framatome cybersecurity



Industrial Cyber-attacks: Post Triton Era

Framatome Cybersecurity

Peter Kirsner

21 October 2026

Table of content

1. Why OT Cybersecurity Matters
2. Evolution of Industrial Cyberattacks
3. Poland Power Grid Attack
4. Resilience Priorities and Take Aways

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

1

Why OT Cybersecurity Matter

From emerging threat to operational reality

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Why this topic today ? Why Framatome ?

From Triton to the Poland Grid attack: a new reality for critical infrastructure

- Threat actors have demonstrated the ability to target industrial operations and safety-critical environments.
- Organizations must move beyond detection and focus on operational resilience, safety protection, and business continuity.

Bridging cybersecurity objectives and industrial realities

- Framatome Cybersecurity combines deep industrial and cybersecurity expertise to secure mission-critical environments.
- We translate regulatory and security requirements into practical, auditable, and operationally sustainable solutions.
- Our approach ensures cybersecurity objectives are achieved without compromising safety, availability, or operational performance for a plant lifetime.

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

ICS Scope

An Industrial Control System (ICS) consists of combinations of control components (...) that act together to achieve an industrial objective" (NIST 800-82 r3)

Present in many sectors of activity:

- Energy (production, distribution)
- Chemical and Manufacturing Industries
- Transport
- Treatment of water...



framatome cybersecurity

 © Framatome - All rights reserved

2

Evolution of Industrial Cyberattacks

A clear change in attacker doctrine

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

From Stuxnet to Triton: Escalation of OT Threats

2010	2016	2016	2017
Stuxnet	**Industroyer**	**Wannacry / Petya**	**TRITON**
APT/ Sabotage	APT/ Sabotage	Ransomware	APT/ Sabotage
1st malware targeting an ICS. Crosses the air-gap via USB stick to destroy Iranian nuclear centrifuges	1st malware using native OT protocols (IEC 104, IEC 61850). Power outage in Kiev	Exploitation of a Windows flaw and paralyzing thousands of companies, hospitals and infrastructures worldwide	Targets safety instrumented systems (SIS). Designed to cause physical accidents



2021	2022	2025	2025
Colonial Pipeline	**Industroyer 2**	**Poland Power Grid**	**Jaguar Land Rover**
Ransomware	Wiper/ APT	Wiper APT	Ransomware
Ransomware on IT causes the preventive shutdown of the OT. 6 days of fuel blackout on the US East Coast	Improved version targeting Ukrainian substations. Wiper deployed in parallel at suppliers	Attack on the Polish power grid via compromised VPN. Partial shutdown of a 230kV operator	Major cyberattack against an industrialist, leading to the shutdown of factories and industrial disruptions

