POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Critical Incident Analysis: "Industroyer2" Cyberattack on Ukrainian Power Grid

Group:

Luigi Tiberio [redacted]
Stefano Moreschi [redacted]
Mattia Silvestri [redacted]

Academic Year: 2025/2026

Contents

1 | Introduction

Nowadays, most critical infrastructures rely on complex cyber-physical systems. This reliance exposes such infrastructures to increasingly dangerous cyber threats. Since digital vulnerabilities are inevitable, a clear and effective cybersecurity framework to ensure robust cyber resilience is mandatory in modern critical infrastructures.

Cybersecurity has therefore become a cornerstone of the geopolitical landscape, as conflicts between nations are progressively shifting toward cyberspace. According to NATO reports, the current threat landscape is highly complex, with China identified as the largest global cyber threat, operating approximately 40 Advanced Persistent Threat (APT) groups, and Russia emerging as the fastest growing attacker, with an estimated 800% increase in cyberattacks following the invasion of Ukraine.

Although the physical invasion of Ukrainian territory began in February 2022, Russia had been targeting Ukraine's critical infrastructures for several years. In December 2016, the Russian hacker group Sandworm developed an industrial malware known as *Industroyer* and used it to attack Ukraine's power grid. That operation caused a temporary blackout in the Kyiv region, leaving tens of thousands of citizens without electricity for approximately one hour. Six years later, Sandworm attempted a similar operation using an evolved version of the malware, referred to as *Industroyer2*, with the objective of sabotaging Kyiv's power supply. However, the attack, which was originally scheduled for April 8, was detected and disrupted in advance by the Government Team for Responding to Computer Emergency Events of Ukraine (CERT-UA), in collaboration with Microsoft and ESET, thereby preventing any blackout.

Although this most recent incident cannot be classified as a critical event, it represents a valuable *near-miss* scenario for research in technology risk governance. It is therefore crucial to analyze which preventive and protective measures proved effective and which did not, and to explore what could have gone wrong, in order to derive insights for strengthening risk management practices for critical infrastructures.

The analysis begins with an assessment of the overall context of the attack and the actors involved, including the victim infrastructure, the attacker, and the malware employed.

Subsequently, Reason's model is applied to identify active and latent failures within the cyber-physical systems of the power grid.

The core of the study focuses on the application of Fault Tree Analysis (FTA), developing multiple branches from the avoided Top Event, namely the scenario in which the malware would have successfully disrupted the city's power supply. Following this, critical vulnerabilities are identified through selected Minimal Cut Sets derived from the FTA, which are then used as a basis for constructing an Event Tree Analysis (ETA) to visualize potential alternative outcomes in the event of barrier failures.

Finally, residual vulnerabilities are examined through a concise Failure Mode and Effects Analysis (FMEA), and the organizational dimension is addressed by applying a qualitative review of the implemented Human and Organizational Factors (HOF).

2 | Incident Description

2.1. Entities Involved

“Sandworm” is a prolific malicious hacker group associated with the Russian military intelligence agency GRU and has been identified as responsible for numerous cyberattacks with clear political intent over recent years. The group has been widely attributed as the perpetrator of both the *Industroyer* and *Industroyer2* attacks.

Cybersecurity researchers have attributed to Russian hacker groups several other high-profile cyber operations, including spearphishing campaigns and hack-and-leak activities during the 2017 French elections, the infamous *NotPetya* attacks of June 2017, and intrusions and malware campaigns targeting the 2018 PyeongChang Winter Olympic Games.

State-driven cyberattacks are becoming increasingly common and targeted, often resulting in significant economic and societal damage to the affected entities. At the same time, specialized institutions play a critical role in public cybersecurity defense. In Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA) operates as a subunit of the State Center for Cyber Defense within the State Service for Special Communications and Information Protection of Ukraine. Since its establishment in 2007, CERT-UA has played a crucial role in countering malicious cyber activity against the Ukrainian state. The attack examined in this study (i.e., the 2022 *Industroyer2* incident) was successfully disrupted by CERT-UA with the support of external cybersecurity teams from Microsoft and ESET.

The original *Industroyer* attack succeeded in sabotaging the power grid, causing a blackout in the Kyiv region, an area with a population of several million inhabitants. This outcome further highlights that cyberattacks against critical infrastructures involve a wide range of stakeholders and cannot be reduced to a simple attacker–defender dichotomy. Infrastructure operators may have their systems compromised or face physical safety risks, military defense capabilities may be impaired due to loss of power, neighboring countries may experience cascading effects, and ultimately civilians remain the most vulnerable stakeholders.

For these reasons, when analyzing a cyberattack against a critical infrastructure, assessing the stakeholder environment represents one of the most crucial initial steps in the overall evaluation process.

2.2. Critical Infrastructure Description

The electrical sector is widely recognized as a critical infrastructure due to its fundamental role in enabling other essential services. Consequently, power grid components have become high-impact targets for cyber–physical attacks. The targeted infrastructure in the analyzed case was an energy facility located in Ukraine, specifically in the Kyiv region.

Public sources do not specify whether the infrastructures involved in the *Industroyer* and *Industroyer2* attacks were the same. It is only reported that electrical grids in the Kyiv region were targeted with the intent of causing a blackout. While a detailed technical description of the affected critical infrastructure is neither possible nor strictly necessary, a concise and clear representation of the power grid structure is useful to visualize the vulnerabilities that were exploited.

