



Introduction to OT Security

Donavan Cheah

MYSTIKON 2022

SPONSORED BY |





MYSTIKO

Contents

- Introduction to OT Security
- The Purdue Model of OT Security
- IT-OT Convergence
- Can I use an IT Security Policy in OT Security?
- Revisiting Threat Models
- Revisiting "Defence-in-Depth"
- Supplementary: Revisiting Cyber Threat Intelligence
- Q & A

MYSTIKON 2022

SPONSORED BY |





MYSTIKO

The Obligatory Disclaimer

- This talk is a technical talk from my own personal capacity.
 - We will cover "how to think" about cybersecurity in the OT domain.
 - This talk will **not** cover specific commercial security products.
- The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of the presenter's current employer, Thales. Thales does not guarantee the accuracy or reliability of the information provided herein.

MYSTIKON 2022

SPONSORED BY |





MYSTIKO

whoami

- Senior cybersecurity consultant at Thales
 - From Government to boutique security consultancy to MNC
- Started out with Physics degree.
- A bunch of Offsec certifications (always improve oneself)
- Author of the digitalworld.local series of machines (Vulnhub)

MYSTIKON 2022

SPONSORED BY |

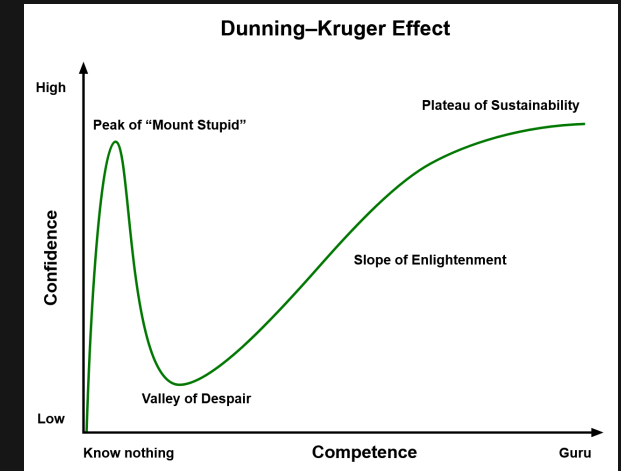




MYSTIKO

How to Approach Today's Talk

- Think about cybersecurity *beyond* the digital world.
 - Cybersecurity impact goes beyond "data exfiltration"
- Today's talk will not make you an expert in OT security.
 - **BUT...** it'll teach you how to *think* of OT security.



CAUTION!

Beware of the Dunning-Kruger Effect! Listening to ONE talk will not make you an OT cybersecurity expert!

https://upload.wikimedia.org/wikipedia/commons/4/46/Dunning%E2%80%93Kruger_Effect_01.svg

SPONSORED BY |



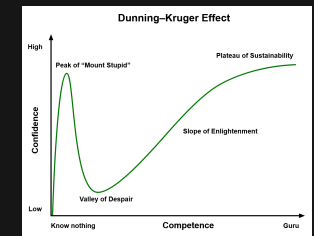


MYSTIKO

Example: Modbus

- Relatively "simple" protocol in the OT world: How much can we learn about it just by Googling?
 - Serial, but the TCP/IP implementation listens on TCP 502.
 - Packet structure is known on Wikipedia.
 - Serial implementation **cannot be encrypted** by default.

<https://modbus.org/>



modbus tcp/ip

About 6,530,000 results (0.48 seconds)

<https://www.rtautomation.com/technologies/modbus...>

Modbus TCP/IP Protocol Overview - Real Time Automation, Inc.

Modbus TCP/IP (sometimes referred to as the Modbus TCP protocol or just Modbus TCP) is a variant of the Modbus family of simple, vendor-neutral communication ...

Input registers: 16-bit quantity, provided by a... Input discretes: single bit, provided by an I...
Output registers: 16-bit quantity, alterable by ... Output discretes: single bit, alterable by an...

People also ask

What is a Modbus TCP IP?

Modbus TCP/IP (also Modbus-TCP) is simply **the Modbus RTU protocol with a TCP interface that runs on Ethernet**. The Modbus messaging structure is the application protocol that defines the rules for organizing and interpreting the data independent of the data transmission medium.

MYSTIKON 2022

SPONSORED BY |



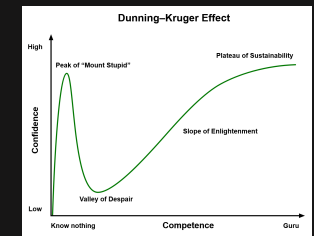


MYSTIKO

Example: Modbus

- Some simple Google searching on Modbus security might lead us to an OT OEM documenting the security risks of the protocol.
 - As the cybersecurity consultant, what will you advise a customer on the Modbus protocol?
 - Modbus/TCP?
 - Migrate to OPC UA?
 - Hybrid?

<https://control.com/technical-articles/security-decisions-in-modbus-systems/>




https://control.com/technical-articles/security-decisions-in-modbus-systems/

CONTROL AUTOMATION

ARTICLES FORUMS EDUCATION TOOLS VIDEOS DIRECTORY CONTROL AUTOMATION DAY

Modbus Security Issues

Modbus/Modbus TCP by itself exhibits many security problems due to a lack of a complete seven-layer OSI model that incorporates security in its design. Unauthorized access or communications errors can seriously compromise performance with disastrous results. Backdoors and exploits can allow bad actors to hack systems and cause misuse or failure of control.



These problems with Modbus are well understood, but it is useful to summarize them briefly here:

- Lack of message confidentiality
- No protocol intrinsic robust integrity checks on communications at higher layers
- Lack of standardized authentication
- Potential reliability issues of network communications

What do these security issues lead to?

The Consequences of Unsecured Systems

The lack of a formal session structure can open systems up to the possibility of injected command messages. For example, an attacker can send an illegal command into a system, and the Modbus slave devices may return an illegal function exception message. Detection of this return tells the attacker a control system is present, enabling reconnaissance. Likewise, illegal address exception responses generated for queries that contain an illegal slave address can help an attacker gather more information about the target.

Several potential mechanisms allow for a denial of service (DoS) attack, so Modbus systems have been adopting newer standards that resolve such problems.

The need to focus on cybersecurity would seem obvious but when is the effort misspent and how much is too much?


The nature of the Modbus network infrastructure already in place but decisions are complicated by the degree of investment an owner is prepared to commit to change. A half-baked system is almost as bad as no system at all.

However, if the system is a straight out simple serial interface Modbus RTU (Remote Terminal Unit) or the four-layer TCP-Modbus that incorporates ethernet frame encapsulation, significant improvement is required. If someone is unable or unprepared to make the necessary investment, it makes sense to consider if Modbus is the right choice going forward.

What are our options?

MOORE'S LOBBY PODCAST
Passing Storm or New Normal? ...

FEATURED RESOURCE



WHITE PAPERS

Customizing Machine Control for Flexible, Real-Time Production Improvements

Explore a single software solution comprised of 5 unique, yet commonly related applications to provide flexibility and process improvement at a moment's notice.

Download PDF ↓

SPONSORED BY |

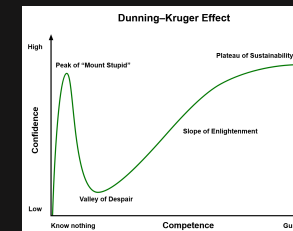




MYSTIKO

Example: Modbus

- Bad news: the OT world is full of protocols such as these.
 - Much time will be spent reading and asking operational questions.
 - Googling alone will not make one an OT cybersecurity hero.
- We must "Try Harder".



MYSTIKON 2022

SPONSORED BY |





Introduction to OT Security

- Questions:
 - What are the differences in IT and OT security?
 - Does the CIA model still apply?
 - Why did I mention the Dunning-Kruger Effect?
 - Why is OT Security so difficult?

