

BLACK START · THREAT TAXONOMY · VERSION 1.0 · 3 NOVEMBER 2026

CRITICAL INFRASTRUCTURE (CYBERWARFARE) THREAT TAXONOMY

The reference for the Black Start card game. 231 entries: 17 suits of 13 and 10 Trumps.

© 2026 Jonathan Brett Crawley · Licensed under CC BY-NC-ND 4.0 with additional permissions

Share it unchanged, with credit, for non-commercial use. Threat modeling with it, internal training and quoting entries with credit are allowed.

Ask before shipping it in a product. Full terms on page 3. https://ostering.com/taxonomies/critical-infrastructure/

About this taxonomy

This is the reference for the Black Start card game: every card's threat, the mitigation principle a sound design follows, design measures, and mappings to STRIDE, CAPEC, CWE, MITRE ATT&CK for ICS and the Cyber-Informed Engineering principles.

It covers the systems that keep a country fed, watered, heated, moving and paid: food retail and the cold chain, water and wastewater, electricity, gas, fuel, transport and logistics, payments, and the platforms that run them remotely. It is written for the people who design, buy, integrate and operate those systems, and it is jurisdiction-neutral.

The adversary is a state, or acting for one. It is patient and well resourced, and it wants an effect: disruption, destruction, coercion or a loss of public confidence, not money. A criminal wants one victim to pay. A state wants many sites to fail at once, at a moment it chooses, for as long as possible, and wants to deny it did it.

Two decks, 17 suits and 10 Trumps

The Campaign: what the adversary does	**The Estate**: what is being defended	**Both decks**
RM Reconnaissance and Mapping	**FD** Field Devices and Controllers	**TR** Trumps: structural hazards, ranked 1 to 10
PP Pre-positioning	**CC** Control Centre and SCADA	
SC Service Chain	**FM** Fleet Management Platforms	
PE Process Effects	**RA** Remote and Vendor Access	
ST Scale and Timing	**TT** Telecoms and Timing	
RD Recovery Denial	**LS** Logistics and Supply	
AD Aftermath and Deniability	**TN** Transport Networks	
AS Air and Spectrum	**IX** Interdependencies	
	MP Money and Payments	

References

Each reference is the game prefix BKS, the suit code and a playing-card rank from Ace down to 2, or 1 to 10 for the Trumps, joined by hyphens: BKS-PE-A, BKS-TR-4. It is the same reference as the card. In the game the ranks follow severity; here a reference only names an entry. The ranks are frozen: an entry added later between two ranks takes an intermediate value, such as BKS-PE-3.1, so no published reference ever changes.

How the mappings were checked

Every identifier was checked against MITRE's own data: ATT&CK for ICS v20.0 (October 2026), CAPEC 3.9 and CWE 5.0 (28 October 2026). Revoked and deprecated entries were excluded, and only CWEs whose mapping usage is Allowed or Allowed-with-Review were used. CIE numbers follow the DOE Cyber-Informed Engineering Implementation Guide v1.0. Where they fit, entries also cite IEC 61000-4-36 and IEC TS 61000-5-10 (intentional electromagnetic interference), CLC/TS 50701 (railway cybersecurity) and IEC 62443.

Scope

Home energy devices are in the Smart Home Threat Taxonomy, vendors' build and release pipelines in the Software Factory taxonomy, and AI agents in control rooms in the AI and Agentic Systems Threat Taxonomy. This taxonomy picks those up only where they become a route into, or a consequence for, the essential service. State theft from banks and crypto platforms for revenue is out of scope; attacks on payments meant to disrupt are in Money and Payments.

Licence

© 2026 Jonathan Brett Crawley. This taxonomy is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0), with the additional permissions below. You can share the whole taxonomy freely for non-commercial purposes, unchanged and with credit.

Use	Permission needed?
Sharing the whole taxonomy non-commercially (OWASP, universities, conferences, individuals)	No
Threat modeling with it, including for paying clients	No
Internal use and training inside any organisation	No
Quoting entries, with credit, in paid courses, reports and talks	No
Shipping the taxonomy in a product: a tool's built-in library, a printed deck, a reprint for sale	Yes, ask me

Additional permissions. In addition to the rights the licence gives, and whether or not the use is commercial, the copyright holder grants you permission to:

- Use the taxonomy to threat model systems you build, operate or assess, including for paying clients;
- Use it internally, and for training, inside any organisation;
- Quote individual entries, with credit, in paid courses, reports, findings and talks.

Any other commercial use, including shipping the taxonomy or a substantial part of it in a product (a tool's built-in library, a printed deck, a reprint for sale), needs written permission. Ask me on LinkedIn.

Credit: “Critical Infrastructure (Cyberwarfare) Threat Taxonomy” by Jonathan Brett Crawley, ostering.com, licensed under CC BY-NC-ND 4.0.

These additional permissions are given alongside the licence. They add to what the licence allows and do not take anything away from it.

Licence text: https://creativecommons.org/licenses/by-nc-nd/4.0/

How to read an entry

Reference: game prefix, suit and rank. **Threat**: the design weakness and what it leads to, written against the system you are reviewing, with any public case that illustrates it. **Principle and design measures**: the mitigation principle a sound design follows, then three concrete measures (four where one more was needed). **Mappings**: STRIDE; CAPEC; CWE; ATT&CK for ICS; the CIE principles, the main one first; and standards where they fit. A dash means nothing fitted well: a loose tag would mislead.

† marks an entry with a physical-safety consequence: fire, poisoning, flooding, explosion, or loss of heat, water or transport safety.

STRIDE letters: S Spoofing, T Tampering, R Repudiation, I Information disclosure, D Denial of service, E Elevation of privilege.

Cyber-Informed Engineering principles

1	Consequence-Focused Design	**7**	Interdependency Evaluation
2	Engineered Controls	**8**	Digital Asset Awareness
3	Secure Information Architecture	**9**	Cyber-Secure Supply Chain Controls
4	Design Simplification	**10**	Planned Resilience
5	Layered Defenses	**11**	Engineering Information Control
6	Active Defense	**12**	Organizational Culture

Many entries in Aftermath and Deniability, Scale and Timing, Interdependencies and Money and Payments have no CAPEC, CWE or ATT&CK for ICS mapping. That is a finding in itself: those frameworks describe techniques and weaknesses, not the campaign a state wages around them.