The architecture of a power grid consists of tightly intertwined cyber and physical components, where Information Technology (IT) and Operational Technology (OT) environments are strongly interconnected, and fully isolated systems are increasingly rare. Hardware components such as circuit breakers and electrical substations are connected to local networks and may be managed remotely. Automation enables fast and large-scale control actions; however, the use of industrial control systems relying on IEC protocols may introduce cyber vulnerabilities inherent to the systems themselves.

According to CERT-UA, the infrastructure elements targeted during the attack included high-voltage substations, computers running the Windows operating system, server equipment based on Linux operating systems, and active network devices. The attackers sought to exploit industrial communication protocols to gain access to the industrial control systems.

The key takeaway is that the increasing integration between IT and OT environments has significantly expanded the attack surface of power grid infrastructures, thereby introducing latent cyber vulnerabilities that can be exploited by sophisticated adversaries.

An illustrative schematic representation of a typical power grid architecture is shown below.

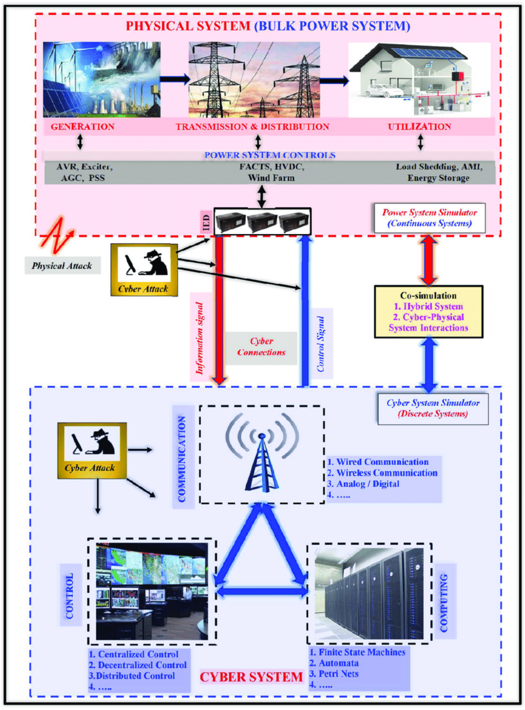


Figure 2.1: Power Grid architecture example (source: ResearchGate)

2.3. Malware Description

Industroyer2 is the evolution of the *Industroyer* malware. *Industroyer* is a malware designed to send commands to industrial control system processes, especially those used in electrical substations. Both were used by Sandworm to attack Ukrainian power-supplier critical infrastructures. The malware was stored in a `.exe` executable file, which contained the instructions to launch the attack on April 8, 2022, precisely at 16:10 UTC.

While the original *Industroyer* could interact with different protocols (IEC-101, IEC-104, IEC 61850, and OPC DA), *Industroyer2* only implements the IEC-104 protocol to communicate with industrial equipment. The malware had to be recompiled for each victim, and each executable file contained a statically specified set of unique parameters for the corresponding substations.

The vulnerabilities were not only in the ICS protocols: researchers have claimed that information about the specific architecture of the power grid had to be known by the attackers in order to be able to develop malware with such a level of specificity.

We hypothesize that it is possible that, through techniques such as spoofing, sniffing, or even simple social engineering, valuable information was stolen from personnel devices. This may highlight the importance of the human factor in critical infrastructures.

Along with *Industroyer2*, Sandworm deployed other malware, called *CaddyWiper*, to slow down the recovery process, prevent the regaining of control over ICS, and cover their tracks. The Linux and Solaris environment, which is different from the ICS one, was attacked with a combination of a Linux worm (*ORCSHRED*), a Solaris wiper (*SOLOSHRED*), and a Linux wiper (*AWFULSHRED*). This IT environment comprises the server equipment of the critical infrastructure. Even though the main target was the control of electrical substations through the ICS network, the local network devices were targeted to slow down the response team.

A simplified schema of the whole attack attempt is shown below:

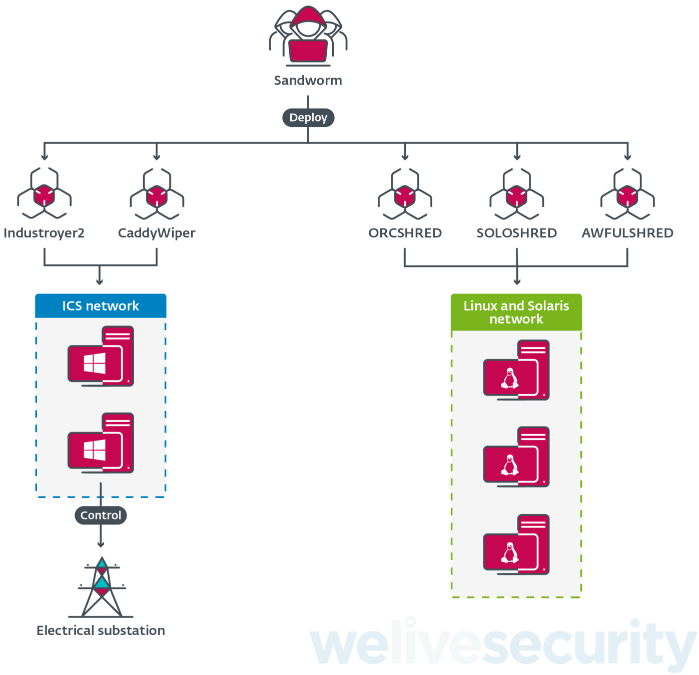


Figure 2.2: Attack schema (source: eset)

3 | Reason's Model

3.1. Reason's Analysis

The hazard is defined as the malicious manipulation of industrial control systems through tailored malware, with the objective of disrupting electricity supply. The exposed target is the continuity of power provision to a densely populated urban area. The Top Event of interest is the successful execution of malicious control commands leading to the opening of circuit breakers and a blackout.