framatome cybersecurity

 © Framatome - All rights reserved

3

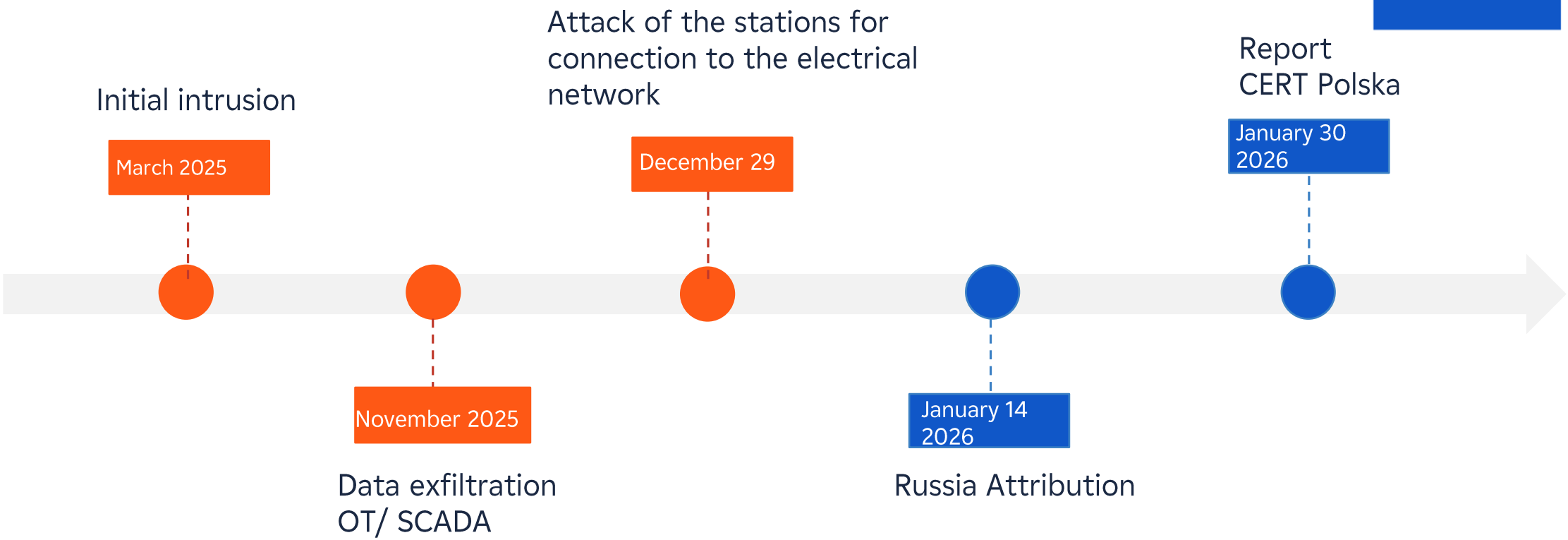
Poland Power Grid Attack

Lessons from a contemporary OT intrusion path

framatome cybersecurity