RM · RECONNAISSANCE AND MAPPING

THE CAMPAIGN · BKS-RM-A TO BKS-RM-2 · https://ostering.com/taxonomies/critical-infrastructure/reconnaissance-and-mapping/

How the estate becomes knowable: what an adversary learns about sites, devices, vendors and people before touching anything.

BKS-RM-A Exposed controllers become a target list
BKS-RM-K Fleet commonality is public knowledge
BKS-RM-Q Advisories outpace patching
BKS-RM-J Engineering detail in public filings
BKS-RM-10 Open data maps the cascade
BKS-RM-9 Leaked files from earlier breaches
BKS-RM-8 The defenders' response is measured
BKS-RM-7 Live telemetry shows the effect
BKS-RM-6 Probing spread too thin to see
BKS-RM-5 Contractors advertise the estate
BKS-RM-4 People and rotas are mappable
BKS-RM-3 Unmanned sites surveyed in person
BKS-RM-2 Radio links readable from the road

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RM-A	**Exposed controllers become a target list** Controllers, HMIs and site managers reachable from the internet answer device search engines with their model and firmware. The adversary builds a list of every site sharing one weakness and can act on all of them at once. *Case: Unitronics PLCs at water utilities, 2023; Supermarket refrigeration attacks, 2026.*	**No control or supervisory interface is reachable from the public internet, and the operator knows what its own estate exposes.** **1** Remove every control interface from direct internet reach; put remote use behind an authenticated broker with MFA. **2** Run continuous external exposure scans of your own address space and your vendors' ranges, and act on findings within days. **3** Require suppliers to ship controllers with remote interfaces disabled until a named owner enables them.	STRIDE I CAPEC CAPEC-310, CAPEC-541 CWE CWE-1327, CWE-497 ATT&CK ICS T0883 CIE 3, 8
BKS-RM-K	**Fleet commonality is public knowledge** Vendor case studies, press releases and banners show that many operators, across companies and countries, run the same platform and version. One capability against that platform becomes an option at national or regional scale. *Case: Supermarket refrigeration attacks, 2026.*	**Treat shared platforms as a common-mode risk and keep what you run, and how widely, out of public material.** **1** Agree with vendors that reference lists, case studies and logos need your consent and omit versions and site counts. **2** Record platform commonality across your estate and sector in the risk register as a single common-mode exposure. **3** Keep a second, diverse means of control or protection for functions that would fail everywhere at once.	STRIDE I CAPEC CAPEC-169 CWE CWE-1230 ATT&CK ICS – CIE 11, 8, 1
BKS-RM-Q	**Advisories outpace patching** A published advisory tells every adversary which product and version is weak, and exposure data tells them where it runs. Operators who need months to test and schedule changes stay exposed long after the attack can be built. *Case: Danish energy sector, 2023.*	**The time from advisory to protection is designed and measured, with compensating controls that do not wait for a patch.** **1** Pre-approve compensating controls per asset class (isolate, block port, disable service) that can be applied within 48 hours. **2** Subscribe to vendor and national advisories and map each to affected assets automatically from the asset inventory. **3** Track and report the median and worst time from advisory to protection for exposed assets.	STRIDE I, E CAPEC CAPEC-310 CWE CWE-1104, CWE-1395 ATT&CK ICS T0819, T0883 CIE 8, 6
BKS-RM-J	**Engineering detail in public filings** Tenders, planning applications, regulatory submissions and grant reports carry network diagrams, single-line diagrams, P&IDs and control philosophies. The adversary assembles a target pack without touching the network.	**Engineering information is classified and released on a need-to-know basis, including to bidders and regulators.** **1** Classify engineering documents and redact network, protection and control detail from anything published or sent to open tender. **2** Release full drawings to shortlisted bidders only, under NDA, through a tracked data room. **3** Review regulatory and planning submissions for control-system detail before they are filed.	STRIDE I CAPEC CAPEC-169 CWE – ATT&CK ICS – CIE 11

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RM-10	**Open data maps the cascade** Outage maps, GIS layers, service territories and lists of critical customers show which substation feeds which pumping station, hospital or distribution centre. The adversary chooses the few nodes whose loss cascades furthest.	**Interdependency information is treated as sensitive in aggregate, even when each piece is public on its own.** 1 Assess published datasets together for what they reveal about critical dependencies, not one at a time. 2 Publish outage and network data at a resolution that serves the public without identifying single critical nodes. 3 Keep critical-customer and priority-restoration lists out of public and shared systems.	STRIDE I CAPEC CAPEC-169 CWE – ATT&CK ICS – CIE 7, 11
BKS-RM-9	**Leaked files from earlier breaches** Engineering files, drawings and passwords stolen in a criminal ransomware attack are published on leak sites. A state adversary picks them up years later and uses them as reconnaissance, against systems the operator assumed were unaffected.	**A data breach is treated as an engineering exposure: what leaked is assessed for what it lets an adversary do to the process.** 1 After any breach, list the engineering documents and credentials taken and rotate or redesign what they expose. 2 Monitor leak sites and criminal markets for your own and your integrators' data. 3 Keep engineering data off general file shares so a routine IT breach cannot reach it.	STRIDE I CAPEC CAPEC-150 CWE CWE-552, CWE-256 ATT&CK ICS T0882 CIE 11, 6
BKS-RM-8	**The defenders' response is measured** Small anomalies, false alarms or a single forced fault let the adversary learn how fast the operator notices, who responds, and which sites are watched at night. The real attack is then timed and placed where response is slowest.	**Unexplained minor anomalies are investigated as possible probes, and response capability does not have predictable gaps.** 1 Log and review unexplained small faults, resets and alarms across sites for patterns, not only one by one. 2 Vary on-call and patrol patterns and test night and weekend response regularly. 3 Share probe indicators with sector peers so an adversary measuring many operators is seen.	STRIDE I CAPEC CAPEC-169 CWE CWE-778 ATT&CK ICS T0868, T0801 CIE 6, 12
BKS-RM-7	**Live telemetry shows the effect** Public dashboards, customer apps and open APIs publish reservoir levels, charger availability, store status or grid load in real time. The adversary uses them to choose timing and to confirm the damage done without staying inside the network.	**Public service information is delayed, aggregated or authenticated so it cannot serve as the adversary's targeting and damage assessment.** 1 Delay or aggregate public operational data so it shows service status, not live process state. 2 Authenticate and rate-limit APIs that expose site-level telemetry, and watch for scraping. 3 Plan to reduce public data detail during an incident or heightened threat.	STRIDE I CAPEC CAPEC-169 CWE CWE-497 ATT&CK ICS – CIE 3, 11

