

Hybrid Cyber-threats in Modern Critical Energy Infrastructures

George Stergiopoulos
University of the Aegean, Greece
February 2022

HYBRID THREATS WORKSHOP 2022

Hybrid cyberthreats in modern Critical Energy Infrastructures

..and how can Resilience help

GEORGE STERGIPOULOS

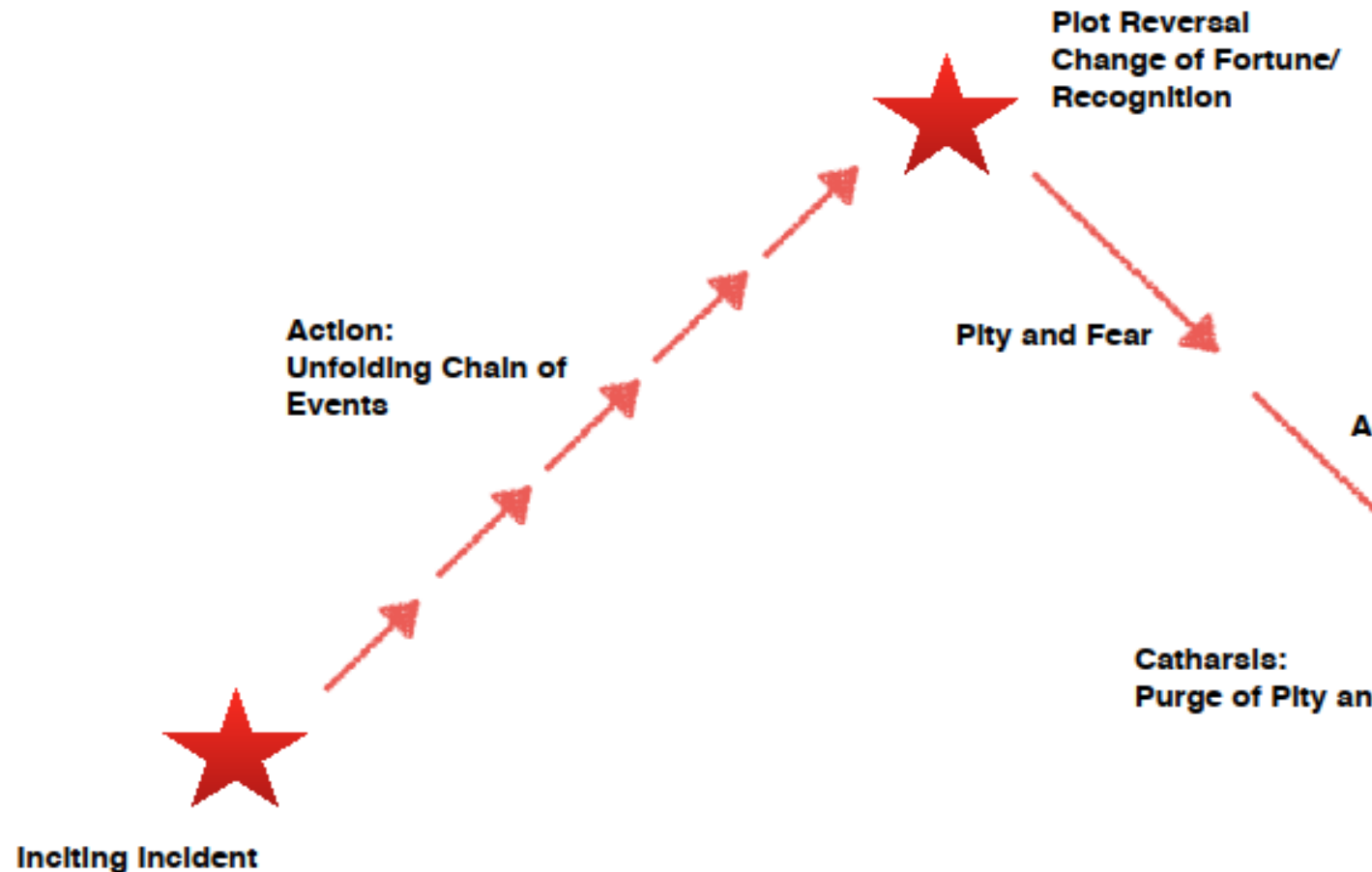
ASSISTANT PROFESSOR – INFORMATION AND TELECOM. SECURITY
INDUSTRIAL & IT SECURITY CONSULTANT

UNIVERSITY OF THE AEGEAN, GREECE
FEBRUARY 2022

Presentation Outline

- Any plot can be divided into five parts: Introduction, Rise, Climax, Fall, and Resolution.
- ...or in Aristotle's Poetics: Prologue, Action, Climax, Pity and Fear, Catharsis.
- **Prologue and Action.**
 - *Critical Energy infrastructures today*
 - *Novelty, Industry 4.0.*
- **Plot Reversal.** *Hybrid Threats.*
- **Pity and Fear.** *No need for subtitles here.*
- **Catharsis.** *...and how can Resilience help?*