MYSTIKON 2022

SPONSORED BY |





Introduction to OT Security

- IT security: *information* technology
- OT security: *operational* technology
- IT and OT used to be separate, but synergies result in them being integrated today.
 - E.g. 1: Data analytics in IT environment to optimise OT systems
 - E.g. 2: Remote management of OT equipment through remote solutions in IT environment (*why?*)





Revisiting "CIA" in OT Security

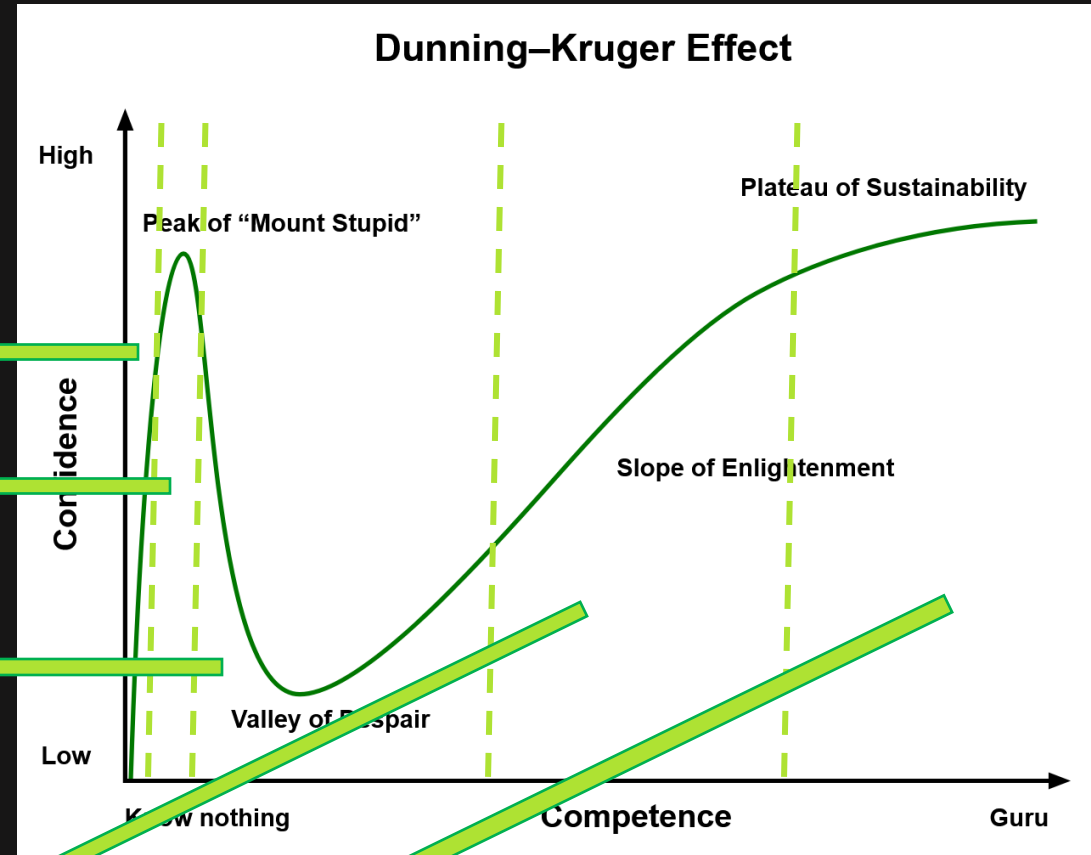
- In IT security:
 - Confidentiality, integrity are often important, whereas availability is not always time-sensitive.
- In OT security:
 - Availability is expected. (E.g. we expect power plants to operate *without interruption*)
 - How about confidentiality and integrity?





"Mount Stupid"

- Stage 1: I know nothing.
- Stage 2: Oh, it's just another routine cybersecurity task, just with different standards (IEC 62443). Just comply!
- Stage 3: I realised, I know nothing, and I keep being perceived as a "copy and paste" consultant! Time to ask the domain experts lots of questions so that I know something about their operations!
- Stage 4: I think I am getting the hang of it. I know enough about the operations to contribute positively to their cybersecurity without being seen as a roadblock
- Stage 5: Finally, I have made it! I'm now useful in that domain of OT!





MYSTIKO

The Importance of Domain Expertise

- In IT security: cybersecurity supports business.
 - Generally well-understood and well-documented by the Internet
- In OT security: cybersecurity supports operations.
 - Operations are not always well-documented
 - Proprietary protocols everywhere!
 - Operations in OT security often affect **lives**.
 - This isn't just restoring VM snapshots or rebuilding an AD...

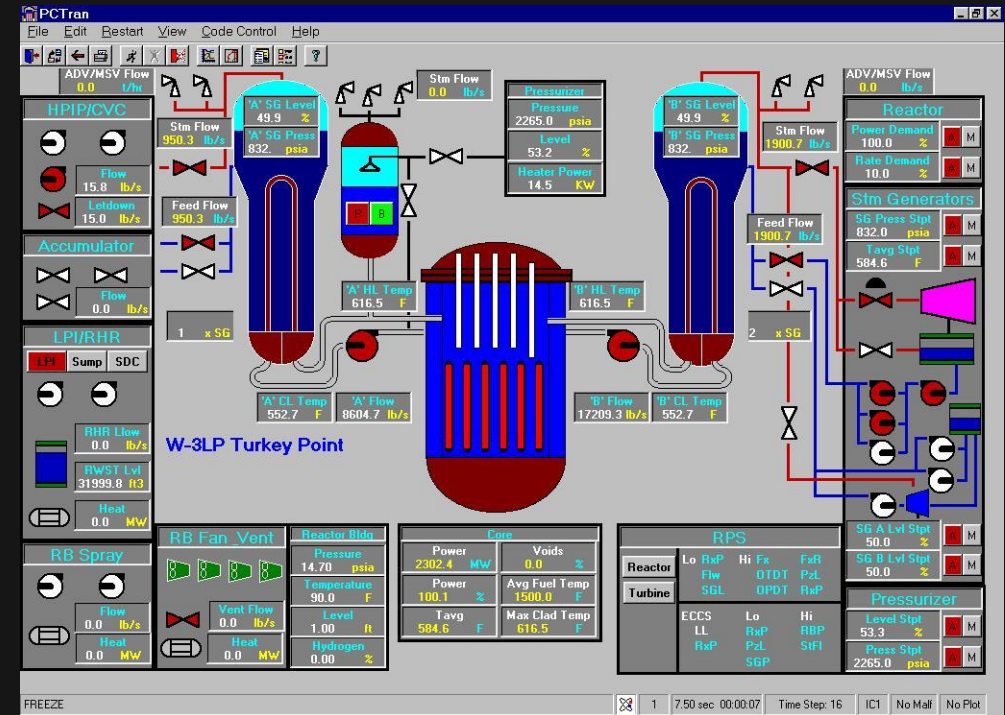
MYSTIKON 2022

SPONSORED BY |



The Purdue Model of OT Security

- Questions:
 - What is the most generic possible architecture that illustrates a proper OT system?
 - Why is this architecture a useful reference architecture?