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RM-6	**Probing spread too thin to see** Credential guessing and protocol probing run at a very low rate against many sites and many operators. Each sees a little noise, nobody adds it up, and the adversary validates access across the sector unnoticed.	**Probing is detected across sites and across operators, not only by thresholds at a single site.** 1 Collect authentication failures and protocol errors from all sites centrally and alert on slow, distributed patterns. 2 Lock or slow authentication on field and edge devices after repeated failures from any source. 3 Exchange probing indicators through the sector's information-sharing body.	STRIDE I, S CAPEC CAPEC-565, CAPEC-300 CWE CWE-307, CWE-778 ATT&CK ICS T0846 CIE 6
BKS-RM-5	**Contractors advertise the estate** Integrators' portfolios, staff profiles, conference talks and job adverts name the sites, systems, versions and remote access methods they work on. The adversary learns the estate and who to target to reach it.	**Suppliers are contractually bound to the same information controls as the operator.** 1 Write publication limits into supplier contracts: no site names, versions or access methods without consent. 2 Review job adverts and conference submissions for control-system detail before publication. 3 Check periodically what suppliers and staff publish about your estate.	STRIDE I CAPEC CAPEC-410, CAPEC-169 CWE – ATT&CK ICS – CIE 11, 9
BKS-RM-4	**People and rotas are mappable** Who operates the control room, who holds administrator rights and who is on call at night can be learned from public profiles and social media. Those people become targets for phishing or coercion, and thin cover shows when to strike.	**People with control-system privileges are protected as part of the system, and their role is not discoverable from outside.** 1 Advise privileged staff on what not to publish about their role, and give them a route to report approaches. 2 Give privileged staff phishing-resistant authentication and separate accounts for control-system work. 3 Avoid publishing rotas or on-call details outside the organisation.	STRIDE I, S CAPEC CAPEC-410, CAPEC-163 CWE – ATT&CK ICS T0865 CIE 12, 11
BKS-RM-3	**Unmanned sites surveyed in person** Pump stations, substations and cabinets with no cameras or alarms can be visited at will. Labels, modem details, Wi-Fi names and lock types are recorded, and the visit sets up hybrid physical and cyber options later.	**Unmanned sites detect and report physical access, and nothing visible on site helps an attacker.** 1 Fit door and cabinet intrusion detection that alarms to the control room. 2 Remove identifying labels, network details and default Wi-Fi names visible from outside the cabinet. 3 Review site camera footage and access logs after unexplained alarms or visits.	STRIDE I CAPEC CAPEC-390 CWE CWE-1263 ATT&CK ICS – CIE 5, 2
BKS-RM-2	**Radio links readable from the road** Telemetry radio, Wi-Fi on controllers and unencrypted links between sites can be received from nearby. The adversary learns the protocol, the addresses and the normal traffic, and prepares to inject or jam later.	**Radio links carrying control or telemetry are encrypted and authenticated, and the operator knows what each site emits.** 1 Encrypt and authenticate telemetry radio and site Wi-Fi; disable controller Wi-Fi not in use. 2 Survey the radio emissions of each site type and remove unexpected ones. 3 Choose radio systems that report jamming and unknown transmitters.	STRIDE I CAPEC CAPEC-157 CWE CWE-319 ATT&CK ICS T0887 CIE 3, 8

PP · PRE-POSITIONING

THE CAMPAIGN · BKS-PP-A TO BKS-PP-2 · https://ostering.com/taxonomies/critical-infrastructure/pre-positioning/

Access taken in peacetime and held for a crisis: where it hides, how it survives, and how it is staged towards the process.

BKS-PP-A Access held for a crisis
BKS-PP-K Edge devices as home
BKS-PP-Q Dormant logic in controllers †
BKS-PP-J The IT-to-OT route is pre-built
BKS-PP-10 Firmware implants survive rebuilds
BKS-PP-9 Project files carry the implant †
BKS-PP-8 Living off the land
BKS-PP-7 Access borrowed from criminals
BKS-PP-6 Service accounts that never expire
BKS-PP-5 Logging gaps the adversary relies on
BKS-PP-4 Identities planted for later
BKS-PP-3 Traffic from inside your own country
BKS-PP-2 Forgotten remote tools