Aristotle's Tragic Plot Structure



Prologue

Modern Critical Energy Infrastructures

Modern Critical Energy Infrastructures

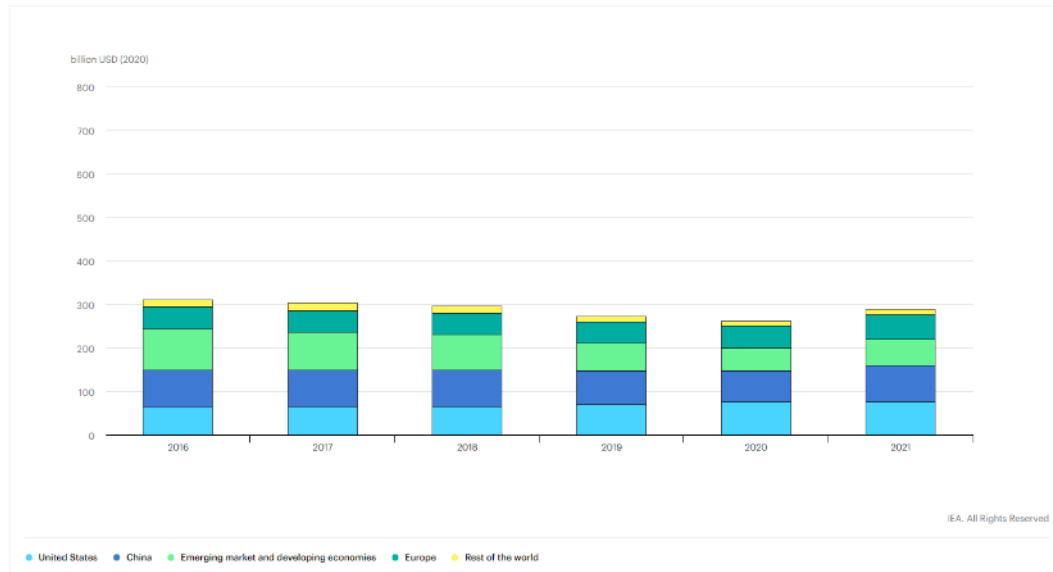
- Critical Infrastructures: “Asset, system or part thereof located in EU Member States essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions” (Council of the European Union 2008)” ¹.
- Critical Energy Infrastructures (CEIs) emphasize on provision of essential services and continuity.
 - **CEIs support all other infrastructures in every societal aspect.**
- “For operators of critical infrastructure in the Gulf Cooperation Countries (GCC), Industry 4.0 solutions provide a wealth of benefits, including enabling both remote monitoring and remote outages, and facilitating greater power plant optimization” ².
 - Connectivity is remote outage support.
 - Optimize capacity, reduce fuel consumption, and lower NOx gases and CO2 emissions and less spending on maintenance

Modern Critical Energy Infrastructures

Investment spending in electricity networks by region, 2016-2021

Last updated 26 Oct 2021

Download chart ↓



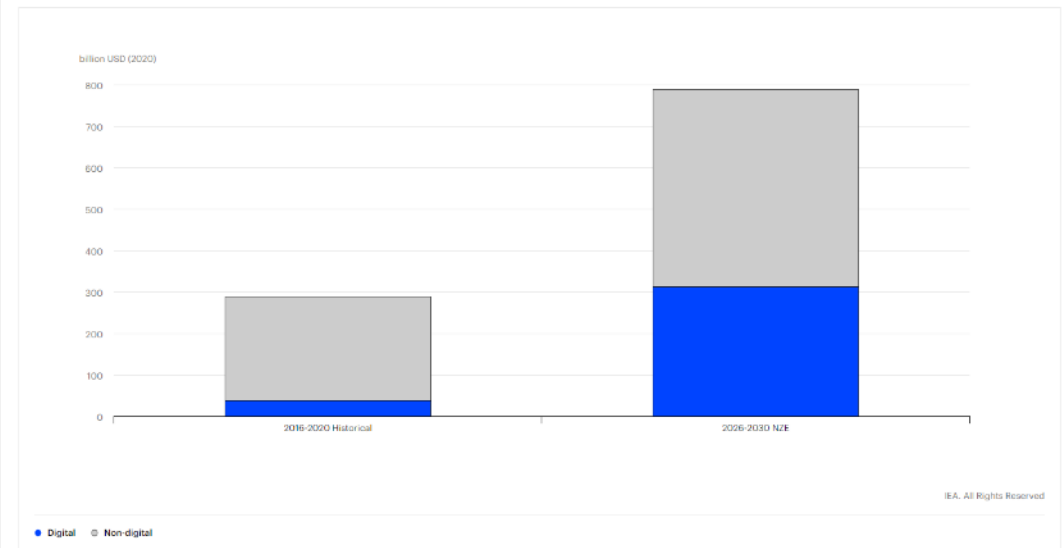
Investment spending in electricity networks, 2016-2020 and 2026-2030 in the Net Zero Scenario