Given the lack of precise publicly disclosed information about the elemnts of the incident, we apply a Reason's model-led analysis at global system level. First we examine the latent and active failures, and then to review the defensive layers and escalation of the attack.

A first set of latent conditions concerns the structural coupling between IT and OT. In modern critical infrastructures, the operational need to exchange data, manage assets, and support engineering workflows often creates boundary points between corporate systems and operational networks. Even when segmentation exists, these interconnections can introduce dependencies and pathways that may be exploited once an attacker gains a foothold. The fact that the malware was staged on systems relevant to the operational environment indicates that, at least in this case, a pathway existed to reach OT-adjacent assets beyond the outer perimeter.

A second structural condition is the reliance on legacy industrial communication protocols. Protocols such as IEC-104 enable interoperability and operational control, but they were not designed to provide strong security properties against a highly capable adversary. This is not a mistake of a single operator or team, but a system-level exposure that becomes critical when an attacker can obtain the addressing and sequencing knowledge needed to issue valid control commands.

A further latent condition relates to operational visibility in OT environments. Achieving uniform, protocol-aware monitoring across heterogeneous and often legacy OT assets is intrinsically difficult: legitimate industrial traffic can be operationally normal in form even when it is malicious in intent. This makes early detection and confident diagnosis challenging, especially if visibility is uneven across network segments and devices.

There are also implications from the organisational context into the defensive boundaries of the system. For example, in the case of the power grid, it was operating under strong external pressure. Operating for long periods under such conditions implies higher demands on personnel, their coordination capacity, and analytical capabilities. Suboptimal organisational conditions therefore represented a clear vulnerability, as they reduce tolerance for delay and increase reliance on rapid coordination across teams and organisations once anomalous activity emerged.

Active failures are described here as system-level events. The progression of the attack involved a sequence of system-level failure events, including the deployment of malware on operationally relevant systems, the preparation of components capable of issuing valid IEC-104 commands, and the staging of destructive payloads intended to hinder recovery. These events indicate that one or more defensive barriers were bypassed and that the attacker assembled the technical capability required to influence the control process.

Crucially, these events represent the transition from a general threat environment to a concrete hazard trajectory. It is hence fundamental to address personnel rapid response. The recognition of anomalous activity, its correct interpretation, and the timely coordination of response actions suggest effective handling by organized and expert defense teams.

The power grid relies on multiple defensive layers spanning technical systems, organisational arrangements, and human activities. Technical protections include segmentation practices, access control mechanisms, endpoint protection, monitoring capabilities, and the operational constraints of industrial protocols. The attack trajectory shows that outer barriers were not sufficient to prevent staging on operationally relevant systems. However, escalation did not reach physical impact because downstream detection, analysis, and coordinated response disrupted the trajectory before command execution.

This reasoning is very important for the following analyzes: we will not focus on outer barriers that eventually failed, but on the overall system defense architecture. This is consistent with a defense-in-depth view: individual barriers may be permeable, but the overall system can still prevent the Top Event if later layers remain effective and are activated in time.

The near-miss outcome becomes clearer when considered over time. Several barriers were penetrated, but the progression was interrupted before the final step. The detection of malicious activity prior to the planned execution time, followed by coordinated mitigation actions, prevented the realization of the Top Event. Clearly, detection alone was not sufficient; timing was decisive as well.

A comparison with the 2016 incident is consistent with this interpretation. Although structural vulnerabilities were relevant in both cases, the 2022 near-miss suggests that the first event was used as a lesson to create resilience and improve security. These developments were effective enough to at least prevent the worst-case scenario, even though fundamental exposures in legacy OT environments still persisted.

3.2. Main Takeaways

The Reason's analysis emphasize human actors as the first effective barrier: human performance represents a critical and fundamental adaptive resource when technical defences fail. In the *Industroyer2* incident, human judgement, expertise, and coordination were central to interrupting escalation. Since latent vulnerabilities born from the interdependency between OT and IT systems are inevitable in these kind of CIs, multiple effective system-level barriers and employement of skilled personnel are crucial. These last aspects will be examined in greater detail in the subsequent Human and Organisational Factors analysis.

4 | Fault Tree Analysis (FTA)

4.1. FTA Construction and Schema

The content of our research relies exclusively on publicly available and easily accessible information concerning the attack. In addition, our research primarily focused on the main events that led to the Top Event, without going too deeply into overly technical issues. Finally, the structure of the discussion will be organized so that first we present the schema, then we'll present each main branch of the diagram, providing its description followed by the failure consequences and any concluding notes.