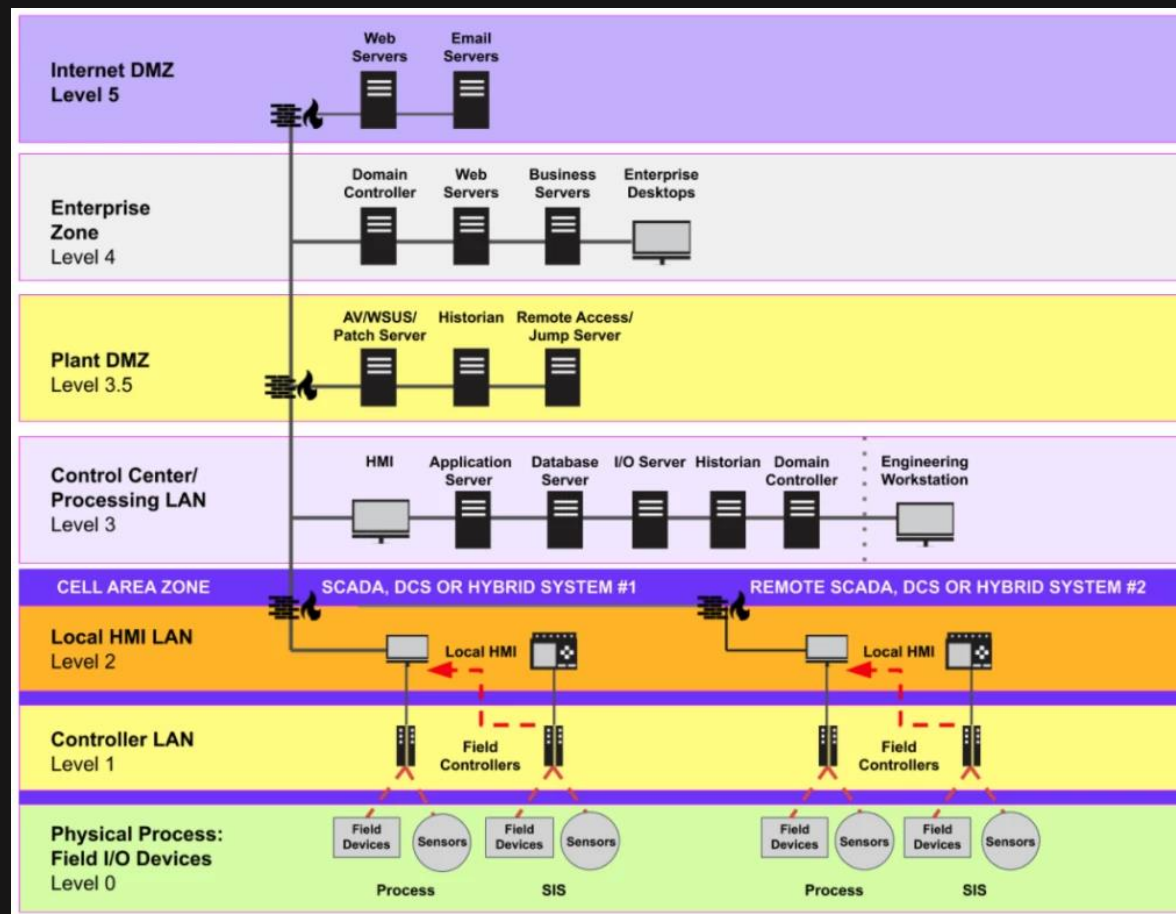


How do we secure a nuclear power plant?
<http://www.microsimtech.com/pctran/tkpt.jpg>



MYSTIKO

The Purdue Model of OT Security



Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>





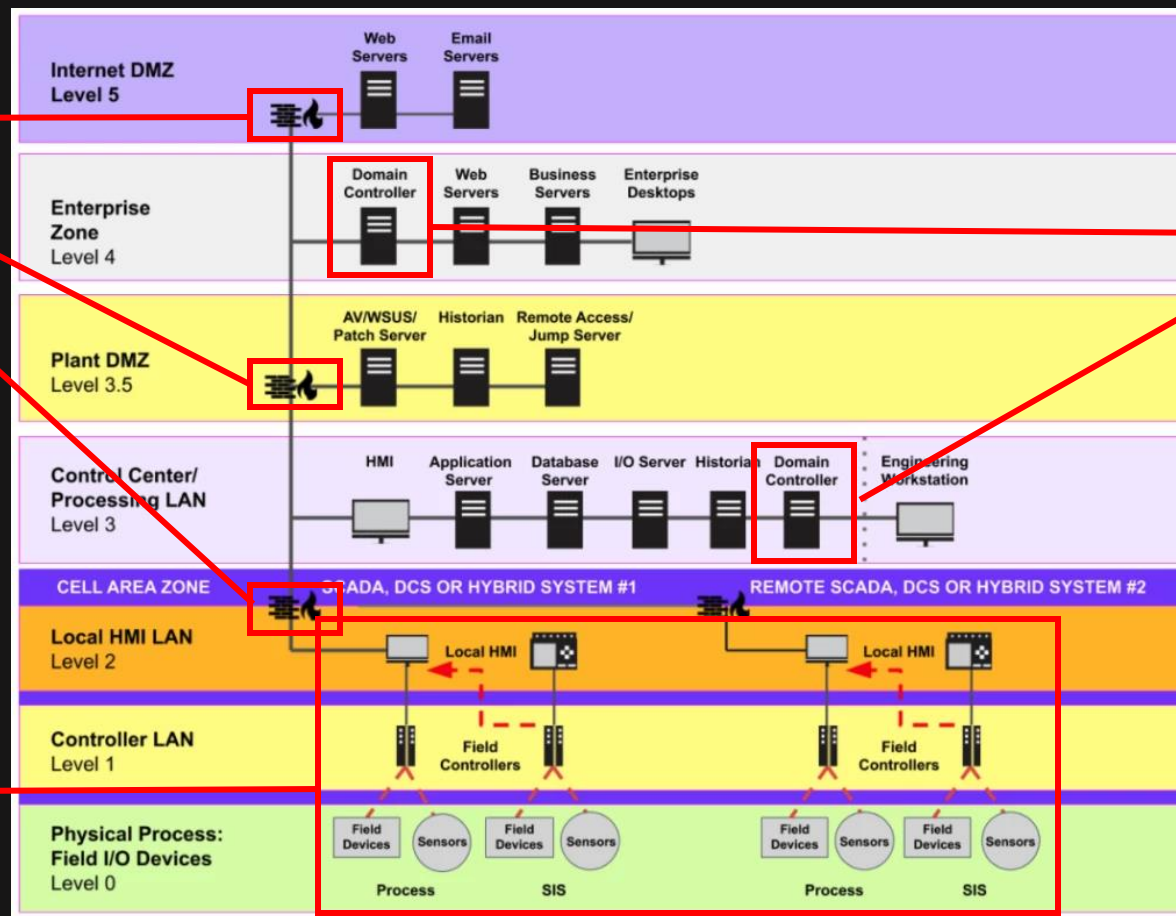
MYSTIKO

The Purdue Model of OT Security

Design consideration: segregation between layers

Design consideration: separate DC for IT and OT networks

Often OEM-supplied, black boxes to customers



Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>





MYSTIKO

IT-OT Convergence

- Questions:
 - What are some examples of systems traversing IT and OT networks?
 - What new security risks have manifested?