Last updated 26 Oct 2021

Cite Share

Download chart ↓

Cite Share



Plot Reversal

Threats and Hybrid cyberthreats

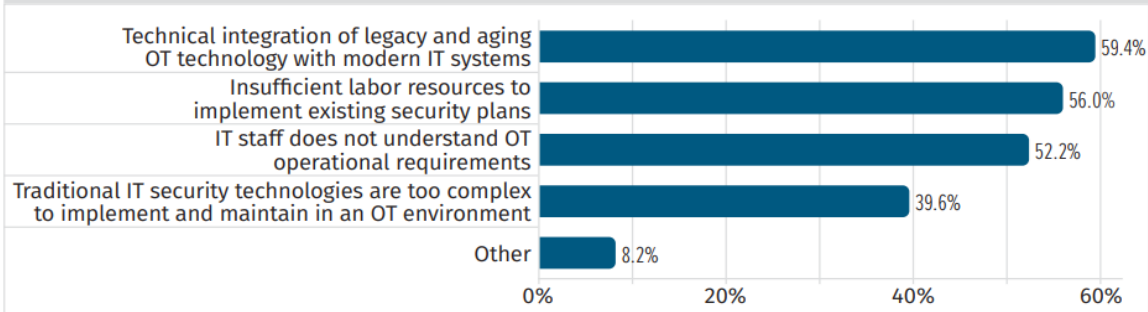
Hybrid cyberthreats – The basics

- What turns an action into a Hybrid Threat?
 - “When a hostile actor deliberately *combines and synchronizes action, specifically targeting the systemic vulnerabilities in democratic societies*” 1.
 - “Usually exploits the seams of democratic society as well as between different jurisdictions”.
 - “Often includes a distraction element, such as action in one place, and a target somewhere else” (centre of gravity analysis, Schmid, 2017).
- Manipulation is the basis of reflexive control.
 - Critical Infrastructures optimal targets to instill reflexive actions.

Hybrid cyberthreats & Energy

- Cyberspace provides a *new delivery mechanism of attacks* against Energy CIs ¹
 - Increases speed, diffusion, and power of an attack, and ensure anonymity and undetectability.
 - This includes cybercrime, propaganda, espionage, influencing, terrorism and even warfare itself.
- Energy and other *infrastructure dependencies can generate economic dependencies* and/or become a *tool for exerting economic pressure* ¹.
 - Russia's energy strategy states that: "Significant energy resources are *instruments for conducting domestic and foreign policy*" ¹.

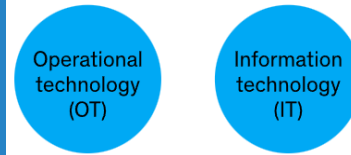
What are the biggest challenges your organization faces in securing OT technologies and processes? Select all that apply.



SANS Survey 2021 - OT ICS Cybersecurity Nozomi Networks

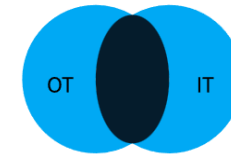
As data analytics drives convergence of OT and IT, organizations will need to rethink technology, policies, and operating model.

Pre-2010: Operational separated



- No connections exist between OT and IT networks
- No attackers focused on OT
- Little awareness of OT or critical infrastructure vulnerabilities
- No dedicated resources for OT security

Today: IT and OT merging



- OT and IT networks connected for monitoring, maintenance, and even remote control
- High number of attacks targeting OT
- Lack of clarity about OT security accountability and OT security managed in the business unit

Future: Potential convergence



- Fully integrated IT-OT environment through adoption of industrial internet and IoT
- Formalized governance and security policies for OT
- Single-point accountability for OT and IT security

