USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

CTO PEER MENTORING PROGRAM

FUNDAMENTALS OF OPERATIONAL TECHNOLOGY, CRITICAL INFRASTRUCTURE AND IT INTEGRATION CYBERSECURITY

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Fundamentals of Operational Technology, Critical Infrastructure and IT Integration Cybersecurity

OPERATIONAL TECHNOLOGY – WHAT IS IT?

"Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)"

NIST SP 800-37 Rev. 2

"Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

Gartner

OPERATIONAL TECHNOLOGY – WHAT IS IT?

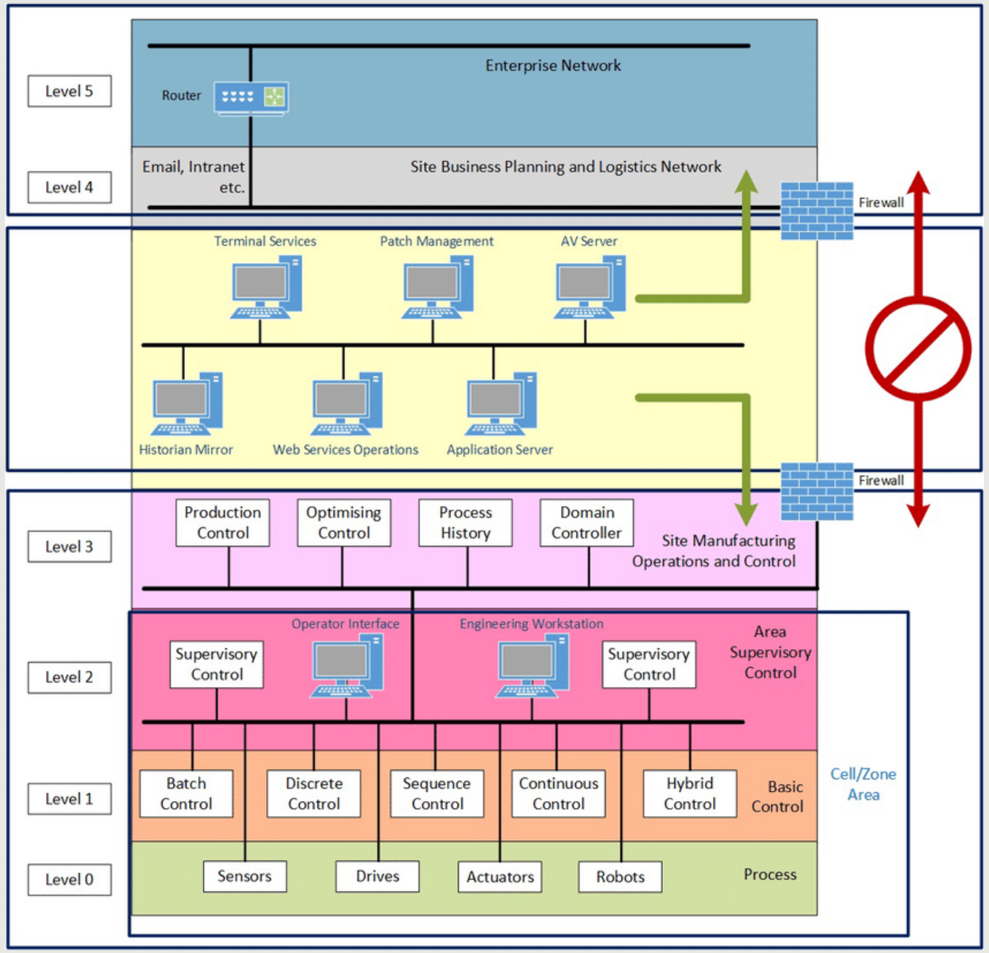
OPERATIONAL TECHNOLOGY – WHAT IS IT?