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PP-A	**Access held for a crisis** The adversary takes access to IT and OT networks and then does nothing visible for years, waiting for a crisis or a political moment. Detection designed to catch active intrusion never fires, and the access is ready to switch to disruption. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**Assume dormant access already exists, and hunt for it on a schedule rather than waiting for an alert.** **1** Run threat hunts against published state-actor techniques at least yearly and after each relevant advisory. **2** Baseline normal administrative behaviour and review accounts and sessions that deviate, even when quiet. **3** Design OT so that critical functions can be isolated from IT and remote access at short notice.	STRIDE S, E CAPEC CAPEC-560 CWE CWE-778 ATT&CK ICS T0859, T0886 CIE 6, 10
BKS-PP-K	**Edge devices as home** VPN concentrators, firewalls and routers are exposed, often unpatched, cannot run endpoint detection and keep few logs. The adversary enters through them and lives on them, outside the view of every other control. *Case: Volt Typhoon pre-positioning, 2024 advisory; Danish energy sector, 2023.*	**Devices at the boundary are monitored and maintained as critical assets, not as appliances.** **1** Send edge device logs and configuration changes to central collection, and alert on changes nobody requested. **2** Patch or mitigate edge devices first and fastest; replace models the vendor no longer supports. **3** Check edge device integrity against vendor tools or known-good images on a schedule.	STRIDE S, T, E CAPEC CAPEC-542 CWE CWE-778, CWE-1104 ATT&CK ICS T0819, T0822 CIE 6, 5
BKS-PP-Q	**Dormant logic in controllers †** A modified controller program carries a trigger, a date, a condition or a command, and behaves normally until then. Routine checks look at the running process, not the logic, so the change waits unseen until it fires. *Case: Stuxnet, 2010.*	**Controller logic is verified against an authoritative, signed version, not judged by how the process behaves.** **1** Compare controller programs with the approved version on a schedule and after every maintenance visit. **2** Store approved logic offline with hashes, and require two people to approve logic changes. **3** Use controllers with a physical run/program key and keep it in run.	STRIDE T, E CAPEC CAPEC-441 CWE CWE-511, CWE-506 ATT&CK ICS T0889, T0821 CIE 2, 8
BKS-PP-J	**The IT-to-OT route is pre-built** Before any effect is needed, the adversary collects jump-host credentials, finds dual-homed machines and changes firewall rules. The step from office network to control network is ready in advance, so action takes minutes. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**The path into OT is narrow, monitored, and cannot be prepared without someone noticing.** **1** Allow access into OT only through a dedicated, monitored broker with separate credentials and MFA. **2** Alert on any change to IT/OT firewall rules and review the rule set against a documented baseline. **3** Find and remove dual-homed hosts and unmanaged links between IT and OT.	STRIDE E, T CAPEC CAPEC-700 CWE CWE-653 ATT&CK ICS T0886, T0867, T0859 CIE 3, 5

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PP-10	**Firmware implants survive rebuilds** Implanted firmware in controllers, network devices or server management chips survives an operating system rebuild. Recovery reuses compromised hardware and the adversary keeps its place.	**Firmware integrity is verifiable from a trusted root, and recovery plans include hardware that cannot be trusted.** **1** Buy devices that verify signed firmware at boot from a hardware root of trust. **2** Record firmware versions and hashes and check them after incidents and before returning devices to service. **3** Hold spare hardware for critical functions so suspect devices can be replaced, not reflashed.	STRIDE T, E CAPEC CAPEC-638 CWE CWE-1326, CWE-347 ATT&CK ICS T1693 CIE 2, 10
BKS-PP-9	**Project files carry the implant †** Infected project files on an engineering workstation are carried to controllers at the next routine download. The engineering process itself spreads the adversary's change. *Case: Stuxnet, 2010.*	**Project files are integrity-checked and engineering workstations are dedicated and controlled.** **1** Keep project files in a version-controlled repository with hashes, and verify before download to a controller. **2** Dedicate engineering workstations to engineering work, with no email or web browsing. **3** Scan and verify project files received from integrators before use.	STRIDE T CAPEC CAPEC-441 CWE CWE-494, CWE-353 ATT&CK ICS T0873, T0843 CIE 11, 2
BKS-PP-8	**Living off the land** The adversary uses built-in administration tools and legitimate accounts rather than malware. Detection tuned for malicious files sees nothing unusual, and the activity looks like routine administration. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**Detection is based on behaviour and context, not only on known-bad files.** **1** Restrict administrative tools on OT hosts to named accounts and approved hosts. **2** Log command-line and remote-session activity and alert on administrative use at unusual times or from unusual hosts. **3** Follow national living-off-the-land guidance and test detections against its techniques.	STRIDE E, R CAPEC CAPEC-560 CWE CWE-778 ATT&CK ICS T0859, T1701 CIE 6
BKS-PP-7	**Access borrowed from criminals** Footholds bought from access brokers or taken over from a ransomware intrusion give the adversary deniable access. Operators treat the criminal incident as closed once systems are restored and do not look for what stayed behind.	**Every intrusion, whatever its apparent motive, is followed by a hunt for persistence.** **1** After any intrusion, hunt for persistence in IT, edge devices and OT before declaring recovery complete. **2** Rotate every credential that could have been exposed, including service and vendor accounts. **3** Report criminal intrusions to the national authority so links to state activity can be made.	STRIDE S, E CAPEC CAPEC-555 CWE – ATT&CK ICS T0859, T0822 CIE 6, 12
BKS-PP-6	**Service accounts that never expire** Vendor, integrator and service accounts keep standing privileges, are never rotated and are often shared across sites. Once taken, they give the adversary lasting, legitimate-looking access.	**Privileged and service accounts are owned, scoped, time-limited and rotated.** **1** Give every service and vendor account a named owner, a scope and an expiry date. **2** Rotate service credentials automatically and on staff or supplier change. **3** Grant vendor privileges just in time, for the session, rather than standing.	STRIDE S, E CAPEC CAPEC-560 CWE CWE-262, CWE-798 ATT&CK ICS T0859, T1694 CIE 9, 3