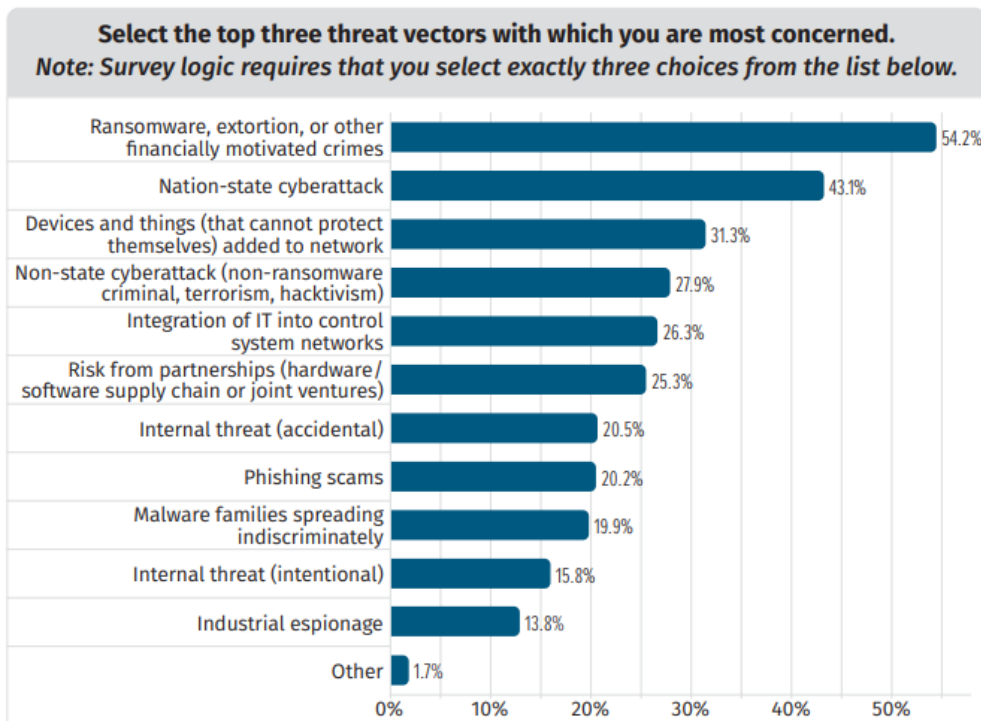
Source: Bengt Gregory-Brown and Derek Harp, *Security in a converging IT/OT world*, SANS Institute white paper, November 2016, ge.com

Vulnerable Critical Energy Infrastructures

Vulnerable Critical Energy Infrastructures

- Modern CEI are distributed, complex Cyber-Physical systems and attacks expand significantly 2.
 - In 2014, the US Dept. of Energy (DOE) revealed more than 1,100 cyberattacks against components, 159 of which were successful cyber intrusions between 2010-2014 exposing critical information about the U.S. power systems 2.

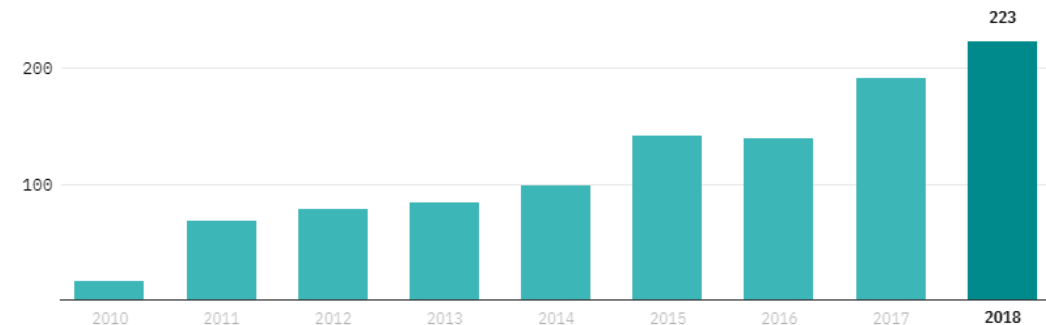
SANS Survey 2021 – OT ICS Cybersecurity Nozomi Networks



As reported by the US Department for Homeland Security, during 2015, the Industrial Control Systems Cyber Emergency Response Team responded to 245 incidents; the Energy sector tops the list with 79 incidents (32%) 2.

US energy systems are increasingly under attack

Security Vulnerability Advisories issued for industrial control systems that support electricity grid operations, 2010–18



Source: Department of Homeland Security

ENERGYMONITOR

Pity and Fear

Pity and Fear - OSINT Resources for adversaries

- Adversaries can now create representative models of the power system, conduct power studies on the model to derive its critical operational points, and finally construct attack vectors against these specific points.
- OSINT-based intelligence leveraged towards achieving these steps.
 - Threat actors seeking to cause a large-scale blackout, investigating the feasibility of utilizing publicly available resources to achieve this objective.
- Possible to obtain information required to model a power system, enabling tactical target analyses through power studies on the constructed model.

Pity and Fear - OSINT Resources for adversaries

- **Power system databases**
 - Power system databases are publicly available (Open Power System Data platform, ENTSO-E)
 - Data include maps of transmission networks, grid interconnection details, real time cross border flows, historical and forecast loads and generation statistics, as well as development plans.
- **Geographic Information Systems**
 - **Topology of a power system can** be constructed or validated by observing the physical components of the system and their interconnections.
 - Possible to generate network topology using satellite imagery Geographic Information Systems (GIS).
- **Public reports**
 - Transmission System Operators (TSOs) or government agencies release reports with operational details and information regarding their power system.
 - E.g. annual financial reports to shareholders, statements that outline future requirements etc.