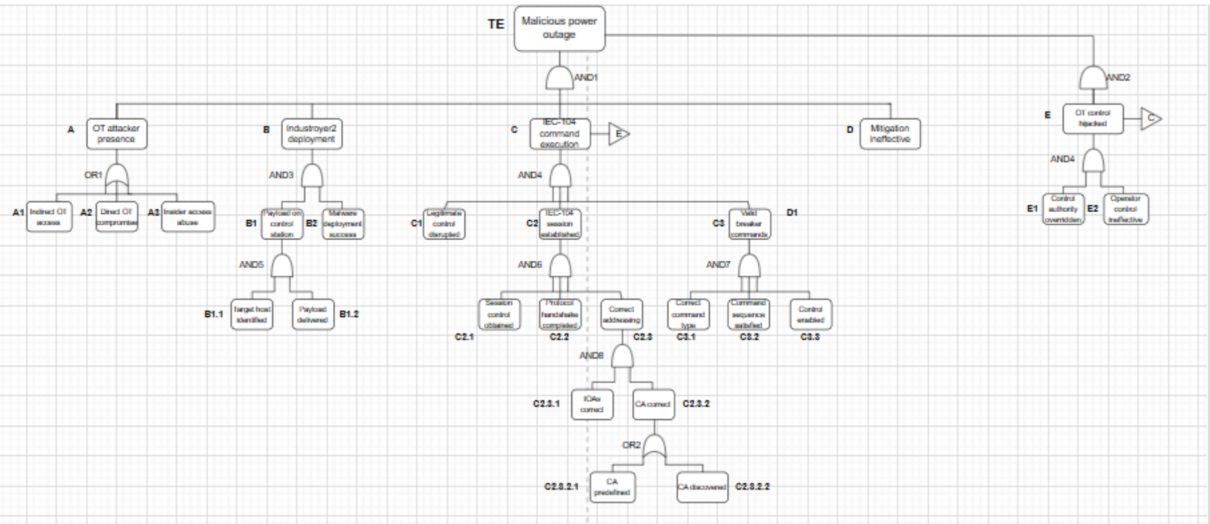


Figure 4.1: Fault Tree

TE | Malicious power outage

Description: The Top Event represents the loss of operational control over OT systems within the power grid, creating the technical conditions for a maliciously induced power outage. It captures what the Industroyer2 attack aimed for and could actually do, using real IEC-60870-5-104 commands to override normal control of substation gear.

Failure Consequences: Legitimate operators would lose effective control over OT assets such as circuit breakers and associated control points within substations. This loss of control could result in the opening of breakers and disruption of power distribution, potentially leading to localized or wider power outages.

Note: Top Event does not describe a fully realized blackout, but a credible and technically achievable failure condition that the malware was engineered to cause.

A | OT attacker presence

Description: This branch represents the conditions that let an attacker gain entry to the OT environment. The OR relationship among Indirect OT access, Direct OT compromise, and Insider access abuse makes sense here, since public sources don't point to a single, clear initial access vector.

Failure Consequences: If A does not occur, the attacker cannot reach the required OT assets and the causal chain leading to the execution of IEC-104 commands cannot be initiated.

B | Industroyer2 deployment

Description: Describes the malware placement and staging phase on the correct host: payload on control station (with target host identified and payload delivered) and malware deployment success (intended as the malware being installed and ready for subsequent activation).

Failure Consequences: If B fails and malware is not delivered or not positioned on the correct host, the attack cannot progress to the IEC-104 command phase; even with OT access, the attacker cannot achieve the intended operational effect without deploying the malware.

Note: We decided to use the term deployment for the placement of the malicious program instead of the term execution because, at the end, the program is never really executed but just deployed inside the system.

C | IEC-104 command execution

Description: Branch C kicks in when the attacker can craft and send valid IEC-60870-5-104 control commands to OT field devices. At the basics, that means hitting the right targets with the right addresses. The target comes down to get the Information Object

Addresses (IOAs) and the Common Address of ASDU (CA) lined up. The CA may be either predefined in the malware configuration or discovered dynamically, while the IOAs have to match the exact control points for the intended physical actions. Once correct addressing is achieved, the attacker must make sure the command semantics are accepted, meaning that the appropriate command types and sequences are used so that breaker operations are enabled by the controlled station. At the same time, a valid IEC-104 session has to be established, meaning that the usual handshakes and data transfer between the controlling station and the target are required. These conditions are effective only if the legitimate control channel gets disrupted, so the attacker's control context can run without being immediately overridden. When these lower-level checks are in place, Branch C materializes as the attacker's capability to issue effective IEC-104 commands to OT targets, enabling direct manipulation of the substation devices.

Failure Consequences: If C fails, even with OT access and a staged malware payload, you will not be able to get control of the field devices: failure to establish a session, incorrect addressing (CA/IOA), an unaccepted command sequence, or control not being enabled will prevent the operation.

Note: During this phase, supporting malware like CaddyWiper and its shredder payloads were rolled out inside the compromised environment to mess up systems and slow recovery. They aren't shown in the fault tree because they don't directly drive the IEC-104 command execution and to keep the schema simple..

D | Mitigation ineffective

Description: Branch D represents the operational response and defensive context surrounding the attack, rather than a direct causal contributor to the Top Event. In the Industroyer2 incident, things like monitoring, network segmentation, and incident-response processes played key roles in spotting, interrupting, and containing the attack before it could fully kick off. These defensive elements aren't broken down into separate fault-tree events because they aren't internal system failures. They're external controls that helped keep the attack in check.

Failure Consequences: If response and mitigation measures are effective, malicious activity can be identified and neutralized before loss of OT control is fully realized, preventing or limiting operational impact.