We all can think of good examples of Operational Technology. Often it is very clear that something is Operational Technology

When definitions are applied it sometime becomes difficult to determine where Operational Technology Stops and Information Technology Starts

Therefore we need to categorize or systems by function

OPERATIONAL TECHNOLOGY – THE PURDUE MODEL



The Purdue model can be found in a number of OT standards

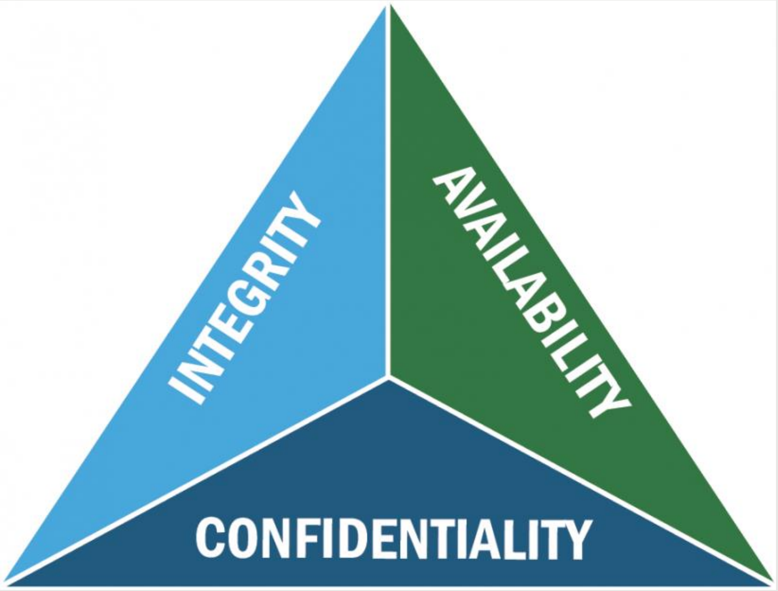
It helps us place our assets into logical levels

It allows us to understand where controls can be placed and understand where different use cases can lead to the traversal of these controls or provide a route for an actor move between those zones to reach their target.

OPERATIONAL TECHNOLOGY – HOW IS IT DIFFERENT

In many ways Operational Technology is very similar to Information Technology – We should not believe it can not be secured and that is too different to implement!

However, we must understand how our environments are different.



OPERATIONAL TECHNOLOGY – THE CIA TRIAD

Confidentiality, Integrity, Availability

Why is this order wrong for OT? It implies an order of importance – Often Availability and Integrity seem the most important in OT.

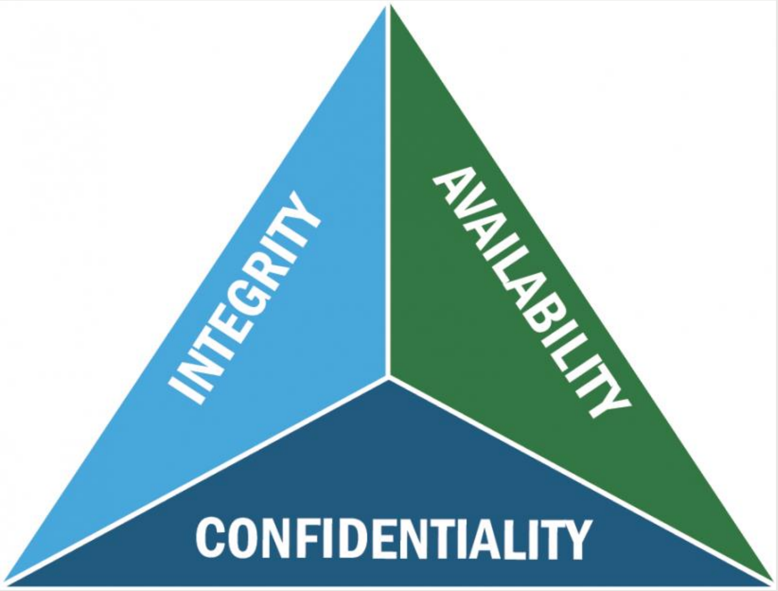
Think about your own processes, what is most important to you?

e.g.

If you have a safety critical system then Integrity is vital, and you would rather shut down than endanger life