Pity and Fear – Real example

- GIS information to map midstream infrastructure
- Cross-validated information through TSO reports, vendor success stories and news articles.
- Example of components and connections for each voltage level are presented in Table below.



Fig. 2 Tracing transmission lines on GIS services

Type	Number
400 KV buses	36
220 KV buses	64
132 KV buses	75
Total buses	175
400 to 400 KV branches	84
220 to 200 KV branches	115
132 to 132 KV branches	155
400 to 220 KV branches	29
400 to 132 KV branches	34
220 to 132 KV branches	4
Total branches	421
Generation stations	12
Maximum load forecast	15 GW
Installed generation capacity	17 GW

Pity and Fear – Example attacks in Energy

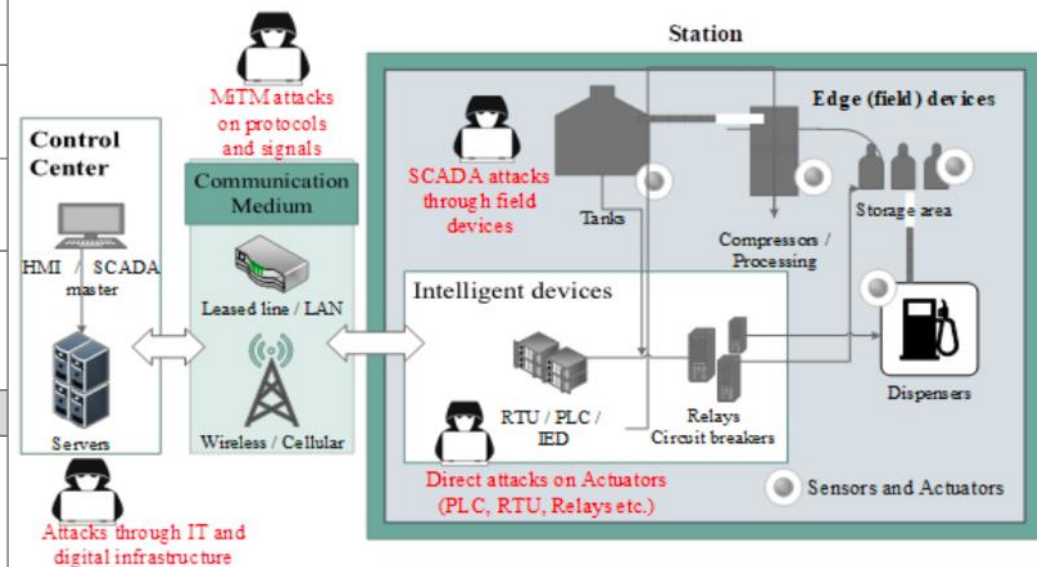
- Table below lists notable power outages of the twenty and relevant societal impact 1.
 - Examples showcase the diversity of possible causes and are sorted by their impact measured in millions of people affected.
 - Pandora’s box was opened in 2010 with Stuxnet.
 - First cyberattack targeting power systems is an incident in Ukraine reported in December 2015, believed to be the work of a nation-state actor.
- According to Symantec, the energy sector is the main target of many campaigns, and the attack focus is not limited to the U.S. 2.

Year	Country	People affected	Cause
2012	India	620 million	Misoperation [21]
2015	Pakistan	140 million	Malicious destruction [15]
2014	Bangladesh	100 million	Equipment failure [1]
2009	Brazil & Paraguay	87 million	Adverse weather conditions [3]
2015	Turkey	70 million	Maintenance and oversupply [50]
2003	U.S. & Canada	55 million	Shortcircuit because of trees [19]

Pity and Fear - Example Attacks Types in Oil & Gas

TABLE 6. Taxonomy of potential O&G attacks with ATT&CK Reference ID.

Vulnerability type	ATT&CK Tactic ID	Description
Hardware Layer		
Lack of tamper resistance	T858 - Utilize/Change Operating Mode T848 - Rogue Master Device	Field devices often do not implement hardware security controls that can detect or prevent physical tampering attacks (e.g. key extraction attacks) [81], both in midstream and downstream O&G infrastructures.
Lack of physical security	T825 - Location Identification T801 - Monitor Process State	Physically altering/attacking industrial systems without fail-safe or monitoring mechanisms can lead to leakage affecting nearby communities [41]-[43].
Use of legacy devices & equipment	T858 - Utilize/Change Operating Mode T801 - Monitor Process State T833 - Modify Control Logic	Legacy field devices, PLC and sensors remain active for extended periods, even though they have known vulnerabilities.
Unknown / untrusted Off-The-Shelf devices	T862 - Supply Chain Compromise T811 - Data from Information Repositories	Removable devices are potential attack vectors that can be overlooked by users. COTS components (not custom-made) provide stability, availability and reduce cost but, at the same time, may introduce unknown vulnerabilities, both in mid and downstream ICS.
Firmware Layer		
Outdated OS	T851 - Rootkit T800 - Activate Firmware Update Mode	Unpatched operating systems are a common vulnerability both for ICS and IT systems [12]. Reports consider the lack of OS patching along with software patching as one of the top ICS vulnerabilities since 2016 [18]. This applies to the O&G sector too.
Lack of firmware protection	T839 - Module Firmware T857 - System Firmware T800 - Activate Firmware Update Mode T851 - Rootkit	Facility and ICS are known to lack security measures against firmware modification [45], mostly due to cost cutting this is not happening [7]-[9],[23].