MYSTIKON 2022

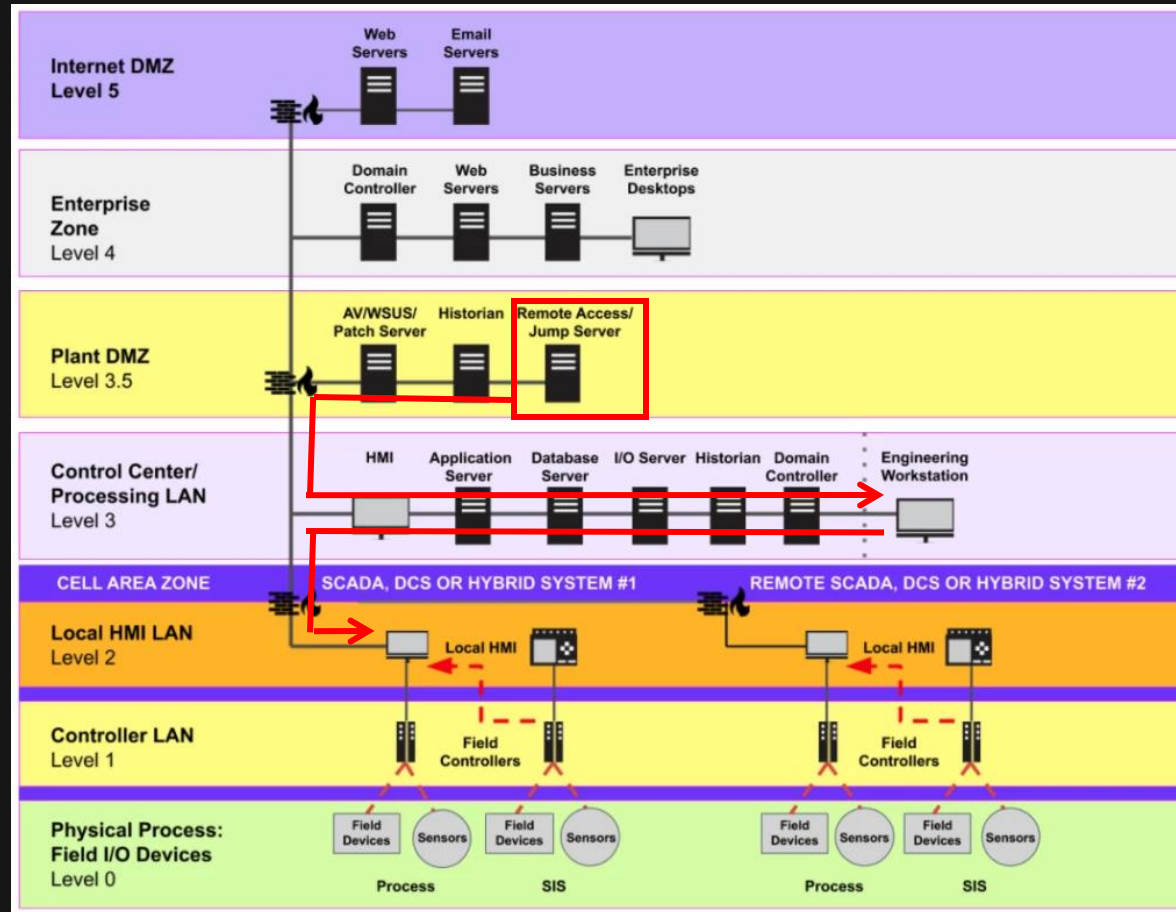
SPONSORED BY |





MYSTIKO

Are the IT and OT World "Convergent"?



RDP into Jump Server, pivot to Engineering Workstation, manage HMI.

Send data to servers in L3 and beyond for data analytics

Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>



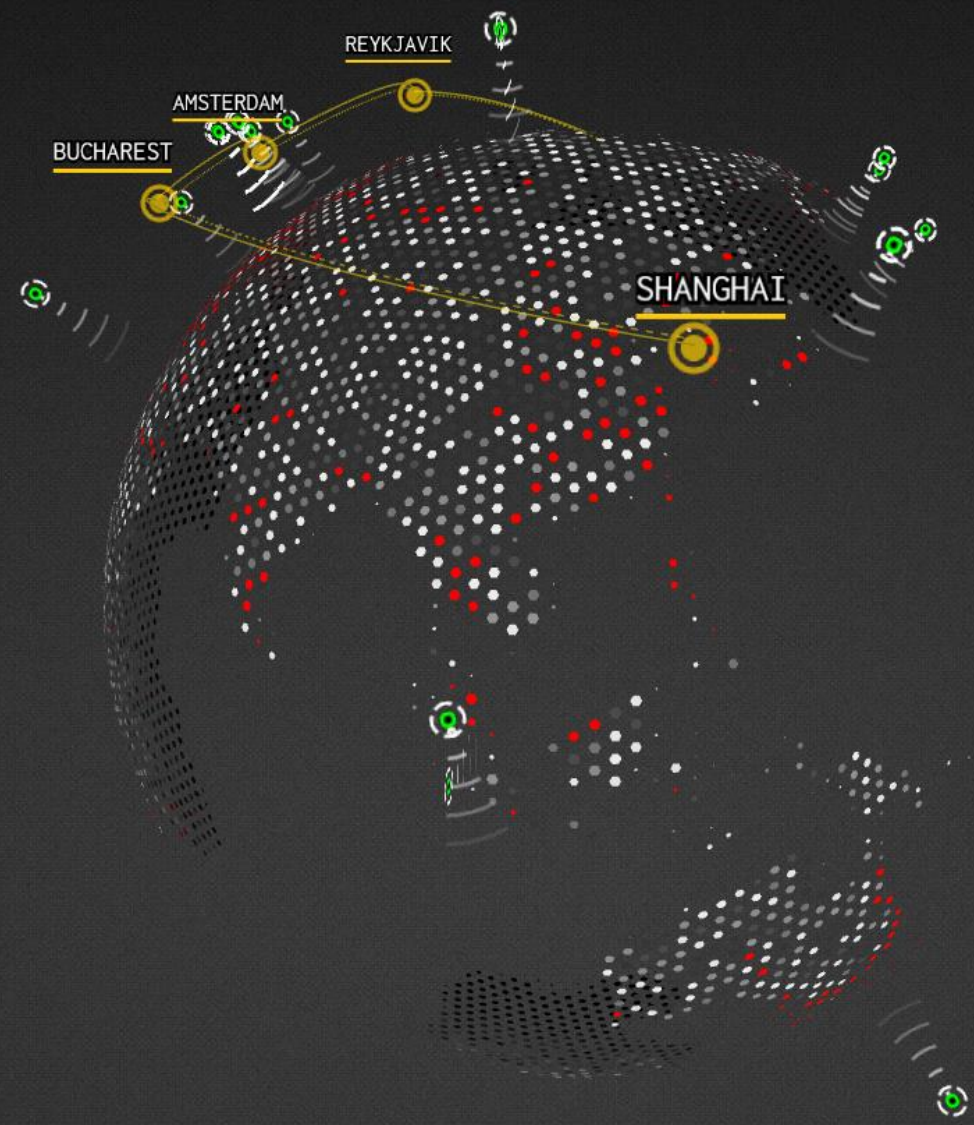
SHODAN ICS Radar

Protocols

BACnet: **10,530**
DNP3: **588**
EtherNet/IP: **3,943**
Modbus: **13,949**
Niagara Fox: **23,294**
Niagara Fox with SSL: **159**
Siemens S7: **2,701**

About

The Shodan search engine has started to crawl the Internet for protocols that provide raw, direct access to industrial control systems (ICS). This visualization shows the location of these industrial control systems on the Internet as well as other related data.



Legend

- ICS device
- Shodan crawler
- ⊗ Honeypot

Contact

For all inquiries relating to Shodan or the ICS Radar please contact:
support@shodan.io
Twitter: @shodanhq

Share

[Tweet](#)

[Share](#)



Internet-Connected OT Systems

- However, OT systems were never really designed for IT-OT convergence.

<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/>

https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/

What Makes OT Systems So Vulnerable To Attacks?

A number of reasons make OT/ICS environments vulnerable:

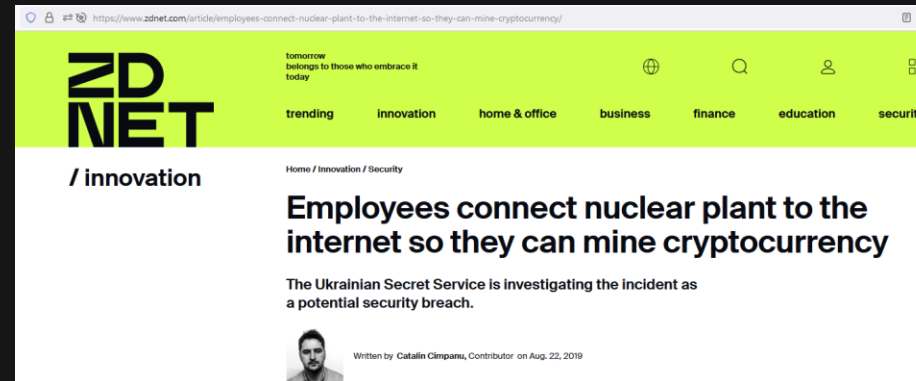
- **Aging technology:** Many OT systems were built decades ago when most devices were air-gapped and nobody was too concerned about cybersecurity, encryption or authentication. It is estimated that **71%** of systems have outdated or unsupported operating systems, 66% have no automatic updates, and 64% have unencrypted passwords.
- **Difficult or infrequent patching:** While **65%** of vulnerabilities have a patch available, it is extremely difficult for organizations to patch systems regularly due to the associated risk of downtime. Most critical infrastructure and ICS environments operate round the clock; they cannot be taken offline) or cannot risk applying untested patches that may have downstream ecosystem impacts or potential to disrupt the overall system.
- **Inherent vulnerabilities:** The number of reported vulnerabilities in ICS environments is **doubling** every year.
- **Remotely exploitable:** Almost **70%** of all operational environments have one or more remote access or external connections to third parties like internet providers, service providers and others.
- **Weak passwords:** OT devices lack strong authentication, and credentials can easily be guessed or brute forced by cybercriminals. Earlier this year, the CISA warned that cybercriminals were gaining access to internet-exposed **UPS** devices through unchanged default usernames and passwords.
- **Limited security resources:** **47%** of ICS organizations do not have an internal team dedicated 24x7 to managing OT/ICS incidents. There is also a lack of alignment between IT and OT security teams.