E | OT control hijacked

Description: This last branch summarizes the final causal state that enables the impact event: OT control hijacked, modeled as an AND relationship between Control authority overridden and Operator control ineffective. In practice, the controlling station or control channel responds to malicious commands, while legitimate control fails to restore operational authority in a timely manner.

Failure Consequences: If E fails, when control authority can't be overridden or operators can quickly take back control, the impact is avoided or significantly constrained, even in the presence of malicious commands.

Note: Separating E as its own sub-tree (through a transfer) makes things clearer and shows the difference between command capability (Branch C) and loss of control (Branch E).

4.2. Minimal Cut Sets

Minimal Cut Sets (MCS) in Fault Tree Analysis (FTA) are the smallest groups of basic component failures that, if they all occur, guarantee the system's top-level failure. Since the Top Event sits at the intersection of several high-level branches, every minimal cut set (MCS) needs:

- one basic event from Branch A (because Branch A is an OR gate),
- and all the required basic events from Branches B, C, and E, except where Branch C includes an OR gate (CA predefined versus CA discovered).

Branch C results in two minimal variants due to the CA being modeled as an OR condition (predefined versus discovered). Branch A has three variants because it is also modeled as an OR condition (A1, A2, A3).

This yields a total of:

$$3 \times 2 = 6$$

minimal cut sets. With that being said, the 6 possible MCS combinations are:

Table 4.1: Comparison of Minimal Cut Sets for the Top Event

Basic Event	**MCS-1**	**MCS-2**	**MCS-3**	**MCS-4**	**MCS-5**	**MCS-6**
A1 Indirect OT access	✓	✓				
A2 Direct OT compromise			✓	✓		
A3 Insider access abuse					✓	✓
B1.1 Target host identified	✓	✓	✓	✓	✓	✓
B1.2 Payload delivered	✓	✓	✓	✓	✓	✓
B2 Malware deployment success	✓	✓	✓	✓	✓	✓
C1 Legitimate control disrupted	✓	✓	✓	✓	✓	✓
C2.1 Session control obtained	✓	✓	✓	✓	✓	✓
C2.2 Protocol handshake completed	✓	✓	✓	✓	✓	✓
C2.3.1 Correct IOAs	✓	✓	✓	✓	✓	✓
C2.3.2.1 CA predefined	✓		✓		✓	
C2.3.2.2 CA discovered		✓		✓		✓
C3.1 Correct command type	✓	✓	✓	✓	✓	✓
C3.2 Command sequence satisfied	✓	✓	✓	✓	✓	✓
C3.3 Control enabled	✓	✓	✓	✓	✓	✓
E1 Control authority overridden	✓	✓	✓	✓	✓	✓
E2 Operator control ineffective	✓	✓	✓	✓	✓	✓

In the context of the table, all minimal cut sets share a common core of events in Branches B, C, and E, meaning that malware deployment, IEC-104 command execution, and loss of OT control are always required to reach the Top Event. Variability among the cut sets arises only from Branch A, which represents alternative access paths to the OT environment, and from Branch C, where addressing may rely on either a predefined or dynamically discovered Common Address. This indicates that once OT access is achieved and the correct protocol is available, command execution becomes largely deterministic, depending on correct protocol interaction rather than on multiple alternative access paths. The presence of CA discovery variants further shows increased attacker efficiency, as successful command execution does not rely solely on complete prior knowledge of the target configuration.

5 | Event Tree Analysis (ETA)

5.1. ETA Construction

Given the identified MCSs from the FTA, we first attempt to simulate different scenarios using an Event Tree Analysis (ETA). This inductive process helps to visualize the possible consequences of the postulated event. Specifically, in our case, we aim to construct an ETA to assess the role of filters and barriers during the attack. As this is a risk governance analysis of a near-miss event, it is essential to understand where the attack can be stopped and, consequently, which defenses require greater attention during an attack.

We focus on a single main MCS, addressing all pivotal event splits and highlighting which barriers were effective and which were not during the *Industroyer2* attack. The selected set is MCS-2, based on the following assumptions:

- The attacker managed to obtain indirect OT access.
- *Industroyer2* was deployed.
- The IEC-104 command was ready to be correctly executed after correct addressing was discovered by the Sandworm group.

This set of events forms our Initiating Event (IE). Additionally:

- Branch D is directly integrated into the events, as we are analyzing possible
- Branch E is treated as the last pivotal event: if defenses fail, can we intervene to regain control of the OT environment?

Starting from the IE, six main outcome classes are simulated, depending on the effectiveness of the defense layer represented by each event split. If the defense is successful and the attack is interrupted, the flow proceeds upwards; if defenses are breached, the flow proceeds downwards.

Pivotal events are derived from the literature review, as well as from the FTA and MCS analyses. These events are five in total, and their outcomes correspond to the following interrogatives:

- **PE1**: The attack is not detected and interrupted through monitoring procedures.
- **PE2**: Valid IEC-104 commands are attempted.
- **PE3**: Breaker operations effectively disrupt the power flow.
- **PE4**: Operators do not quickly regain OT control.
- **PE5**: Destructive activity in IT/server environments (e.g., wiping) and supporting disruption slow down the recovery process.

A severity score (0 = null, 1 = partial, 2 = total) is assigned to each outcome. The highlighted green flow represents the sequence of events observed during the *Industroyer2* attack.