Catharsis

...and how can Resilience help?

Cyber Resilience - Basics

- Traditional risk management strategies identify vulnerable critical components of systems and harden them.
 - Appropriate for many isolated cyber systems, but not for hybrid/unknown threats.
 - Identifying all critical components to protect against all types of threats increasing expensive.
- Funding can be re-allocated towards resilience enhancement efforts.

Cyber Resilience - Basics

- New approaches needed to address threats & vulnerabilities integrated within a wide variety of interdependent computing systems and accompanying architecture (DiMase et al. 2015; Ganin et al. 2017).
- Resilience often confused with several related but different concepts.
 - Risk, robustness, and security and so on..

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources” (NIST SP.800-160).

w

“The continued ability to “endure” and “recover” from disrupting events” 1.

Cyber Resilience - Basics

- “*Cyber resiliency engineering practices are the methods, processes, modeling, and analytical techniques used to identify and analyze proposed cyber resiliency solutions*” (NIST SP.800-160).
 - Application of cyber resiliency engineering ensures solutions are driven by stakeholder requirements and protection needs.
- Cyber resilience should be considered in the context of complex systems that comprise not only physical and information *but also **cognitive and social domains*** (Smith, 2005).
- Difficult task in Energy Infrastructures as it involves various interdependent layers with heterogeneous computing equipment, physical components, network technologies, and data analytics.

Cyber Resilience - How To

GOAL	DESCRIPTION
Anticipate	Maintain a state of informed preparedness for adversity.
Withstand	Continue essential mission or business functions despite adversity.
Recover	Restore mission or business functions during and after adversity.
Adapt	Modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments.

OBJECTIVE	DESCRIPTION
Prevent or Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.
Constrain	Limit damage ²³ from adversity.

* **Objectives** refer to techniques while **Goals** realize a long-term, high-level vision 1

Cyber Resilience - How To

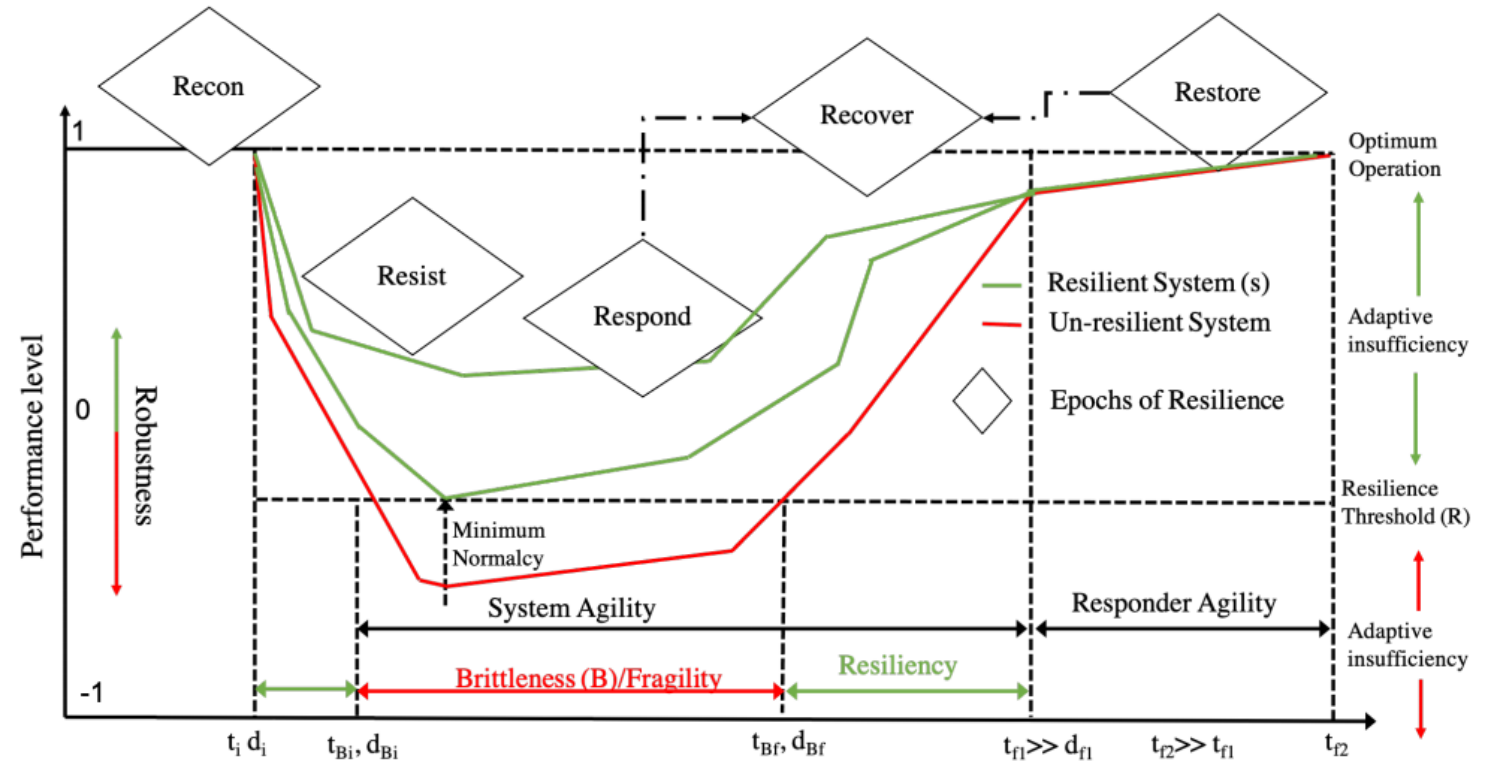
- **ANTICIPATE**
 - Correct planning of critical functions and services.
 - Validate important dimensions to assess system performance.
- **WITHSTAND**
 - Thresholds.
 - Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift.
- **RECOVER**
 - Aspects of Impact and Duration of degraded system performance.
- **ADAPT**
 - Adaptive Management.
 - Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences.