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PP-5	**Logging gaps the adversary relies on** OT hosts and devices keep little or no log, logs are local and overwritten, and nothing is collected centrally. The adversary deletes what exists, and after an incident nobody can tell what happened. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**Security-relevant events from OT and edge devices are collected off the device and kept long enough to investigate years-long intrusions.** **1** Forward logs from OT hosts, edge devices and controllers that support it to a protected central store. **2** Keep logs for at least the dwell times seen in state-actor intrusions, which can be years. **3** Alert when a source stops sending logs.	STRIDE R CAPEC CAPEC-268, CAPEC-571 CWE CWE-778, CWE-223 ATT&CK ICS T0872 CIE 6, 8
BKS-PP-4	**Identities planted for later** The adversary adds its own accounts, SSH keys, certificates, API tokens or VPN profiles. Nobody reconciles identities against an authoritative list, so the additions stay.	**Every identity and credential in OT is reconciled regularly against an authoritative register.** **1** Keep an authoritative register of accounts, keys and certificates for OT and remote access. **2** Reconcile live identities against the register monthly and remove anything unregistered. **3** Alert on creation of accounts, keys or tokens outside a change.	STRIDE S, E CAPEC CAPEC-560 CWE – ATT&CK ICS T0859 CIE 8, 6
BKS-PP-3	**Traffic from inside your own country** Command traffic arrives through compromised home and small-office routers in the defender's own country. Geographic blocking and IP reputation filters let it through as local traffic. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**Access decisions rest on strong authentication of the user and device, not on where traffic appears to come from.** **1** Do not rely on country blocking or IP allow-lists as the control for remote access. **2** Require phishing-resistant MFA and device certificates for every remote connection. **3** Watch for logins from residential address ranges to administrative interfaces.	STRIDE S CAPEC – CWE CWE-290 ATT&CK ICS T0884 CIE 3, 6
BKS-PP-2	**Forgotten remote tools** Remote desktop and support tools installed by vendors years ago remain on HMIs and servers, still able to connect out. The adversary reuses them as ready-made, trusted persistence.	**Only approved remote access paths exist, and every installed tool is known and justified.** **1** Inventory remote access software on all OT hosts and remove what is not approved. **2** Block outbound connections from OT hosts except to named, approved destinations. **3** Check for new remote access software after every vendor visit.	STRIDE S, E CAPEC CAPEC-555 CWE CWE-1188 ATT&CK ICS T0822, T0886 CIE 8, 4

SC · SERVICE CHAIN

THE CAMPAIGN · BKS-SC-A TO BKS-SC-2 · https://ostering.com/taxonomies/critical-infrastructure/service-chain/

The companies that touch the estate, and the trust the estate gives them, as the way in.

BKS-SC-A The maintenance provider as master key †
BKS-SC-K Trusted updates carry the payload
BKS-SC-Q Provider tools reach every customer
BKS-SC-J Help desk resets hand over keys
BKS-SC-10 One password for every customer
BKS-SC-9 The integrator holds the only copy
BKS-SC-8 Contractor laptops cross the boundary
BKS-SC-7 Spares arrive compromised
BKS-SC-6 Ownership and jurisdiction change
BKS-SC-5 The vendor stops serving you
BKS-SC-4 Fourth parties nobody sees
BKS-SC-3 A call from the vendor
BKS-SC-2 Monitoring that cannot act

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-SC-A	**The maintenance provider as master key †** One service provider holds remote access to the sites of many operators, across companies and countries. Compromising the provider gives the adversary simultaneous access to all of them, and each customer sees only its own part. *Case: Supermarket refrigeration attacks, 2026; Kaseya VSA and Coop Sweden, 2021.*	**No single provider can act on many operators' sites at once without independent checks by each operator.** **1** Require providers to use separate credentials and access paths per customer, with no shared accounts. **2** Give each operator its own approval or veto on provider sessions and on commands that change the process. **3** Include provider compromise in the risk register and in exercises, with a plan to cut provider access quickly.	STRIDE S, E CAPEC CAPEC-555 CWE CWE-653 ATT&CK ICS T0822, T0886, T0859 CIE 9, 7
BKS-SC-K	**Trusted updates carry the payload** The vendor's own update channel is compromised, and signed, malicious updates are pushed to management software or field devices at every customer. Integrity checks pass because the vendor signed it. *Case: SolarWinds Orion, 2020.*	**Updates are staged and verified by the operator before they reach critical functions, even when signed.** **1** Stage vendor updates on a test system and release to production in waves, never to all sites at once. **2** Ask vendors for build provenance and protected signing keys, and verify signatures yourself. **3** Keep the ability to roll back each update and run the previous version.	STRIDE T, E CAPEC CAPEC-186, CAPEC-669 CWE CWE-494, CWE-829 ATT&CK ICS T0862 CIE 9, 10
BKS-SC-Q	**Provider tools reach every customer** Remote management tools used by managed service providers can run scripts on every customer endpoint at once, with the highest privilege and no customer approval. One compromise reaches every customer in a single push. *Case: Kaseya VSA and Coop Sweden, 2021.*	**Mass-action capability in provider tools is limited, approved and visible to the customer.** **1** Require customer-side approval for scripts and deployments from provider tools. **2** Exclude OT hosts from IT managed-service tooling, or put them on a separate, tightly scoped instance. **3** Limit provider tool agents to least privilege and log every action they take.	STRIDE E, T CAPEC CAPEC-122 CWE CWE-250, CWE-1220 ATT&CK ICS T0862, T0867 CIE 9, 4
BKS-SC-J	**Help desk resets hand over keys** An outsourced help desk resets the password or MFA of a privileged account for a convincing caller. The adversary walks in with valid credentials, and the help desk did what its process allowed. *Case: Marks & Spencer and Co-op, 2025.*	**Recovery of privileged credentials requires verification that a caller cannot provide by talking.** **1** Require in-person or strong out-of-band verification for privileged account resets. **2** Never reset MFA for privileged OT accounts by phone or chat alone. **3** Alert the account owner and security team on every privileged reset.	STRIDE S CAPEC CAPEC-413, CAPEC-415 CWE CWE-640 ATT&CK ICS T0859 CIE 12, 9
BKS-SC-10	**One password for every customer** Vendor technicians use the same default or service password at all customer sites. One leak, one ex-employee or one breach at the vendor opens every site.	**Each customer site has unique credentials for vendor access.** **1** Require unique, generated credentials per site for vendor and service accounts. **2** Change vendor default passwords at commissioning and verify it in acceptance tests. **3** Revoke vendor credentials when the contract or the technician changes.	STRIDE S CAPEC CAPEC-70 CWE CWE-798, CWE-1392 ATT&CK ICS T1694 CIE 9, 3