If you run an electricity network then availability may be the most important

But all factors are important



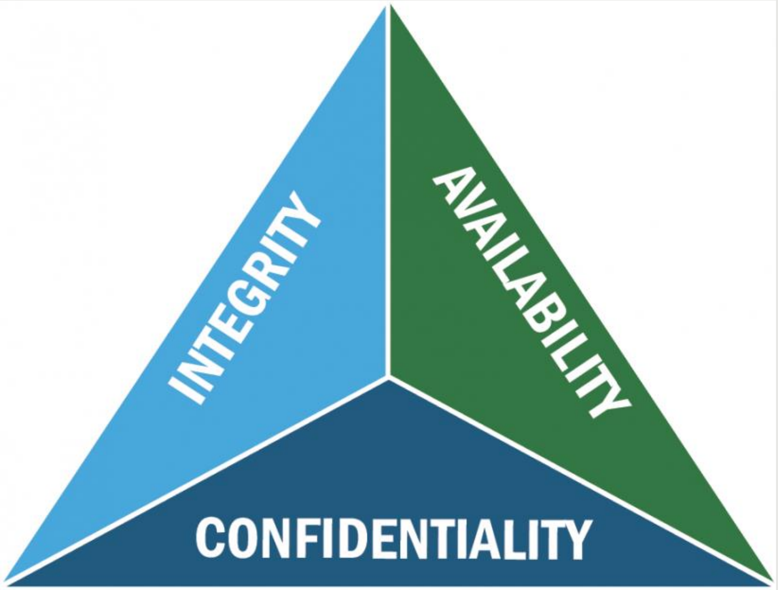
OPERATIONAL TECHNOLOGY – THE CIA TRIAD

What does confidentiality in OT mean?

It is often achieved through the careful handling of sensitive data rather than through encryption.

Encrypting traffic between a SCADA server and a PLC may not be practical or possible.

Traffic between locations should be protected, even if natively insecure. E.g. using a VPN tunnel. This is not to stop the loss of the data but to ensure trust in the source and destination.



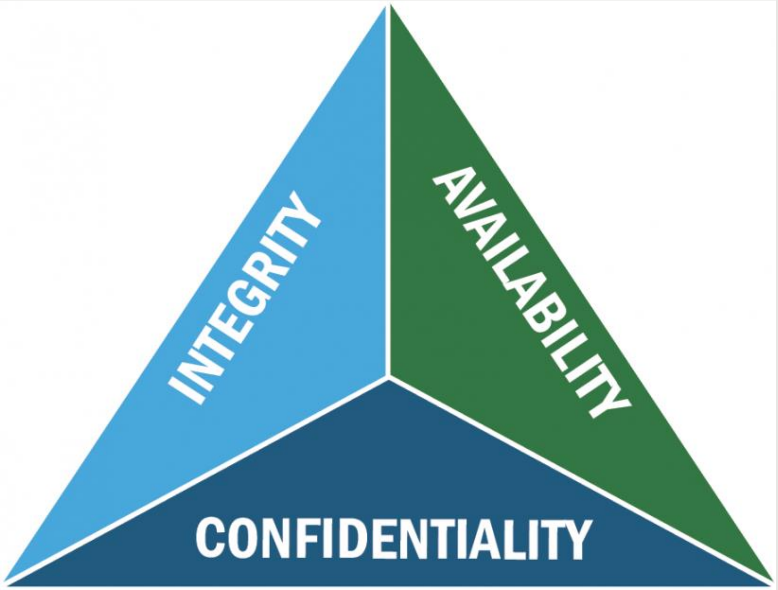
OPERATIONAL TECHNOLOGY – THE CIA TRIAD

What does confidentiality in OT mean?