Internet-Connected OT Systems

- Sometimes, we have cheeky insiders too...



References:

<https://www.zdnet.com/article/employees-connect-nuclear-plant-to-the-internet-so-they-can-mine-cryptocurrency/>



Can I Use an IT Security Policy in OT Security?

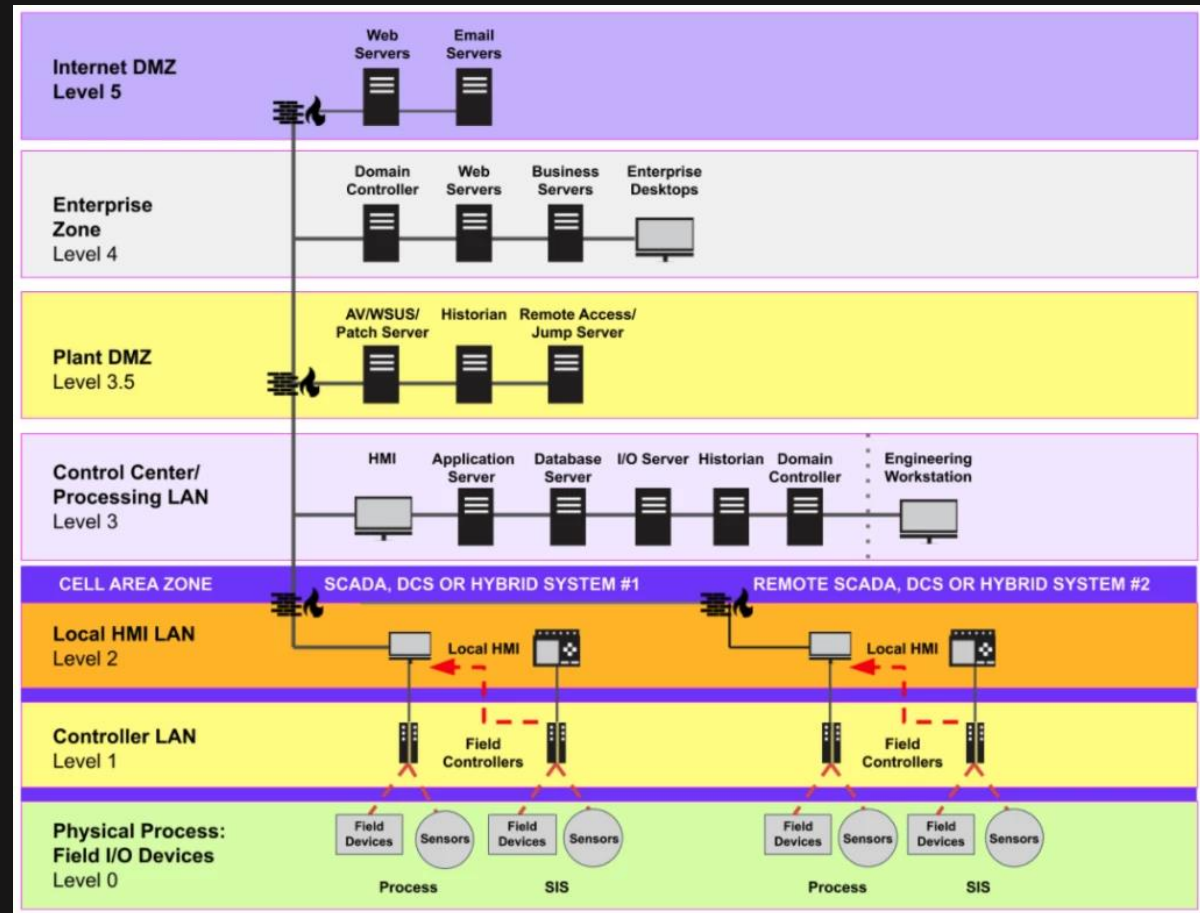
- Considerations:
 - What is the objective of an IT security policy?
 - What is the objective of an OT security policy?
 - Are the objectives the same?



MYSTIKO

Recall: Purdue Model

- What are the "crown jewels" in the IT and OT worlds?
- What does it take to ensure the "crown jewels" remain secure?



Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>

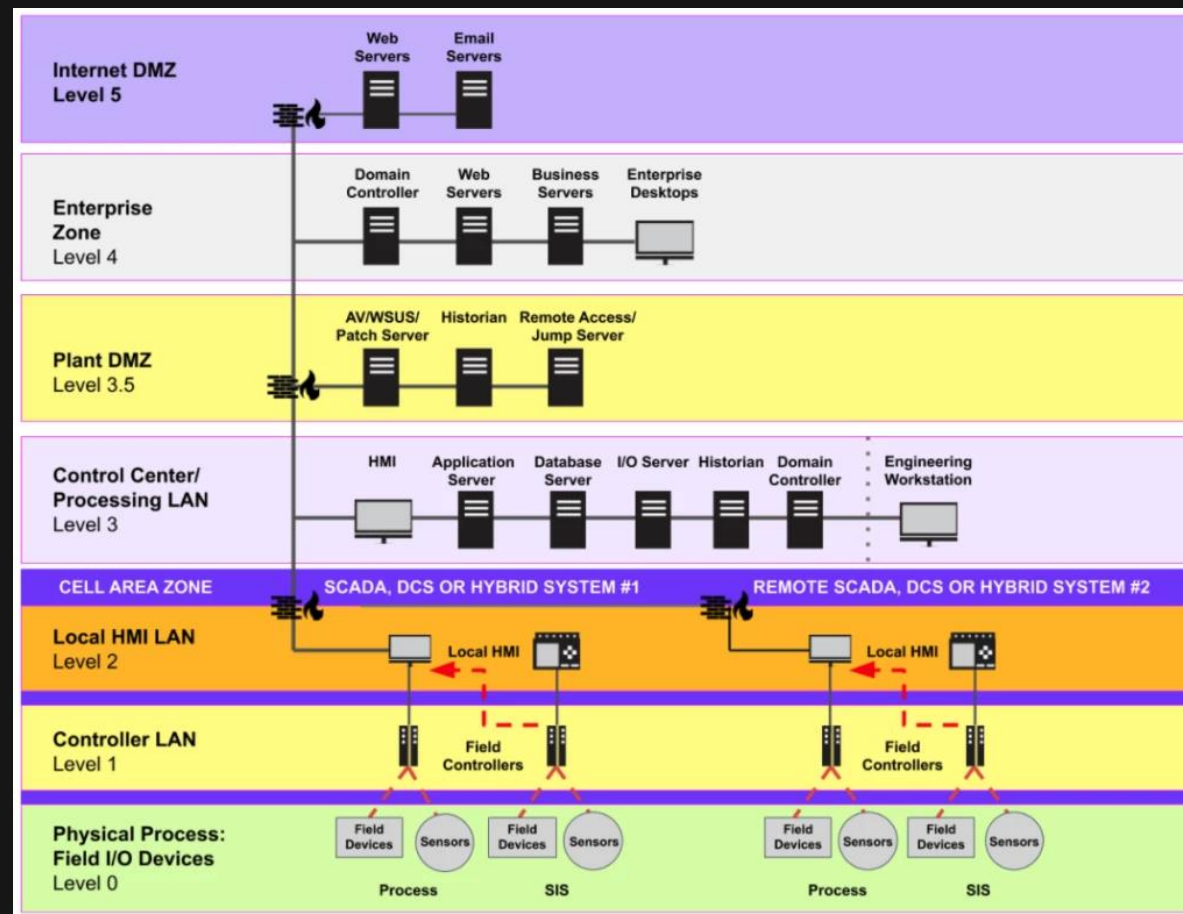




MYSTIKO

IT-OT "Divergence"

- IT world: data is most important
- OT world: operations are most important



Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>





MYSTIKO

OT Constraints

- User centricity: can we tolerate an OT system going "unavailable"?
 - What are some of these consequences towards cybersecurity in OT systems?
- Diversity of OT systems: requirement of different standards!
 - E.g. IEC 62443, in railway CENELEC 50701.