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-SC-9	**The integrator holds the only copy** The integrator keeps project files, passwords and drawings for many clients on its own network. A breach there yields credentials and engineering data for dozens of operators, and its loss leaves operators unable to rebuild.	**The operator owns and holds current engineering data, and suppliers protect what they keep to the operator's standard.** 1 Contract for delivery of all project files, passwords and drawings to the operator after every change. 2 Audit how integrators store client engineering data and credentials. 3 Keep an offline copy of current project files and configurations you control.	STRIDE I, D CAPEC CAPEC-150 CWE CWE-522, CWE-256 ATT&CK ICS T0811 CIE 11, 9, 10
BKS-SC-8	**Contractor laptops cross the boundary** Integrator laptops and USB drives are plugged straight into control networks, carrying whatever they picked up at other clients. The boundary controls are bypassed by design. *Case: Stuxnet, 2010.*	**Transient devices are checked and controlled before they touch OT.** 1 Provide operator-owned, maintained laptops for work on OT, or scan contractor devices at a kiosk before connection. 2 Disable unused USB ports and control removable media on OT hosts. 3 Log every transient device connection.	STRIDE T, E CAPEC CAPEC-457 CWE – ATT&CK ICS T0864, T0847 CIE 5, 9
BKS-SC-7	**Spares arrive compromised** During shortages or a crisis, spares come from grey markets or unverified suppliers to meet lead times. Counterfeit or tampered devices enter the estate when checks are most likely to be skipped.	**Spares are sourced and verified through the same controls in a crisis as in normal times.** 1 Hold strategic spares for critical functions so a crisis does not force unverified sourcing. 2 Buy only from authorised channels and verify device authenticity and firmware on receipt. 3 Pre-qualify alternative suppliers before they are needed.	STRIDE T CAPEC CAPEC-535, CAPEC-530 CWE CWE-1357 ATT&CK ICS T0862 CIE 9, 10
BKS-SC-6	**Ownership and jurisdiction change** A vendor or its parent is bought by, or becomes subject to, an entity in a hostile jurisdiction, or laws there oblige it to assist intelligence services. Remote access, update keys and support move with it.	**Vendor ownership and jurisdiction are reviewed as security controls throughout the contract.** 1 Require notification of changes of control, and a right to terminate or isolate on them. 2 Assess where vendor support, development and signing keys sit, and which laws apply to them. 3 Be able to run critical functions without the vendor's remote access.	STRIDE E, I CAPEC – CWE CWE-1357 ATT&CK ICS – CIE 9, 10
BKS-SC-5	**The vendor stops serving you** Sanctions, conflict or insolvency cut off updates, licences or the vendor cloud. Devices that depend on the cloud stop working or can no longer be patched, at the moment conflict makes them a target.	**Critical functions keep working, and can be maintained, if the vendor disappears.** 1 Design devices and software to keep operating without vendor cloud or licence servers. 2 Put source, keys and documentation in escrow for critical systems. 3 Plan and test operation through a period without vendor support.	STRIDE D CAPEC – CWE CWE-1104, CWE-1329 ATT&CK ICS – CIE 10, 9

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-SC-4	**Fourth parties nobody sees** The vendor's cloud and support depend on subcontracted developers, offshore support and other providers. The operator's contract and assessment stop at the vendor, but those fourth parties can reach the operator's systems.	**The operator knows every party that can reach its systems, however far down the chain.** **1** Require vendors to disclose subcontractors and hosting providers with access to customer systems or data. **2** Set access requirements that flow down to subcontractors in the contract. **3** Review fourth-party access during supplier assessments and after vendor incidents.	STRIDE E, I CAPEC – CWE CWE-1357 ATT&CK ICS T0862 CIE 9, 7
BKS-SC-3	**A call from the vendor** Someone posing as the vendor's support desk asks the operator to open a remote session for an urgent fix. The operator grants access because the request matches what the vendor really does.	**Vendor sessions are requested and verified through an agreed channel that a caller cannot impersonate.** **1** Agree a verification channel with each vendor for session requests, and never act on inbound calls alone. **2** Require a ticket in the vendor's own portal before granting a session. **3** Train operators to expect this approach and reward reports of it.	STRIDE S CAPEC CAPEC-413, CAPEC-415 CWE – ATT&CK ICS T0822 CIE 12
BKS-SC-2	**Monitoring that cannot act** Security monitoring is outsourced to a provider that watches IT, has no view of OT and no authority to isolate anything at night. Alerts are seen, but nobody can act until morning.	**Whoever monitors has the visibility and the authority to act on OT, or a direct line to someone who does, at any hour.** **1** Include OT telemetry in monitoring scope and define what the provider may isolate without asking. **2** Agree a 24-hour escalation path to an operator engineer with authority over the process. **3** Test the escalation path out of hours.	STRIDE R, D CAPEC – CWE CWE-778 ATT&CK ICS – CIE 6, 12

PE · PROCESS EFFECTS

THE CAMPAIGN · BKS-PE-A TO BKS-PE-2 · https://ostering.com/taxonomies/critical-infrastructure/process-effects/

What is done to the physical process, its safety functions and the operators' view of it.

BKS-PE-A Safety system answers to the network †
BKS-PE-K Protection disabled before the strike †
BKS-PE-Q Setpoints accept any value †
BKS-PE-J Operators see a false picture †
BKS-PE-10 Built-in functions turned into weapons †
BKS-PE-9 Commands in an unsafe sequence †
BKS-PE-8 Operators locked out of control †
BKS-PE-7 Alarms silenced before the damage †
BKS-PE-6 Product leaves out of specification †
BKS-PE-5 Controller logic quietly rewritten
BKS-PE-4 Wear inflicted below alarm thresholds
BKS-PE-3 Equipment cycled until it fails
BKS-PE-2 Control traffic flooded or blocked