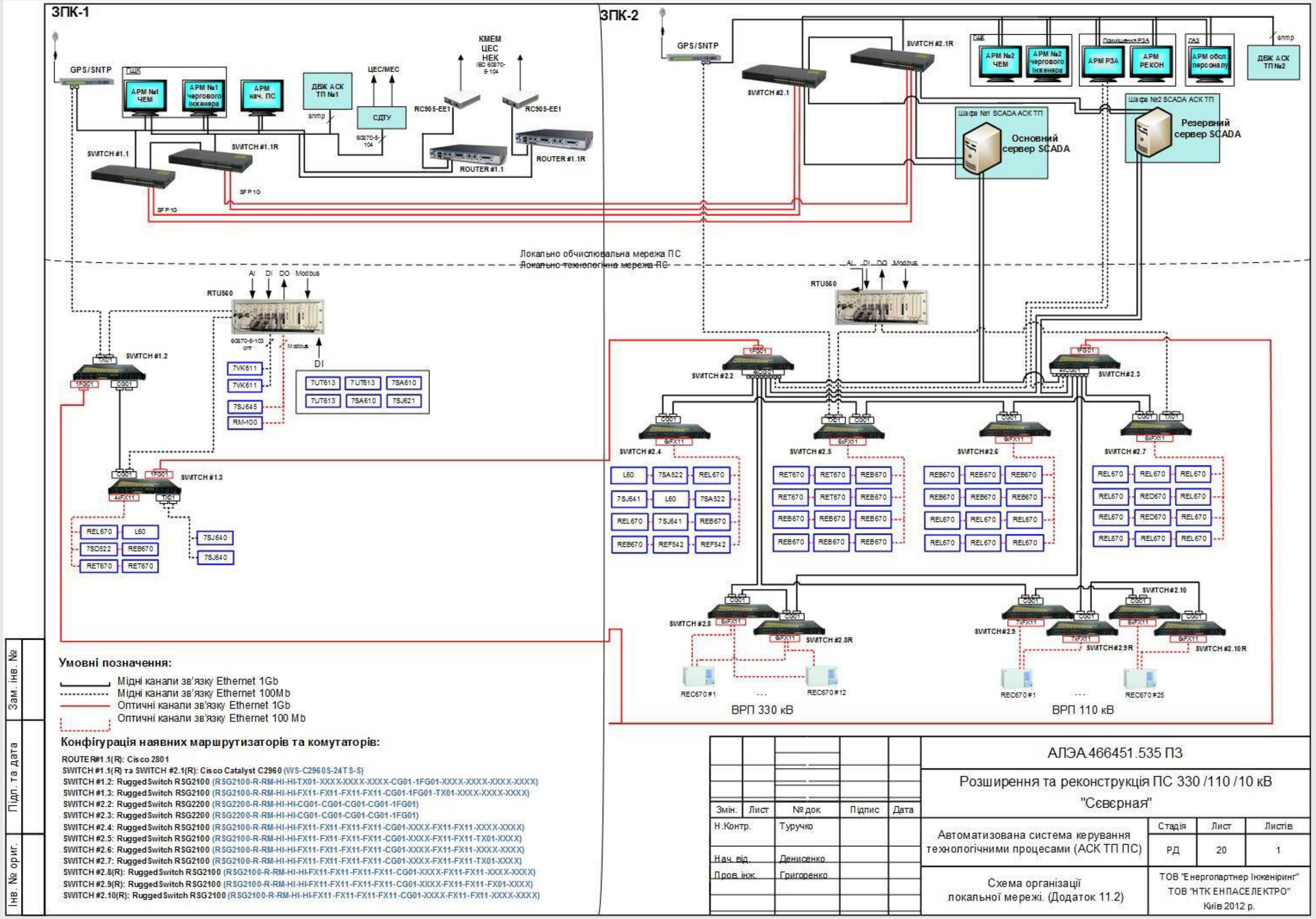
Protecting Confidentiality has do be done with people not just technology.

Attacking OT networks, especially where there is good defence in depth requires reconnaissance. It's not always possible to maintain persistence so crafted attacks mean understanding the target.

But…



OPERATIONAL TECHNOLOGY – ENSURING CONFIDENTIALITY



Умовні позначення:

▬	Мідні канали зв'язку Ethernet 1Gb
┄	Мідні канали зв'язку Ethernet 100Mb
🟥 ▬	Оптичні канали зв'язку Ethernet 1Gb
🟥 ┄	Оптичні канали зв'язку Ethernet 100 Mb

Конфігурація наявних маршрутизаторів та комутаторів:

ROUTER#1.1(R): Cisco 2801
SWITCH #1.1(R) та SWITCH #2.1(R): Cisco Catalyst C2960 (WS-C2960S-24TS-S)
SWITCH #1.2: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-TX01-XXXX-XXXX-XXXX-CG01-1FG01-XXXX-XXXX-XXXX-XXXX)
SWITCH #1.3: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-1FG01-TX01-XXXX-XXXX-XXXX)
SWITCH #2.2: RuggedSwitch RSG2200 (RSG2200-R-RM-HI-HI-CG01-CG01-CG01-CG01-1FG01)
SWITCH #2.3: RuggedSwitch RSG2200 (RSG2200-R-RM-HI-HI-CG01-CG01-CG01-CG01-1FG01)
SWITCH #2.4: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-XXXX-XXXX)
SWITCH #2.5: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-TX01-XXXX)
SWITCH #2.6: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-XXXX-XXXX)
SWITCH #2.7: RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-TX01-XXXX)
SWITCH #2.8(R): RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-XXXX-XXXX)
SWITCH #2.9(R): RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-FX01-XXXX)
SWITCH #2.10(R): RuggedSwitch RSG2100 (RSG2100-R-RM-HI-HI-FX11-FX11-FX11-FX11-CG01-XXXX-FX11-FX11-XXXX-XXXX)