Additionally, we attempted to represent the original 2016 *Industroyer* attack using the highlighted red flow. While we acknowledge that the defensive procedures, protocols, and tools of the critical infrastructure have evolved, along with the nature of the attack, we consider this simplified schema useful for visualizing differences in cybersecurity measures between the two incidents (i.e., which defenses improved compared to the previous attack).

5.2. ETA Schema

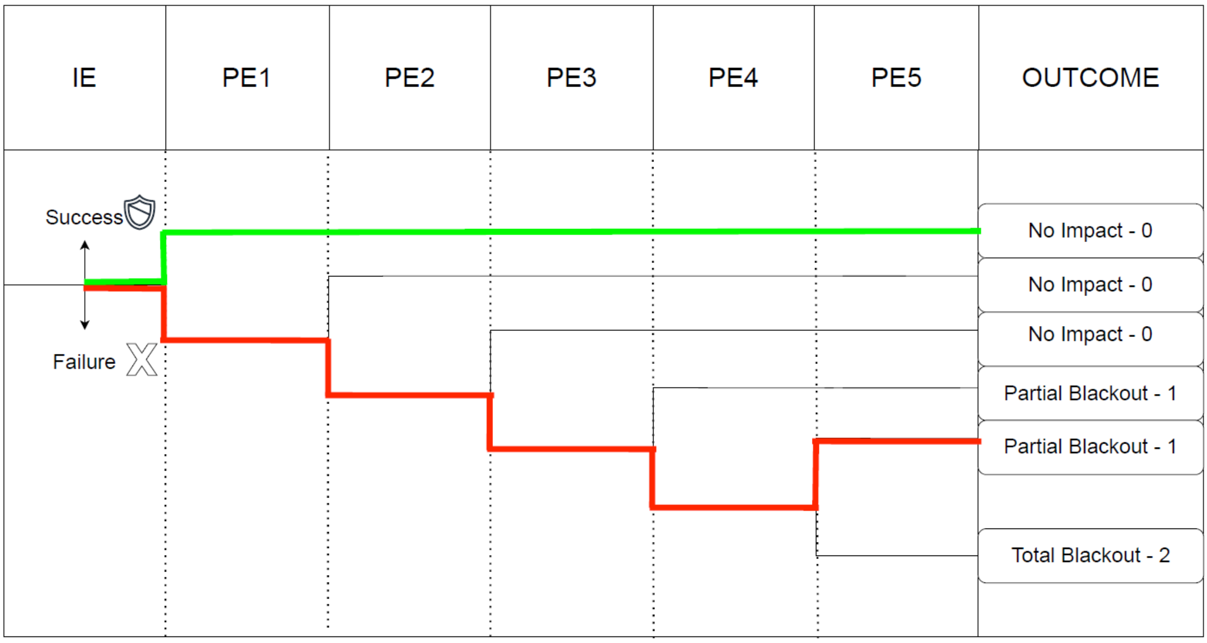


Figure 5.1: ETA schema

6 | Failure Mode Effect Analysis (FMEA)

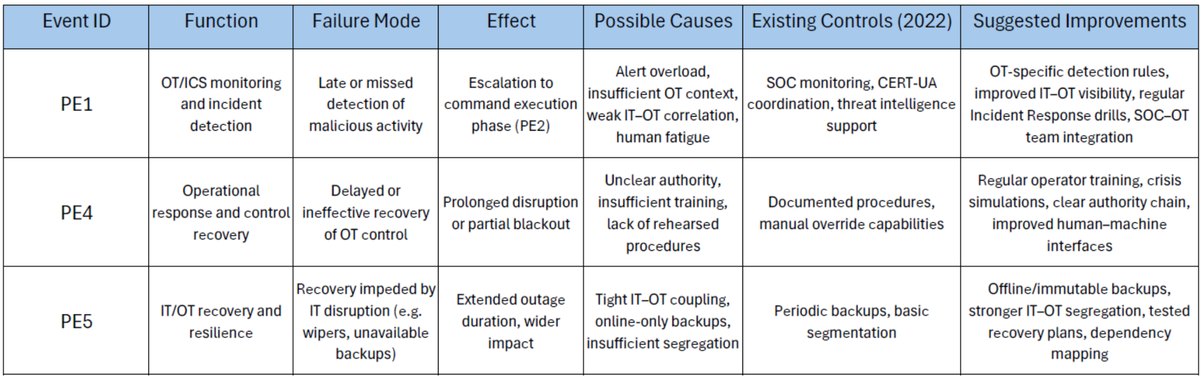
6.1. Construction of Focused FMEA on Residual Vulnerabilities

A brief Failure Mode and Effects Analysis (FMEA) is conducted to understand and assess possible additional defensive mechanisms that were not exercised during the *Industroyer2* attack. Given that the attack was blocked after the first Pivotal Event (PE1), the other defensive measures were not activated. Starting from the MCS-2 derived from the FTA and the schema provided by the ETA, the FMEA is constructed with a focus on the Pivotal Events that are strongly influenceable by technology risk governance interventions.

Given that this event is a near-miss, we consider it fundamental to develop a clear understanding of the range of available defensive and recovery actions within the organization. For these reasons, PE2 and PE3 are not included in the FMEA, as they represent technical and physical transition points rather than primary defense barriers.