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PE-A	**Safety system answers to the network †** The safety instrumented system can be reprogrammed, bypassed or put into maintenance from the control network. An adversary removes the last automatic protection first, then drives the process into a fire, explosion or toxic release that the plant was designed never to reach. *Case: TRITON safety system attack, 2017.*	**The final layer of protection must act on its own, and nothing reachable over a network may switch it off.** **1** Keep a hardwired trip path that operates on process limits even if every programmable component is compromised. **2** Require a physical key switch at the safety controller to enter program or bypass mode, and alarm when it changes. **3** Run safety systems on their own network with no route from business IT or remote access. **4** Compare running safety logic with a signed baseline every shift, and treat a mismatch as a plant trip condition.	`STRIDE` T, E `CAPEC` CAPEC-441 `CWE` CWE-653, CWE-306 `ATT&CK ICS` T0880, T0837, T0858 `CIE` 2, 1
BKS-PE-K	**Protection disabled before the strike †** Protection relays, interlocks and trips can have their settings changed or be knocked offline remotely. With protection quietly gone, the next fault or commanded switching destroys transformers, turbines or pumps instead of tripping safely, turning a short outage into months of repair. *Case: Kyiv substation attack, 2016.*	**Protection settings must be as hard to change as the equipment they protect is hard to replace.** **1** Lock protection settings at the device, changeable only through a local port with a physical enable. **2** Report every protection setting change and relay loss of communication to an independent alarm path. **3** Back up critical protection with an independent, non-networked device for equipment with long replacement times.	`STRIDE` T, D `CAPEC` CAPEC-176 `CWE` CWE-15, CWE-306 `ATT&CK ICS` T0837, T0836, T0814 `CIE` 2, 1
BKS-PE-Q	**Setpoints accept any value †** Controllers accept whatever setpoint, dose or limit the network sends. An adversary commands values no engineer would choose: chemical overdosing of drinking water, overpressure in gas mains, or heat in a cold store. The process obeys because nothing checks the value against physics.	**Every setpoint must be bounded by engineering limits enforced in the controller and backed by physical limits.** **1** Enforce engineering limits in controller logic, not only in the HMI, and reject out-of-range values whatever their source. **2** Size physical equipment so it cannot reach dangerous values: dosing pump capacity, relief valves, high-temperature cut-outs. **3** Require a second authorised person, on site, to widen any safety-relevant limit.	`STRIDE` T `CAPEC` CAPEC-153 `CWE` CWE-1284, CWE-15 `ATT&CK ICS` T0836, T0831 `CIE` 2, 1
BKS-PE-J	**Operators see a false picture †** The HMI shows whatever the controllers report, from a single path. An adversary who replays normal values or alters readings in transit runs the process into damage while operators see a healthy plant and take no action until physical evidence appears. *Case: Stuxnet, 2010.*	**Operators must be able to confirm the state of the process from a source the adversary does not also control.** **1** Bring independent measurements over a separate path and alarm when they disagree with the HMI values. **2** Authenticate telemetry from field device to HMI so values cannot be injected or replayed in transit. **3** Train operators to check local gauges and physical signs when the process behaves unlike its readings.	`STRIDE` S, T `CAPEC` CAPEC-148 `CWE` CWE-1293, CWE-924 `ATT&CK ICS` T0832, T0835, T1692.002 `CIE` 5, 2

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PE-10	**Built-in functions turned into weapons †** Maintenance functions such as defrost, flush, purge, test and firmware update can be started remotely with no limit on duration, frequency or the number of sites at once. A feature meant to protect the equipment becomes the attack: a defrost cycle held on turns every freezer into an oven. *Case: Supermarket refrigeration attacks, 2026.*	**Every built-in function must be bounded by the controller so its worst use cannot harm the process.** **1** Bound each maintenance function in the controller: maximum duration, minimum interval and the conditions under which it may run. **2** Disable remote start of functions that have no remote use, leaving them available only at the local panel. **3** Alarm centrally when a function runs outside its schedule, and stop it automatically when it passes its limit.	STRIDE T, E CAPEC CAPEC-74 CWE CWE-749, CWE-799 ATT&CK ICS T1692.001, T0831, T0858 CIE 4, 2
BKS-PE-9	**Commands in an unsafe sequence †** Interlocks check each command on its own but not the order in which commands arrive. An adversary who knows the process issues individually valid commands in a sequence the plant cannot survive, such as valves and pumps operated to cause water hammer or breakers switched out of order.	**The control system must enforce the safe order of operations, not only the safety of single actions.** **1** Encode permitted operating sequences as interlocks in the controller, and block commands that arrive out of order. **2** Rate-limit commands to large plant items so changes cannot happen faster than the process tolerates. **3** Review sequence interlocks in hazard studies, treating a hostile operator as an initiating cause.	STRIDE T CAPEC CAPEC-74 CWE CWE-841, CWE-696 ATT&CK ICS T0821, T0806, T0831 CIE 2, 1
BKS-PE-8	**Operators locked out of control †** Controllers can have credentials changed, operating modes switched or communications blocked so that legitimate commands are ignored. Operators can see the process going wrong but cannot stop it from the control room, and the plant runs on whatever the adversary last set. *Case: Ukraine grid attack, 2015.*	**Operators must always have a path to bring the process to a safe state that does not depend on the systems under attack.** **1** Provide local, hardwired stop and isolate controls at each site that work without the control network. **2** Alarm on any credential, mode or firmware change at a controller, and require local confirmation for each. **3** Exercise the loss-of-control procedure, including who travels to which site and how long it takes.	STRIDE D, E CAPEC CAPEC-115 CWE CWE-306, CWE-671 ATT&CK ICS T0813, T0827, T0892 CIE 10, 2
BKS-PE-7	**Alarms silenced before the damage †** Alarm thresholds, priorities and notifications can be changed or suppressed by the same accounts that change the process. An adversary raises thresholds or blocks alarm messages first, so the harmful change happens without anyone being told.	**Alarm configuration must be protected and monitored separately from the process it watches.** **1** Keep critical alarm limits in protected configuration that only a separate role can change, with every change logged off-system. **2** Send critical alarms over a second, independent path such as hardwired annunciators or a separate notifier. **3** Alert when alarm rates drop unexpectedly or alarm points stop reporting, not only when they fire.	STRIDE T, R CAPEC – CWE CWE-1320, CWE-223 ATT&CK ICS T0878, T0838, T1691.002 CIE 5, 6