Source: <https://claroty.com/blog/how-the-purdue-model-enables-industrial-operational-resilience>

SPONSORED BY |



MYSTIKON 2022

Revisiting Threat Models

- Questions:
 - What do I have that constitutes the attack surface?
 - Do attacks come from the IT network, or the OT network?
 - What should I tell my C-suite on a risk assessment?



Bill of Material (BOM)

- Recall NIST's "IPDRR" framework.
 - Identification is the first step.
- Identify all components through a BOM.
 - Use BOM as a basis to understand possible threats that can arise.





Revisiting Threat Models: STRIDE-LM

STRIDE-LM Property	Description
Spoofing	Impersonating another user or system component to obtain its access to the system
Tampering	Altering the system or data in some way that makes it less useful to the intended users
Repudiation	Plausible deniability of actions taken under a given user or process
Information Disclosure	Release of information to unauthorized parties (e.g., a data breach)
Denial of Service	Making the system unavailable to the intended users
Elevation of Privilege	Granting a user or process additional access to the system without authorization
Lateral Movement	Expanding control over the target network beyond the initial point of compromise.

<https://csf.tools/reference/stride-lm/>





MYSTIKO

Revisiting Threat Models: Security Properties

STRIDE-LM Property	Description	Security Property
Spoofing	Impersonating another user or system component to obtain its access to the system	Authenticity
Tampering	Altering the system or data in some way that makes it less useful to the intended users	Integrity
Repudiation	Plausible deniability of actions taken under a given user or process	Non-repudiability
Information Disclosure	Release of information to unauthorized parties (e.g., a data breach)	Confidentiality
Denial of Service	Making the system unavailable to the intended users	Availability
Elevation of Privilege	Granting a user or process additional access to the system without authorization	Authorisation
Lateral Movement	Expanding control over the target network beyond the initial point of compromise.	Multiple

Which properties are most important for an OT system?

<https://csf.tools/reference/stride-lm/>

MYSTIKON 2022

SPONSORED BY |





MYSTIKO

Revisiting Threat Models: MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise						Wireless Sniffing	Modify Alarm Settings			Manipulation of Control	
Transient Cyber Asset									Manipulation of View		
Wireless Compromise									Theft of Operational Information		

This is the ICS equivalent for the MITRE ATT&CK Framework, as compared to the one we are always familiar with! What's the difference?

https://collaborate.mitre.org/attackics/index.php/main_Page

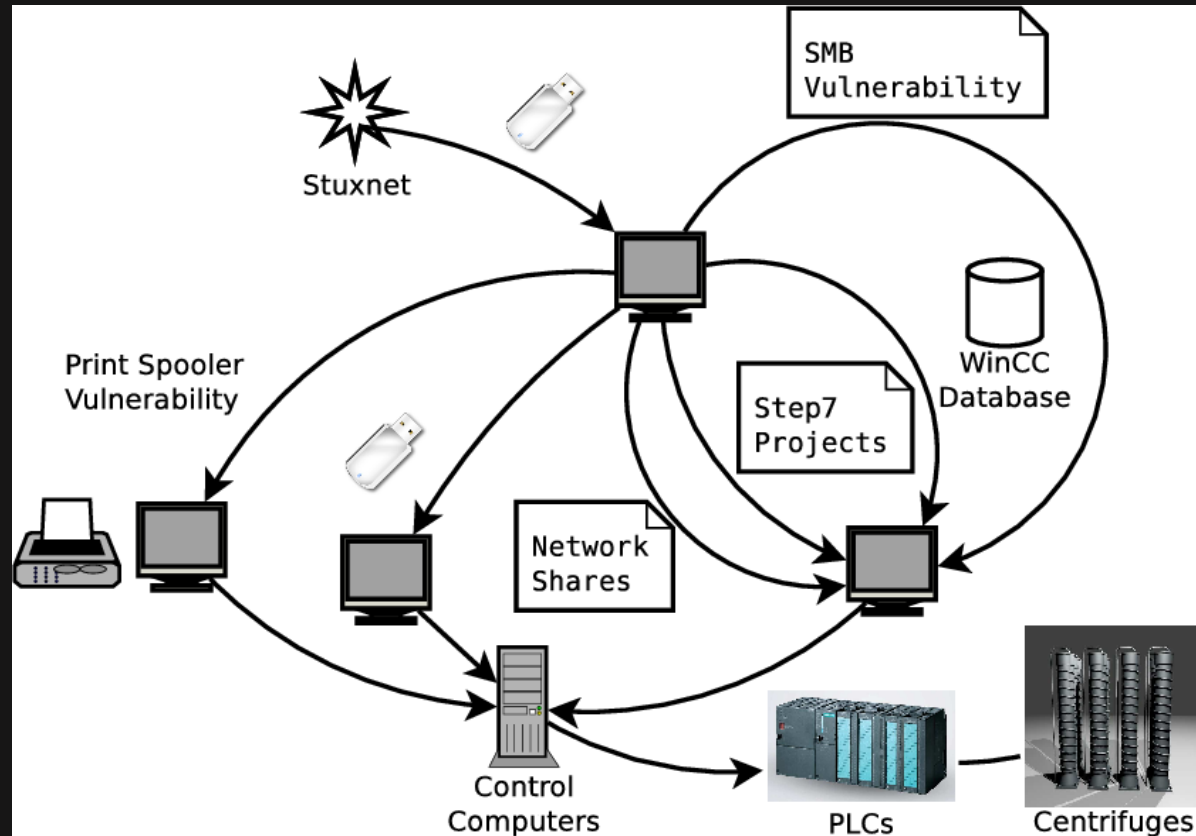
SPONSORED BY |





MYSTIKO

Example: Stuxnet



<https://www.semanticscholar.org/paper/The-Stuxnet-Worm-Mueller/1501b8b7da65c8fc15846bd67765db735b23cda8/figure/3>

SPONSORED BY |



MYSTIKON 2022



MYSTIKO

Revisiting the OT System Landscape

- Questions: with the attack surface of OT systems now incorporating IT systems, but with OT system weaknesses, what is the threat model now?

<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/>

<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/>

What Makes OT Systems So Vulnerable To Attacks?

A number of reasons make OT/ICS environments vulnerable:

- **Aging technology:** Many OT systems were built decades ago when most devices were air-gapped and nobody was too concerned about cybersecurity, encryption or authentication. It is estimated that **71%** of systems have outdated or unsupported operating systems, 66% have no automatic updates, and 64% have unencrypted passwords.
- **Difficult or infrequent patching:** While **65%** of vulnerabilities have a patch available, it is extremely difficult for organizations to patch systems regularly due to the associated risk of downtime. Most critical infrastructure and ICS environments operate round the clock; they cannot be taken offline) or cannot risk applying untested patches that may have downstream ecosystem impacts or potential to disrupt the overall system.
- **Inherent vulnerabilities:** The number of reported vulnerabilities in ICS environments is **doubling** every year.
- **Remotely exploitable:** Almost **70%** of all operational environments have one or more remote access or external connections to third parties like internet providers, service providers and others.
- **Weak passwords:** OT devices lack strong authentication, and credentials can easily be guessed or brute forced by cybercriminals. Earlier this year, the CISA warned that cybercriminals were gaining access to internet-exposed **UPS** devices through unchanged default usernames and passwords.
- **Limited security resources:** **47%** of ICS organizations do not have an internal team dedicated 24x7 to managing OT/ICS incidents. There is also a lack of alignment between IT and OT security teams.