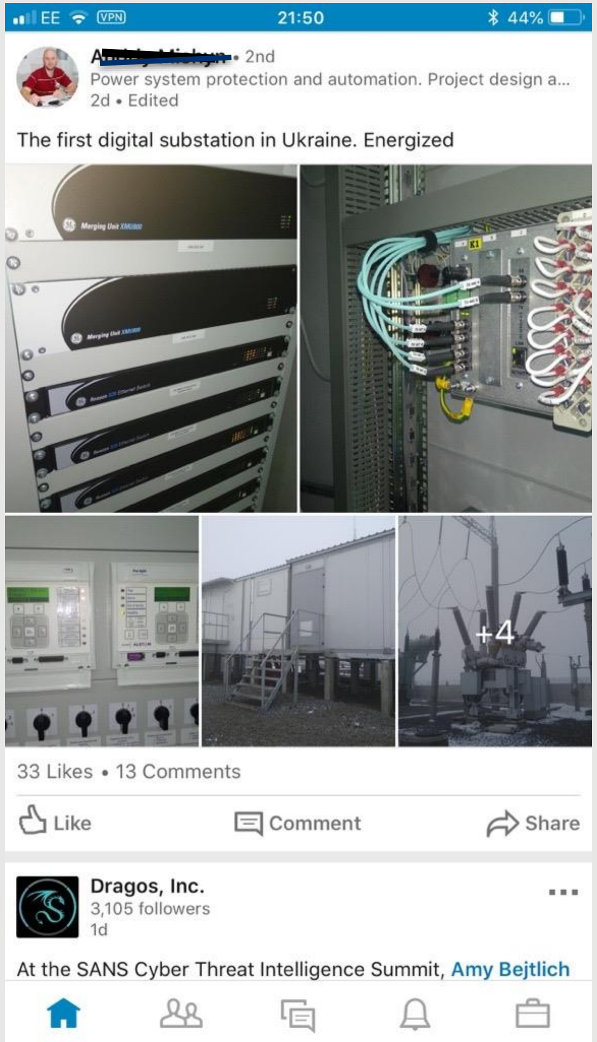
					АЛЭА 466451.535 ПЗ			
					Розширення та реконструкція ПС 330 /110 /10 кВ "Сєвєрная"			
Змін.	Лист	№ док	Підпис	Дата				
Н.Контр.		Туручко			Автоматизована система керування технологічними процесами (АСК ТП ПС)	Стадія	Лист	Листів
						РД	20	1
Нач. від.		Денисенко			Схема організації локальної мережі. (Додаток 11.2)	ТОВ "Енергопартнер Інженірииг" ТОВ "НТК ЕНПАСЕЛЕКТРО" Київ 2012 р.		
Пров. інж.		Григоренко						

Ensure Suppliers do not publish detailed information about the projects they deliver for you.

This level of information tells an attacker:

1. How to the environment is connected to the outside world.
2. How to navigate within the environment
3. The devices and software versions and their functions

OPERATIONAL TECHNOLOGY – ENSURING CONFIDENTIALITY



[redacted] • 2nd
Power system protection and automation. Project design a...
2d • Edited

The first digital substation in Ukraine. Energized

33 Likes • 13 Comments

Dragos, Inc.
3,105 followers
1d

At the SANS Cyber Threat Intelligence Summit, Amy Bejtlich

Ensure Staff don't overshare details of OT Projects

Often pride and the desire for recognition make social media a risky area

1. Vendors
2. Location
3. Even how the devices are connected to the Process Bus and Station Bus networks

IN SUMMARY

- Identify all of your assets – keep a robust inventory and hold it securely
- Discover your end to end architecture
- Look at where the data flows, how and why do people cross those boundaries
- Ensure robust separation of services
- Identify the controls you can implement in the OT environment and take gradual steps towards having equal controls in all areas

1. Ensure your OSINT programme includes checking for information about your OT assets
2. Make sure your staff are educated on the risks
3. Monitor for specific threats
4. Work Collaboratively, IT and Operational Engineering teams working together from the start!

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

THANK YOU