While technical safeguards and system resilience may reduce their likelihood or impact, these events are not fully preventable once the attacker reaches the command execution phase. Governance-oriented defenses are therefore more appropriately represented by the remaining Pivotal Events.

6.2. FMEA Schema



Event ID	Function	Failure Mode	Effect	Possible Causes	Existing Controls (2022)	Suggested Improvements
PE1	OT/ICS monitoring and incident detection	Late or missed detection of malicious activity	Escalation to command execution phase (PE2)	Alert overload, insufficient OT context, weak IT–OT correlation, human fatigue	SOC monitoring, CERT-UA coordination, threat intelligence support	OT-specific detection rules, improved IT–OT visibility, regular Incident Response drills, SOC–OT team integration
PE4	Operational response and control recovery	Delayed or ineffective recovery of OT control	Prolonged disruption or partial blackout	Unclear authority, insufficient training, lack of rehearsed procedures	Documented procedures, manual override capabilities	Regular operator training, crisis simulations, clear authority chain, improved human–machine interfaces
PE5	IT/OT recovery and resilience	Recovery impeded by IT disruption (e.g. wipers, unavailable backups)	Extended outage duration, wider impact	Tight IT–OT coupling, online-only backups, insufficient segregation	Periodic backups, basic segmentation	Offline/immutable backups, stronger IT–OT segregation, tested recovery plans, dependency mapping

Figure 6.1: FMEA schema

Existing controls are supported by different public sources online. Failure modes and effects are inferred by model-based risk analysis. The reported data are not absolute or exhaustive findings, but a useful starting point for identifying possible improvements.

7 | Human and Organizational Factors Analysis (HOF)

We reckon that a macroscopic Human and Organizational Factors (HOF) analysis is necessary to complement and deepen the topics treated both in Reason's model and in the technical schemas (FTA, ETA, FMEA). The analysis aims to highlight which organizational elements were crucial for the prompt blocking of the attack and to link them with the main regulatory frameworks (i.e., the NIST Cybersecurity Framework and ENISA Critical Infrastructure Resilience guidance). A first critical human and organizational factor concerns situational awareness. In complex OT environments, effective monitoring is not limited to the presence of technical detection tools, but depends on the ability of personnel to correctly interpret anomalous behaviors within their operational context and to understand their potential impact on physical processes. This view is consistent with the NIST Cybersecurity Framework, which explicitly identifies continuous monitoring and contextual awareness as core elements of the Detect function.

Furthermore, it is highlighted that OT monitoring requires protocol-aware visibility and close integration between IT security monitoring and operational technology expertise. The early interruption of the *Industroyer2* attack suggests that such organizational capabilities were sufficiently mature to detect and interpret malicious activity before command execution. Detection alone is insufficient if it is not followed by timely and authoritative decision-making. A second key HOF therefore concerns escalation and decision-making processes during incident response. The ability to reduce organizational latency through clear decision authority and effective communication is considered critical for emergencies such as the discovery of malware in the power grid. The prompt blocking of the malware suggests efficient and effective coordination between different defense teams (as previously noted, coordination between SOC and OT teams is crucial for detection in cyber-physical environments).

Additionally, recovery governance is crucial: wipers were employed by Sandworm to slow down the recovery process. Coordination prior to an attack is therefore essential, both between internal and external actors. ENISA guidance on critical infrastructure resilience emphasizes that such coordination must be established before incidents occur, through shared procedures, trusted communication channels, and joint preparedness activities.

From a near-miss perspective, the absence of recovery actions during the 2022 incident does not imply that recovery-related human and organizational factors are secondary. Training and preparedness represent latent organizational conditions in Reason's sense: they may remain invisible during normal operations but become critical when defenses are stressed. The NIST Cybersecurity Framework stresses the importance of regular training, exercises, and preparedness activities to ensure that personnel can respond effectively to incidents. Although these factors were not exercised during the *Industroyer2* attack due to early detection, they remain decisive in determining whether operators can regain control quickly and safely in scenarios where the attack breaks through one or more barriers. Additionally, effective recovery can be developed through organizational tools such as training and incident simulations.

Overall, this brief HOF analysis confirms that cyber resilience in critical infrastructures is a socio-technical property. The near-miss was strongly supported by organizational preparedness, decision-making structures, and coordination capabilities (both inter- and intra-organizational), as described in established cybersecurity governance frameworks.

8 | Final Takeaways

The *Industroyer2* cyberattack represents a very interesting case due to its near-miss nature and the cyber-physical architecture of the critical infrastructure involved. The analysis is also useful for comparison with the original 2016 *Industroyer* attack, which had concrete consequences for the power supply in the Kyiv region. The application of Reason's model, Fault Tree Analysis, and Event Tree Analysis showed that the decisive factor preventing physical impact in 2022 was not the absence of vulnerabilities, but rather the effectiveness and timely activation of defensive barriers. Additionally, we reckon that the FTA represents a useful foundational basis for all subsequent analyses, as it provides a simplified representation of the attack and the associated defenses. The ETA highlighted that early detection and interruption (PE1) constituted the most leverageable control, capable of stopping escalation before malicious control commands could be executed. This contrasts with the 2016 attack, where limited detection and response maturity allowed the hazard trajectory to progress to physical disruption. The focused FMEA further demonstrated that, even when early detection succeeds, residual vulnerabilities remain at the organizational and recovery levels. Recovery-related capabilities (PE4 and PE5), although not exercised during the 2022 near-miss, play a decisive role in determining the severity of worst-case scenarios. This confirms that resilience cannot rely exclusively on detection, but must also include preparedness for recovery under adverse conditions. The brief Human and Organizational Factors analysis reinforced this interpretation by showing that cyber resilience in critical infrastructures is a socio-technical property. The lessons learned from the incident analysis can be summarized in one brief sentence: prevention is key, but resilience must not be ignored. Vulnerabilities that made the attack possible, such as OT-IT interdependence, information leakage, and the complexity of OT environments, persist. However, from a Technology Risk Governance perspective, preventive measures and tested recovery governance represent key pillars for improving cyber resilience in critical infrastructures.