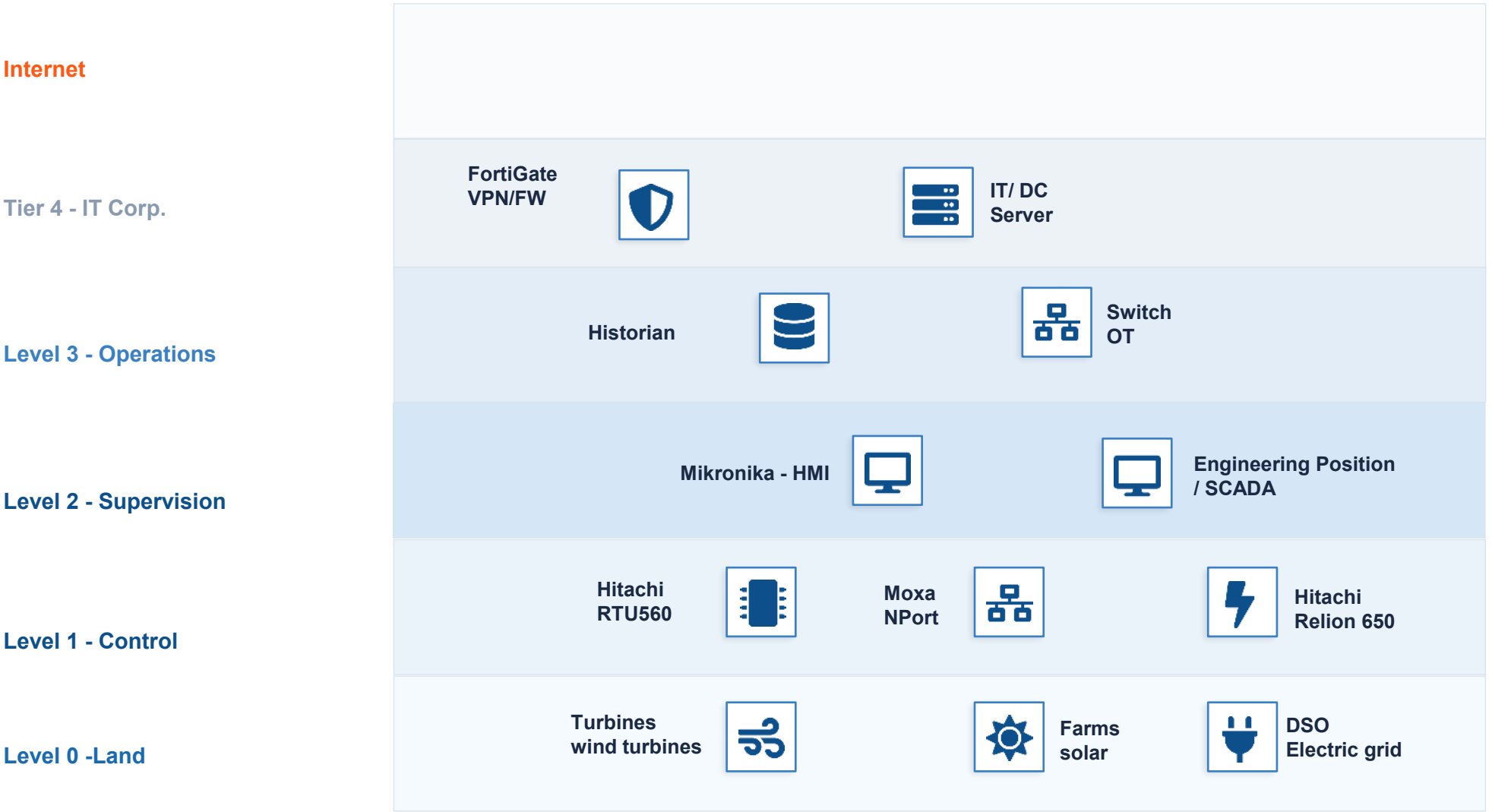
 © Framatome - All rights reserved

Focus: Poland, power grid attack



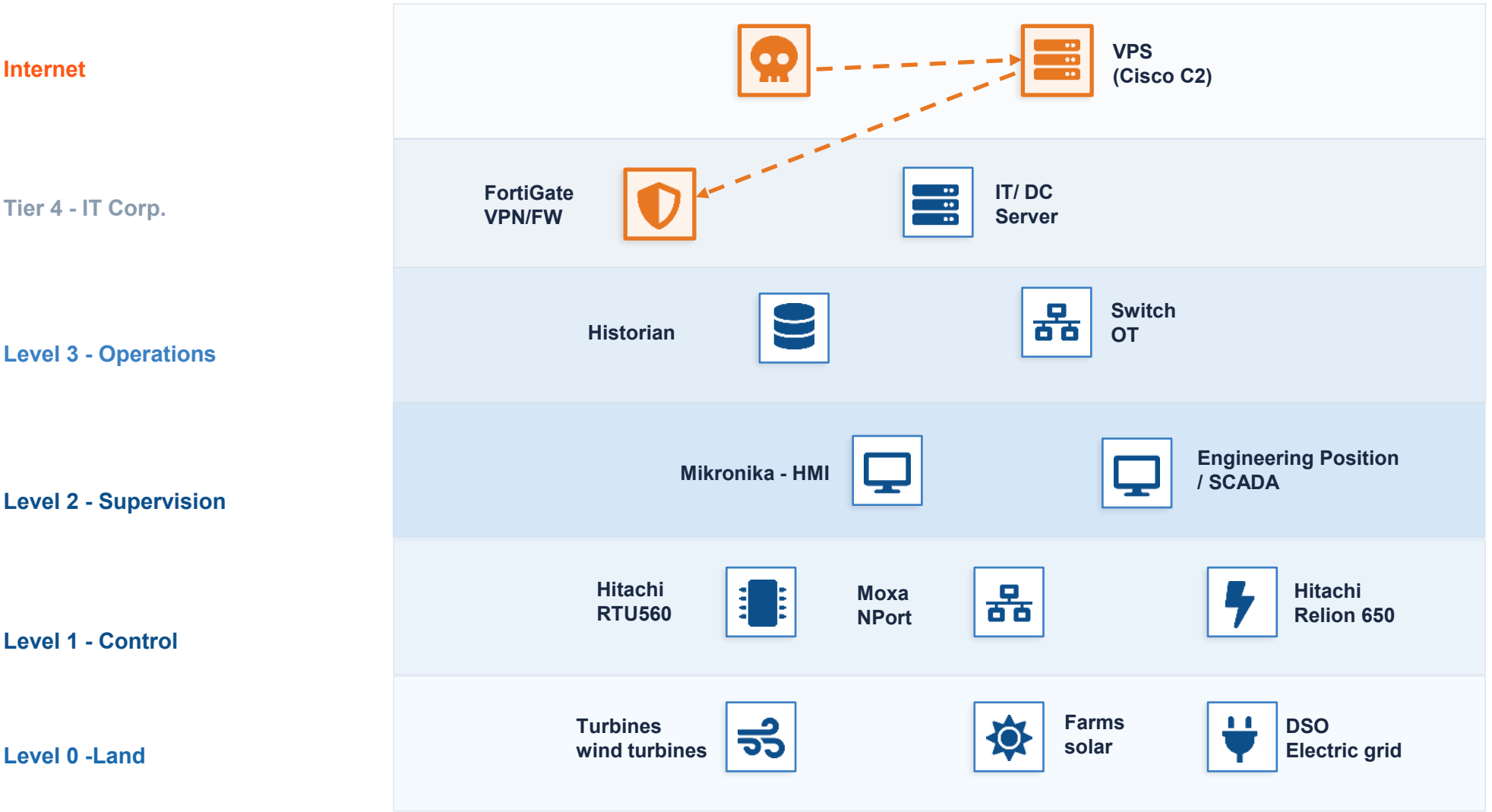
Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack



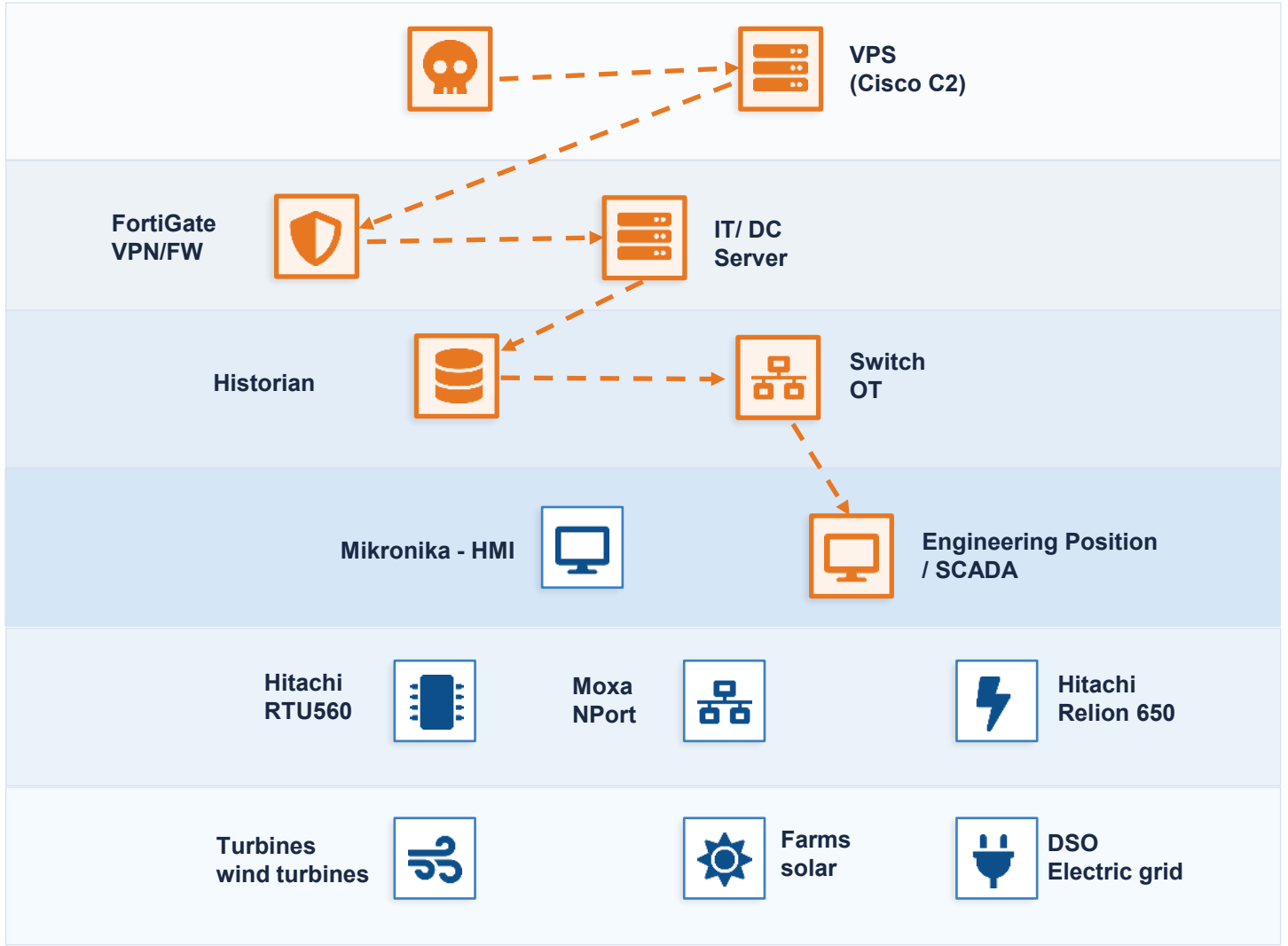
Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack



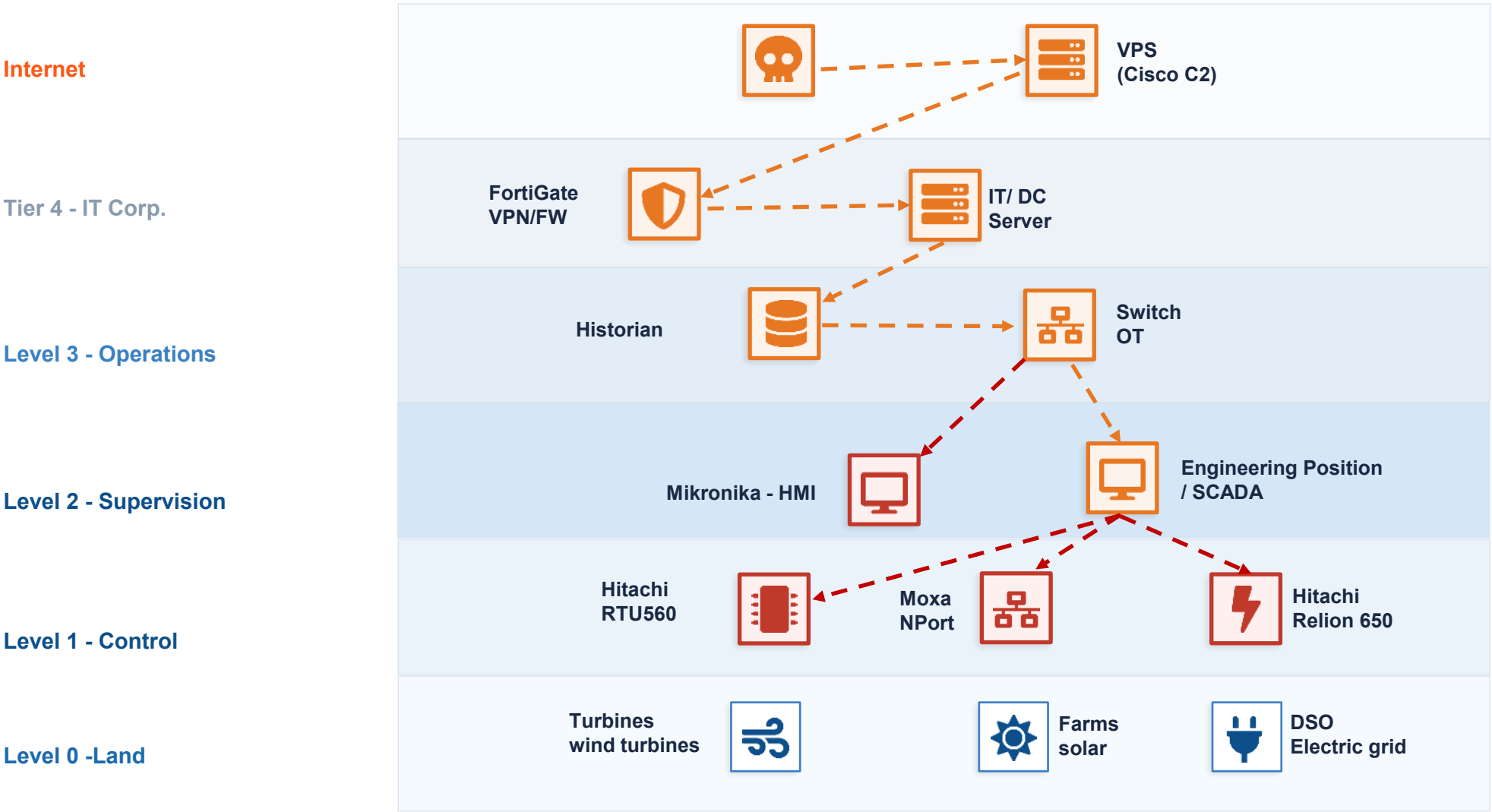
Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack



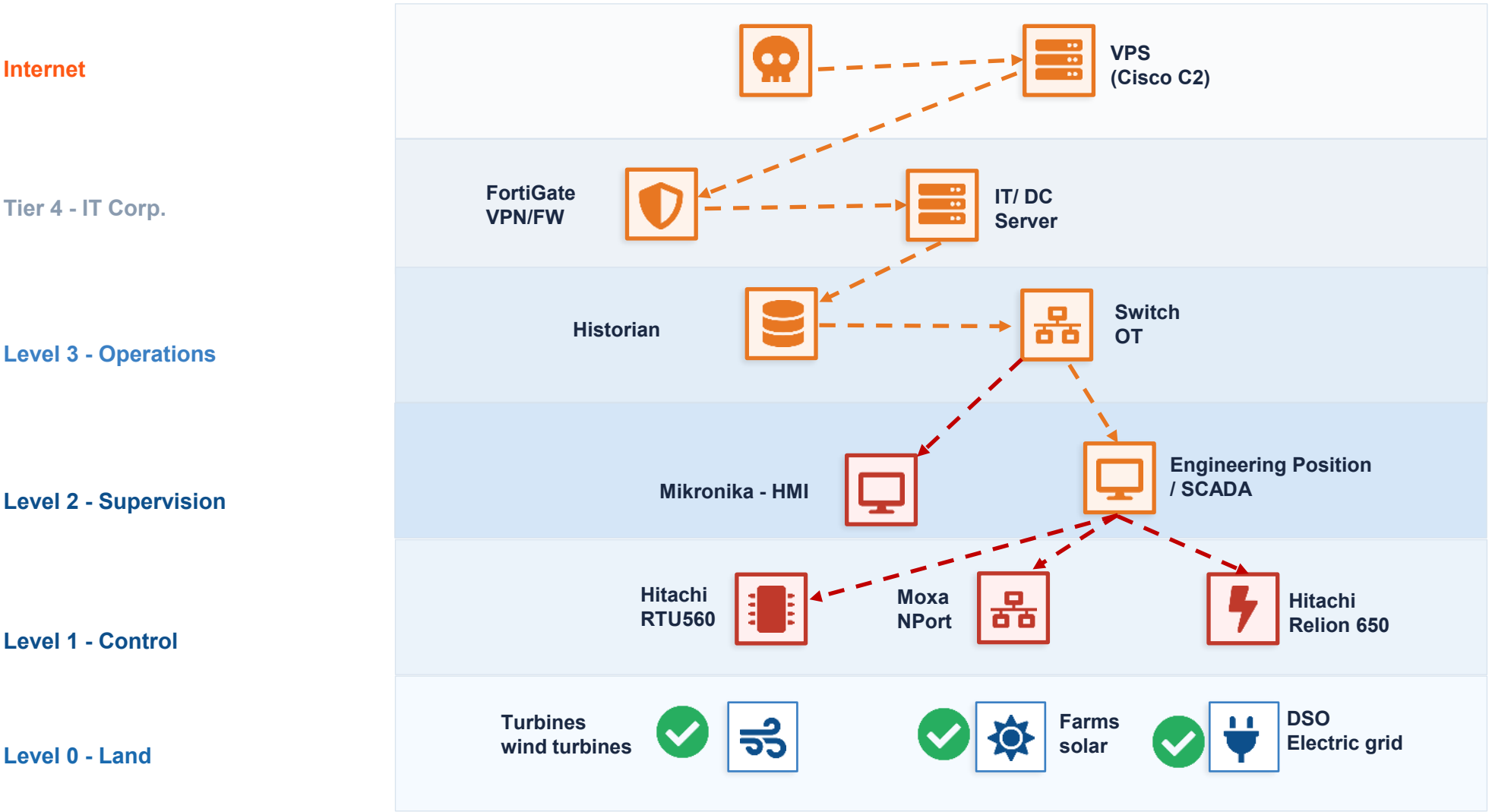
Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack



Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack



Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Focus: Poland, power grid attack

Fundamentals were not applied

- Absence of MFA on all remote access interfaces (VPN, RDP, SSH)
- Default passwords on OT equipment
- Absence of IT/OT segmentation and active monitoring of inter-segment traffic
- Lack of Integrity Firmware and Inventory Verification

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

4

Resilience Priorities and Take aways

Detect, protect, react and recover

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Resilience as a cornerstone

Are your processes resilient enough to detect and recover from an OT attack?

Organize

(Secure operating procedures, SLA...)

Protect/ Detect

(Hardening, Segregation, Log Collection and analysis)

React

(Incident Management, PCA)

Anticipating reconstruction

(PRA, Configuration management, Backups...)

framatome cybersecurity

 © Framatome - All rights reserved



Framatome Cybersecurity: Protecting What powers the world

Leveraging its position as a global leader in the nuclear industry and its cybersecurity expertise, Framatome develops solutions that protect nuclear and other critical infrastructure while ensuring safety, security, and cyber resilience.

Who Are We:

- 260+ cybersecurity experts
- 1000+ Critical infrastructure customers
- Global presence
- Ecosystem of cybersecurity vendors:

allentis cyberwatch foxguard

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Our Nuclear customer references



Cyber Program Build for a Nuclear research reactor



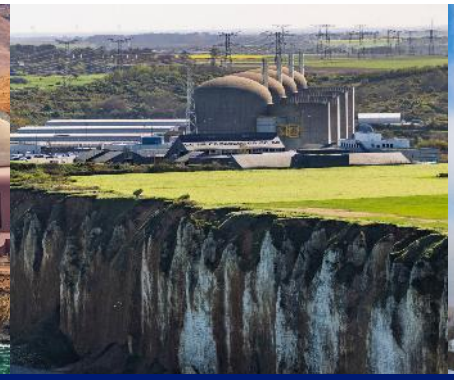
Governance & compliance for a Nuclear Power Plant



Technical audit for a Nuclear research reactor



Cybersecurity drill for a Nuclear Power Plant



System risk analysis for Nuclear Power Plants



System hardening for Nuclear Power Plants



Digital systems obsolescence management for Nuclear Power Plants



Firewall Upgrade for Nuclear Power Plants



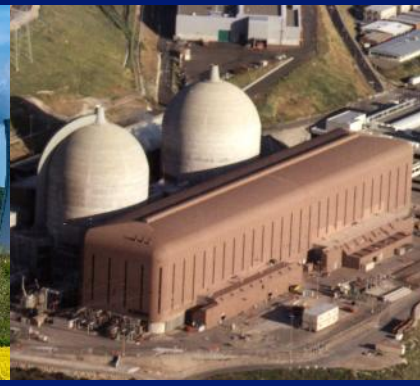
Sensitive systems Homologation support for a Nuclear plant



Risk analysis & Vulnerability Operation Center for a Nuclear Power Plant



Asset & Vulnerability Management for a Nuclear Power Plant



CSAT support for a Nuclear Power Plant

framatome cybersecurity

Post Triton OT Cyberattacks - 21/06/2026 © Framatome - All rights reserved

Thank you

Contact Us:
cyber-services@framatome.com

Find out more:
Cybersecurity - Framatome Solutions Portfolio