MYSTIKON 2022

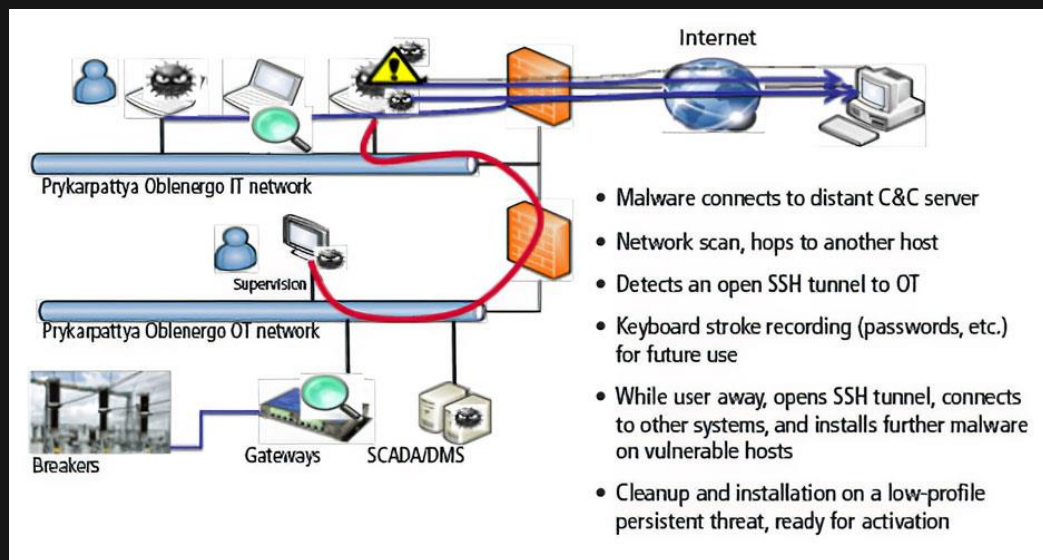
SPONSORED BY |



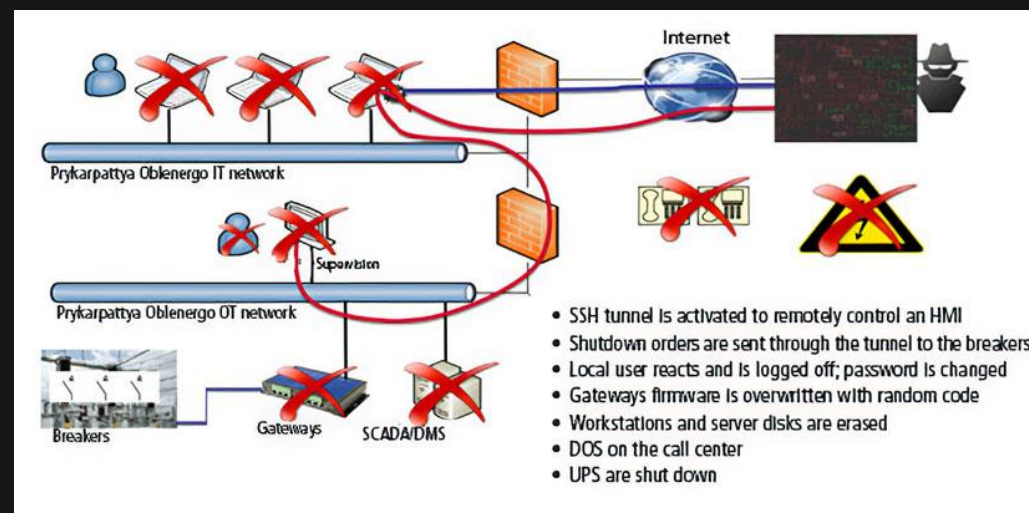


Example: Ukrainian Power Plant Attack (2015)

Compromise of Machines from Internet (began with spear phishing)



Impact of Attacker-Controlled Supervisory Machine: Months of Recon before DoS Attack



<https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware>



MYSTIKO

Risk Management

- What we take for granted and perform in IT systems cannot be so easily done in OT systems.

<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/>

<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/>

What Makes OT Systems So Vulnerable To Attacks?

A number of reasons make OT/ICS environments vulnerable:

- **Aging technology:** Many OT systems were built decades ago when most devices were air-gapped and nobody was too concerned about cybersecurity, encryption or authentication. It is estimated that **71%** of systems have outdated or unsupported operating systems, 66% have no automatic updates, and 64% have unencrypted passwords.
- **Difficult or infrequent patching:** While **65%** of vulnerabilities have a patch available, it is extremely difficult for organizations to patch systems regularly due to the associated risk of downtime. Most critical infrastructure and ICS environments operate round the clock; they cannot be taken offline) or cannot risk applying untested patches that may have downstream ecosystem impacts or potential to disrupt the overall system.
- **Inherent vulnerabilities:** The number of reported vulnerabilities in ICS environments is **doubling** every year.
- **Remotely exploitable:** Almost **70%** of all operational environments have one or more remote access or external connections to third parties like internet providers, service providers and others.
- **Weak passwords:** OT devices lack strong authentication, and credentials can easily be guessed or brute forced by cybercriminals. Earlier this year, the CISA warned that cybercriminals were gaining access to internet-exposed **UPS** devices through unchanged default usernames and passwords.
- **Limited security resources:** **47%** of ICS organizations do not have an internal team dedicated 24x7 to managing OT/ICS incidents. There is also a lack of alignment between IT and OT security teams.

IT world: tech refresh and upgrades

IT world: patch management with well-defined downtime window

IT world: Internet connections are designed with some security.

IT world: incentive to incorporate MFA, cooperate across software vendors.

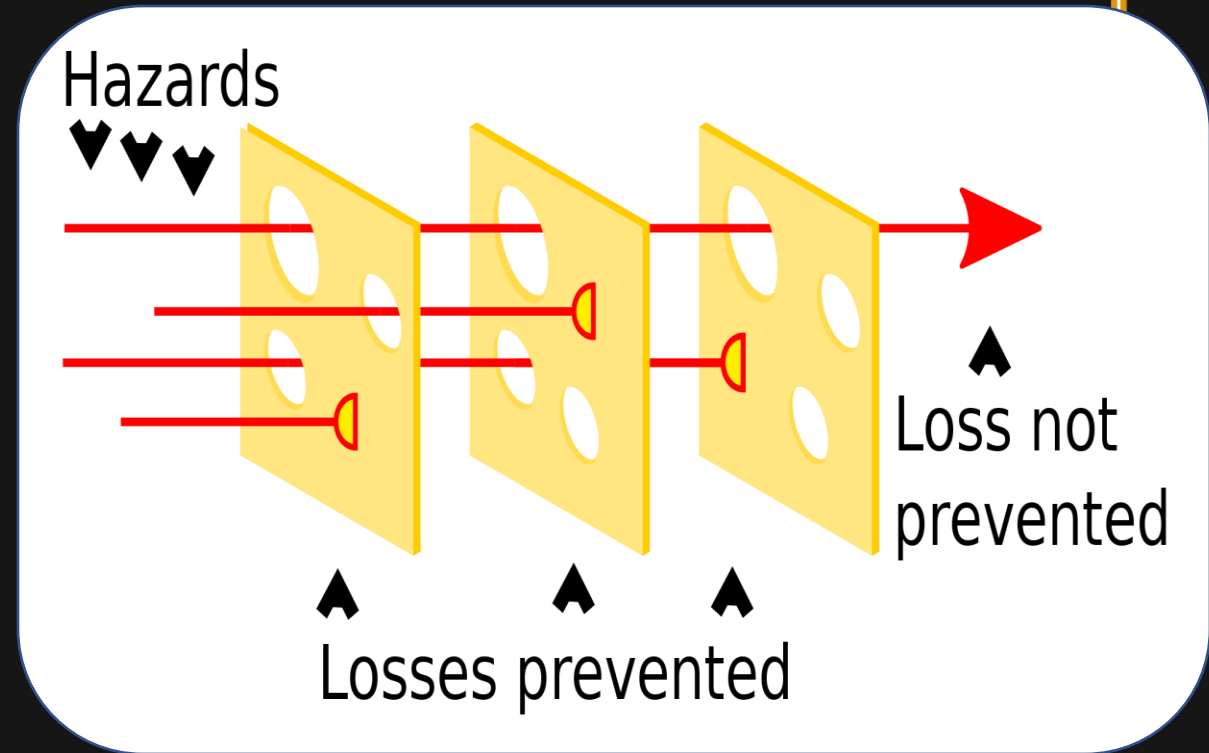
MYSTIKON 2022

SPONSORED BY |



Revisiting "Defence in Depth"

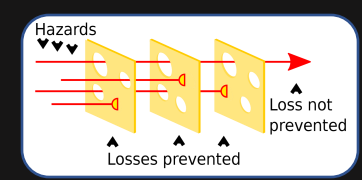
- Questions:
 - Do each of the security controls in IT systems apply to OT systems?
 - What information do I know from my security controls?
 - What information do I *not* know due to these missing security controls?
 - What is my security posture like now?