Bibliography

[1] Baiardi, F. (2022). *Industroyer2, perché l'attacco russo alla rete elettrica ucraina è così importante*. Agenda Digitale. Available at: `https://www.agendadigitale.eu/sicurezza/industroyer2-perche-lattacco-russo-alla-rete-elettrica-ucraina-e-cosi-importante/` (Accessed: 22 December 2025).

[2] Beccia, M. (2025). *Cybersecurity and Geopolitics: The New Battlefield of the Digital Age*.

[3] CERT-UA (2022). *Cyberattack group Sandworm (UAC-0082) on energy facilities in Ukraine using malicious programs INDUSTRIYER2 and CAADDYWIPER (CERT-UA#4435)*. Available at: `https://cert.gov.ua/article/39518` (Accessed: 22 December 2025).

[4] Cherepanov, A. (2017). *WIN32/INDUSTROYER: A New Threat for Industrial Control Systems*.

[5] Cisco IoT Security Research Lab (2022). *Mitigating New Industroyer2 and Incontroller Malware Targeting Industrial Control Systems*. Cisco Blogs. Available at: `https://blogs.cisco.com/industrial-iot/mitigating-new-industroyer2-and-incontroller-malware-targeting-industrial-control-systems` (Accessed: 22 December 2025).

[6] Council of the European Union and European Parliament (2022). *Directive (EU) 2022/2557 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC*. Available at: `https://www.europeansources.info/record/proposal-for-a-directive-on-the-resilience-of-critical-entities/` (Accessed: 24 December 2025).

[7] ENISA (2024). *Cybersecurity of Critical Sectors*. Available at: `https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors` (Accessed: 16 January 2026).

[8] ESET Research (2022). *Industroyer2: Industroyer Reloaded*. WeLiveSecurity. Avail-

able at: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Accessed: 22 December 2025).

[9] FortiGuard Labs (2025). *Threat Signal Report: Industroyer2 Discovered Attacking Critical Ukrainian Verticals.* Available at: https://www.fortiguard.com/threat-signal-report/4494/industroyer2-discovered-attacking-critical-ukrainian-verticals (Accessed: 22 December 2025).

[10] Hjelmvik, E. (2022). *Industroyer2 IEC-104 Analysis.* Netresec. Available at: https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis (Accessed: 22 December 2025).

[11] MITRE (2023). *Industroyer2, Software S1072.* MITRE ATT&CK for ICS. Available at: https://attack.mitre.org/software/S1072/ (Accessed: 22 December 2025).

[12] Nelson, A., Rekhi, S., Souppaya, M., and Scarfone, K. (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management.* NIST Special Publication 800-61r3. Available at: https://doi.org/10.6028/nist.sp.800-61r3.

[13] NIST (2025). *Cybersecurity Framework.* National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework (Accessed: 16 January 2026).

[14] Nozomi Networks Labs (2022). *Industroyer2: Nozomi Networks Labs Analyzes the IEC-104 Payload.* Available at: https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload (Accessed: 22 December 2025).

[15] Pajani, G., and Peix, P. (2022). *Industroyer 2: The Russian Cyberattack on Ukrainian Infrastructure.* HeadMind Partners. Available at: https://www.headmind.com/industroyer-2/ (Accessed: 22 December 2025).

[16] Pereira, D. (2024). *Industroyer2 and Pipedream ICS/SCADA Malware: DOE, CISA, NSA, and the FBI Release Joint Cybersecurity Advisory.* OODAloop. Available at: https://oodaloop.com/analysis/archive/industroyer2-and-pipedream-ics-scada-malware-doe-cisa-nsa-and-the-fbi-release-joint-cybersecurity-advisory/ (Accessed: 22 December 2025).

[17] Splunk (2025). *Detection: Windows Processes Killed by Industroyer2 Malware.* Splunk Security Content. Available at: https://research.splunk.com/endpoint/d8bea5ca-9d4a-4249-8b56-64a619109835/ (Accessed: 22 December 2025).

[18] Team82 (2022). *Industroyer2 Variant Surfaces in Foiled Attack Against Ukraine Elec-*

tricity Provider. Claroty. Available at: `https://claroty.com/team82/blog/industroyer2-variant-surfaces-in-foiled-attack-against-ukraine-electricity-provider` (Accessed: 15 January 2026).

[19] U.S. Department of Justice (2020). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. Available at: `https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and` (Accessed: 24 December 2025).

[20] Uchill, J. (2022). *Researchers Believe Russian Group Tried to Blackout Ukraine with Updated Industroyer*. SC Media. Available at: `https://www.scworld.com/analysis/russia-allegedly-targeted-ukrainian-energy-with-updated-destructive-industroyer` (Accessed: 24 December 2025).