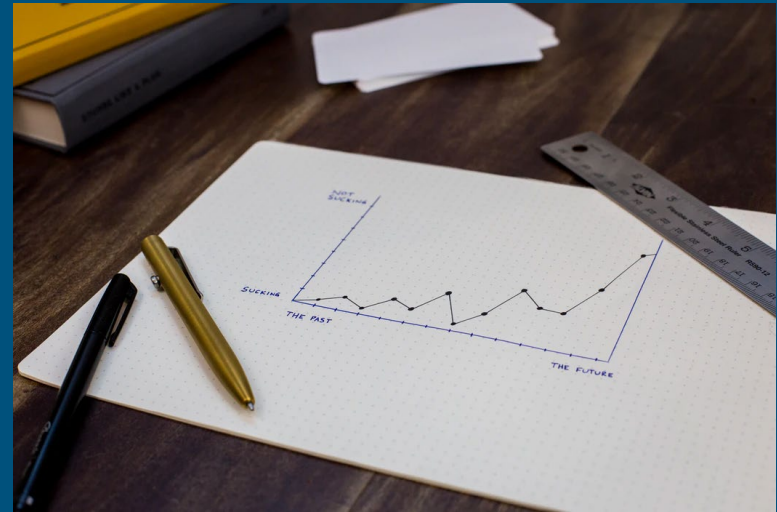
Terminology

- HMI - Human Machine Interface
- PLC - Programmable Logic Controller
- SCADA- Supervisory Control and Data Acquisition
- DCS- Distributed Control System
- Supervisory PC
- Historian - Operational logging

OT
is not
IT

OT is a (growing) niche in Cyber

- Majority of cyber products & services are in IT-based cyber
- OT Cyber is a growing problem
 - Lack of solutions
 - Lack of services
 - Lack of skills
- Easier to do Novel Research
- Hard to Develop
- Greater Reward



OT Cyber Attacks Case Studies

Stuxnet

Uncovered: 2010
Natanz, Iran
Nuclear Enrichment

- Used Windows Vulnerabilities
- Searched for Siemens STEP7 engineering software
- Caused physical damage

Havex

Uncovered: 2013

Target: energy, aviation, pharma,
defence, and petrochem

- EnergeticBear / Dragonfly
- Remote Access Trojan (RAT)
- OPC Protocol

BlackEnergy

Uncovered: 2007

Target: various

- Group: “Sandworm”
- Targeted HMIs
- BE2 in 2008/10
- BE3 in 2014
- Successful Blackouts in Ukraine in 2015

CrashOverride or Industroyer

Uncovered: 2016

Target: Ukraine Power Grid

- Involved 2 backdoors and a launcher
- Issued commands over OPC DA, IEC61850, IEC60870-5-104 & IEC60870-5-101
- Deleted registry keys to make it harder to recover
- Successful Blackouts in Ukraine in 2016

TRITON or TRISIS

Uncovered: 2017
Target: Petrochemical

- "World's most murderous malware"
- Disabled industrial safety systems:
 - Triconex by Schneider
- Shutdown a Saudi petrochemical facility

LockerGoga

March 2019
Norsk Hydro

EKANS

June 2020
Honda & Enel Group

86%

of Critical National Infrastructure organisations
have detected and experienced OT cyber attacks during
2020

Bridewell Consulting "CNI Cyber Report: Risk and Resilience"



<https://giphy.com/gifs/season-3-the-simpsons-3x5-l2Je6xTnSDh4dmA4o>

<https://www.awencollective.com/>

Post Incident

Severely Lacking!!!!

Increase skills in:

- Incident Readiness - inc. wargaming
- Incident Response Planning & Executing
- Digital Forensics for Operational Technologies (OT)

Some names:

- Fireye, ESET, Kaspersky

During Incident

Crowded Market!!!!

Industrial Intrusion Detection Systems:

- Nozomi Networks
- Clarity
- Dragos
- CyberX (or whatever Microsoft have renamed it to)

Industrial Firewalls:

- Cisco

Pre Incident

Standards Checking:

- [Awen Collective - Profile](#)



Asset & Vulnerability Checking:

- [Awen Collective - Dot](#)
- Langner OT-BASE
- Armis



Supporting the lifecycle of industrial cyber security



Note on Standards / Frameworks

- NCSC Cyber Assessment Framework (CAF)
- IEC 62443
- ISO 27001
- *and more related*

There we have it...

- The Problem
- What is OT
- OT is NOT IT
- Sectors
- Terminology
- Case Studies & We're all doomed
- Solution Space
- Standards



Daniel Lewis - Founder & Exec. Chair,
Awen Collective

<https://www.linkedin.com/in/danieljohnlewis/>

daniel@awencollective.com

<https://www.awencollective.com/>

QUESTIONS?