Cyber Resilience - How To

- **ANTICIPATE / RECON**
 - Correct planning of critical functions and services.
 - Validate important dimensions to assess system performance.
- **WITHSTAND / RESIST**
 - Thresholds.
 - Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift.
- **RECOVER**
 - Aspects of Impact and Duration of degraded system performance.
- **RESTORE / ADAPT**
 - Adaptive Management.
 - Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences.

“Disturbance and Impact Resilience Evaluation Curve” (DIRE)

- “Disturbance and Impact Resilience Evaluation Curve” (DIRE)
- A conceptual resilience curve with resilient control metrics
- Expresses the “R-s” of resilience
 - Recon, Resist, Respond, Recover, and Restore



Cyber Resilience - Approaches

- **Manage Complexity:** Resilience of a system or network depends greatly on complexity of links within the system (Kott and Abdelzaher 2014).
 - High complexity of links which lead to interactions that the system's designer cannot anticipate and guard against.
- **Topology:** Quite apart from complexity, the choice of appropriate topology of the system or network can improve resilience.
- **Diversity and Redundancy:** Additional and different resources help improve resilience.
 - E.g.(1), Limit the possibility of loss of critical functions due to failure of replicated common components.
 - E.g.(2), adding capacity to nodes in a power generation and distribution network may reduce likelihood of cascading failures and speed up the service restoration.
- **Monitoring:** Maximize ability to detect potential adverse conditions.
 - Analyze monitoring data and analysis results from different information sources or at different times together with externally provided threat intelligence.

Cyber Resilience - Approaches

- **Reversibility:** Components of the system should be designed in a manner that allows them to revert to a safe mode when failed or compromised.
- **Propagation:** Infrastructure engineers should guard against cascading failures.
 - Dependencies or links between nodes designed in a way that minimizes the likelihood that a failure propagates.
- **Privilege Restriction:** Restrict privileges based on attributes of users and system elements as well as on environmental factors.
- **People:** Active employees with plans, processes and preparation.
- **Simulation and Analysis:** Test test test test! Oh, and test.
 - Did I mention test?
 - You should test more.
 - Processes and security measures introduced with appropriate analysis to reveal potential negative impacts and systemic effects (Kott et al 2017).

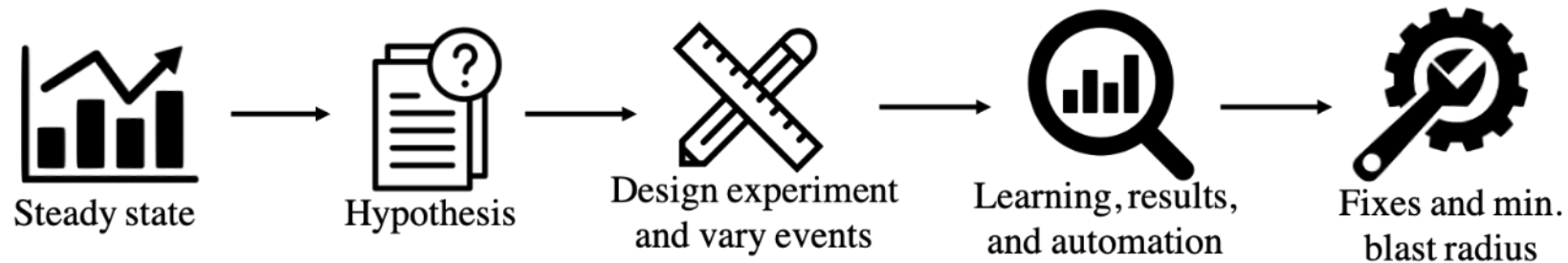
A little bit of future:

Chaos Engineering analysis in industrial systems

KONSTANTINOU, C., STERGIOPOULOS, G., PARVANIA, M., & ESTEVES-VERISSIMO, P. (2021, OCTOBER). CHAOS ENGINEERING FOR ENHANCED RESILIENCE OF CYBER-PHYSICAL SYSTEMS. IN INL RESILIENCE OPTIMIZATION CENTER 2021 RESILIENCE WEEK (RWS) (PP. 1-10). IEEE.

Chaos engineering for enhanced resilience

“The discipline of experimenting on a system in order to build confidence in the system’s capability to withstand turbulent conditions in production”.



Benefits?

- **Quantitative**: e.g., reduce no. of preventable outages, financial loss, etc.
- **Qualitative**: e.g., improvement in design decisions, growth in understanding service criticality, confidence in validating reliability measures, etc.

Steady state in ICS

Objective: model development to describe the steady states according to the anticipated conditions of the system metrics

- E.g., metrics could be the level of sodium hydroxide in a water treatment

The steady state of an output state can be seen the difference between setpoints for state regulation and unmeasured control disturbances

- E.g., the difference of load demand and generation control inputs in a power grid model

In ICS, the effort is to operate across nominal system setpoint metrics. The target setpoints can be determined in a min.-type of problem:

Hypothesis

Objective: determine what is expected as the result of an experiment, in terms of the system's steady state conditions, if we apply a set of diverse events into the ICS

The hypotheses in CE experiments are typically in the form of “the events we are injecting into the system will not cause the system’s behavior to change from steady state”

For the purposes of CE experimentation, we can form the hypothesis that the output of the target metric will remain within acceptable bounds, given any set combination of control inputs

- Different types of key performance indicators (KPIs) can be chosen, based on operator knowledge and on the characteristics of the system under test, e.g., manufacturing process performance KPIs, computing resources performance KPIs, OPC data exchange performance KPIs, etc.

Chaos engineering - Run experiments in ICS production & automation

A major difference of CE compared to accepted forms of security testing is the automation within the system's production environment as well as the focus on the overall system behavior

We cannot be aware a priori which conditions to the production environment will change the results of a CE test. In this stage, ideally, the tests need to be tested on the production environment

Objective: reduce risks in terms of experiments validity increased reliability, and provide enhanced insight into the performance of the experiments in terms of results confidence

References

1. Dedousis P., Stergiopoulos G., Arampatzis P., Gritzalis D., "A security-aware framework for designing industrial engineering processes", *IEEE Access*, Vol. 9, pp. 163065-85, December 2021.
2. Dimitriadis A., Prassas C., Flores J.-L., Kulvatunyong B., Ivezic N., Gritzalis D., Mavridis I., "Contextualized filtering for shared cyber threat information", *Sensors*, Vol. 14 (4890), July 2021.
3. Gritzalis D., Iseppi G., Mylonas A., Stavrou V., "Exiting the risk assessment maze: A meta-survey", *ACM Computing Surveys*, Vol. 51, No. 1, pp. 1-30, January 2018.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, 2013.
5. Lykou G., Moustakas D., Gritzalis D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensors technologies", *Sensors*, Vol. 20 (3537), June 2020.
6. Lykou G., Dedousis P., Stergiopoulos G., Gritzalis D., "Assessing interdependencies and congestion delays in the aviation network", *IEEE Access*, Vol. 8, pp. 223234-54, December 2020.
7. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 46-60, 2016.
8. Stergiopoulos G., Kapetanas N., Vasilellis E., Gritzalis D., "Leaking SCADA commands over unpadded TCP/IP encryption through differential packet size analysis", *Security & Privacy*, Vol. 2, No. 5, pp. 1-21, October 2019.
9. Stergiopoulos G., Dedousis P., Gritzalis D., "Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0", *International Journal of Information Security*, February 2021.
10. Stergiopoulos G., Gritzalis D., Limnaios E., "Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns", *IEEE Access*, Vol. 8, pp. 128440-75, July 2020.
11. US-CERT, *Cyber Resilience Review*, 2016. Available at: <https://www.us-cert.gov/ccubedvp/assessments>