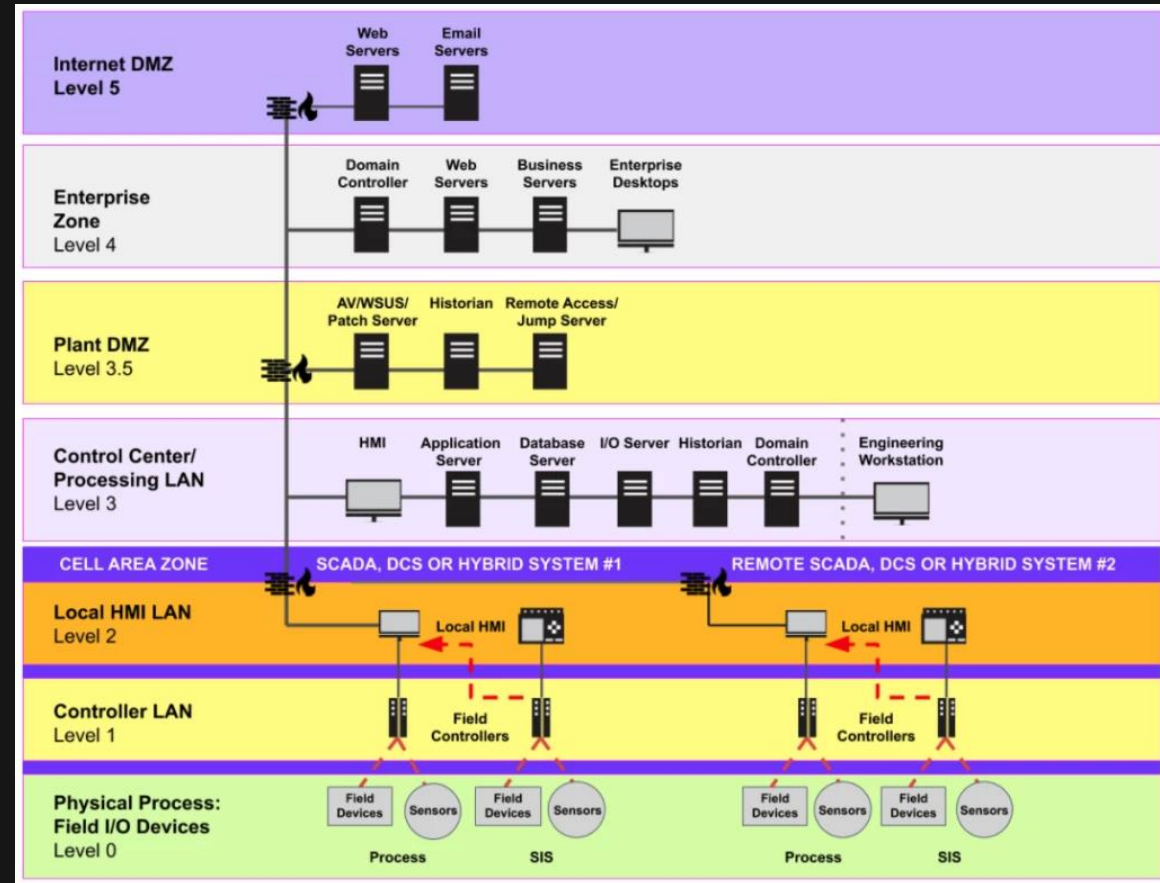


MYSTIKO

Revisiting "Defence-in-Depth"



- Questions:
 - Where can defences be implemented at?
 - What types of defences can be implemented? (are all defences implementable?)
- How will the strategy differ from that of an IT network?



MYSTIKON 2022

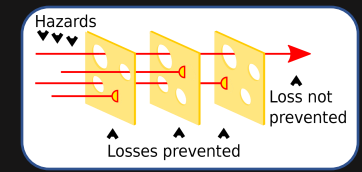
SPONSORED BY |



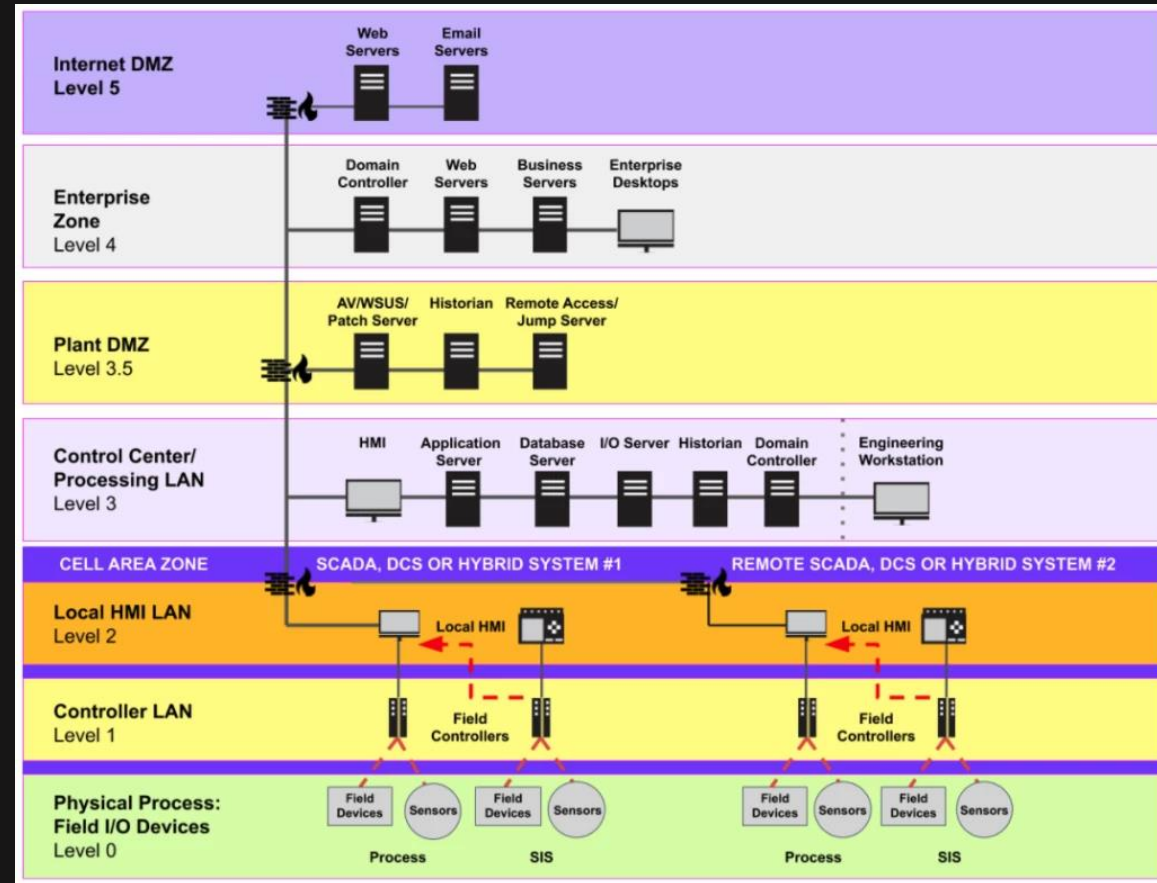


MYSTIKO

Revisiting "Defence-in-Depth"



- Another defence-in-depth perspective:
 - Think about administrative, physical and technical controls.
 - In some OT systems, physical attacks can become cyber incidents (and vice-versa)



MYSTIKON 2022

SPONSORED BY |



Supplementary: Revisiting "Threat Intelligence"

- Questions:
 - Are the threat actors attacking IT systems the same as the ones attacking OT systems?
 - If the threat actors are different... what IOCs should we watch out for?



Ooops, your files have been encrypted! English



What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37



MYSTIKO

Q & A

- Contact me:
 - LinkedIn: <https://www.linkedin.com/in/donavan-cheah-90548977/> -- just drop a DM!

MYSTIKON 2022

SPONSORED BY |