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PE-6	**Product leaves out of specification †** Quality is checked by the same automation that makes the product, so tampering can let unsafe water, food or fuel leave the plant while records show it in specification. The harm appears downstream as illness, recalls or damaged engines, long after the change was made.	**Release decisions for anything people consume must rest on a check the production system cannot falsify.** **1** Verify critical quality parameters with independent analysers or laboratory samples outside the control system. **2** Record quality data to write-once storage at the point of measurement so later edits are detectable. **3** Hold a manual release step for safety-critical product when automated quality checks and independent samples disagree.	STRIDE T, R CAPEC – CWE CWE-1293 ATT&CK ICS T0836, T0832 CIE 1, 5
BKS-PE-5	**Controller logic quietly rewritten** Controllers accept new or modified logic from any engineering station that can reach them, without checking who signed it. An adversary changes the program itself, so the harmful behaviour persists through restarts and survives operators correcting setpoints by hand. *Case: Stuxnet, 2010.*	**Only signed, approved logic may run in a controller, and any change to it must be detected.** **1** Require signed logic and firmware, and reject downloads that are not signed by the asset owner's engineering key. **2** Use the controller's physical run/program key and keep it in run mode except during approved work. **3** Compare running logic with the approved version on a schedule and after every outage.	STRIDE T CAPEC CAPEC-441 CWE CWE-494, CWE-347 ATT&CK ICS T0889, T0843, T0873 CIE 2, 11
BKS-PE-4	**Wear inflicted below alarm thresholds** Equipment can be run just outside its design for weeks, with speed, temperature or cycling kept below alarm limits. Bearings, membranes and motors wear out early, failures look like age or poor maintenance, and nobody looks for an adversary. *Case: Stuxnet, 2010.*	**Operating envelopes must be monitored over time, not only against instant limits.** **1** Track cumulative stress such as hours outside nominal range, start counts and vibration trends, and alarm on drift. **2** Include deliberate tampering as a cause in failure investigations of critical rotating and process equipment. **3** Keep design operating envelopes in the controller so sustained marginal operation is reported.	STRIDE T CAPEC – CWE – ATT&CK ICS T0831, T0879 CIE 1, 6
BKS-PE-3	**Equipment cycled until it fails** Outputs to pumps, compressors, breakers and valves can be switched on and off as fast as commands arrive. Rapid cycling overheats motors, stresses mechanical parts and trips upstream supplies, causing damage that local protection was never designed to prevent.	**The controller must limit how often any large item of plant can change state.** **1** Enforce minimum on and off times and maximum starts per hour in the controller for each large motor and breaker. **2** Alarm when command rates to any output exceed normal operating patterns. **3** Fit hardware anti-cycle timers on equipment whose replacement time is long.	STRIDE T, D CAPEC CAPEC-125 CWE CWE-799 ATT&CK ICS T0806, T0831 CIE 2

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-PE-2	**Control traffic flooded or blocked** Control networks are sized for normal traffic and have no priority for commands and telemetry. Flooding or blocking messages delays or drops them, so the process holds its last state or falls back to defaults no one has reviewed.	**Loss of communication must leave the process in a state that was chosen and reviewed, not one that happens.** 1 Define and test a safe default state for every controller on loss of communication with supervision. 2 Separate control traffic from other traffic and give commands and safety messages priority. 3 Alarm on rising latency and message loss on control links, not only on total failure.	STRIDE D CAPEC CAPEC-125 CWE CWE-770, CWE-636 ATT&CK ICS T0814, T1691, T0815 CIE 5, 10

ST · SCALE AND TIMING

THE CAMPAIGN · BKS-ST-A TO BKS-ST-2 · https://ostering.com/taxonomies/critical-infrastructure/scale-and-timing/

Many sites at once, at a moment the adversary chooses, and the small strikes that test the mechanism first.

BKS-ST-A Several sectors hit at once †
BKS-ST-K Timed for the worst moment †
BKS-ST-Q One technique fits every site †
BKS-ST-J A rehearsal that tests the mechanism
BKS-ST-10 Cyber attack paired with physical sabotage †
BKS-ST-9 Struck when nobody is on site †
BKS-ST-8 Waves that exhaust responders
BKS-ST-7 Logic set to fire unattended †
BKS-ST-6 Operators that span borders
BKS-ST-5 Small sites attacked in bulk †
BKS-ST-4 Effect long after the cause
BKS-ST-3 Timed to a political decision
BKS-ST-2 A decoy draws the responders away

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-ST-A	**Several sectors hit at once †** Plans assume one sector fails while the others support it. An adversary who strikes power, water, telecoms and food distribution together removes the help each relies on: generators without fuel deliveries, pumps without power, responders without phones.	**Resilience plans must be tested against the simultaneous loss of the other sectors they depend on.** **1** Exercise incident plans with power, telecoms and fuel supply lost together, not one at a time. **2** Agree priorities and contact routes with other sectors' operators in advance, through channels that work without the public network. **3** Hold enough local stock of fuel, chemicals and spares to operate for the time a combined outage would take to clear.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 7, 10
BKS-ST-K	**Timed for the worst moment †** Attacks can be held until conditions make loss most harmful: deep winter, a heatwave, peak demand, a holiday or the start of a military crisis. A loss that would be an inconvenience in spring becomes a risk to life, and response capacity is already stretched. *Case: FrostyGoop, Lviv, 2024; Ukraine grid attack, 2015.*	**Design and recovery targets must be set for the worst season and moment, not the average one.** **1** Set recovery time objectives for the worst conditions, such as hours to restore heat in sub-zero weather. **2** Raise monitoring and staffing levels during known high-risk periods and periods of political tension. **3** Keep manual and local fallback capacity sized for peak demand, not average load.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826, T0813 CIE 1, 10
BKS-ST-Q	**One technique fits every site †** Hundreds of sites run the same controller model, firmware, configuration and default accounts. One technique that works at one site works at all of them, so the adversary can turn a single finding into a national event in a single night. *Case: Supermarket refrigeration attacks, 2026; Viasat KA-SAT modems, 2022; Danish energy sector, 2023.*	**No single weakness should be able to affect more sites than the operator can recover at once.** **1** Vary credentials, keys and network paths per site so access to one site does not grant access to the rest. **2** Know which sites share each model and firmware, and size response plans for all of them failing together. **3** Introduce diversity in controllers or protection for the most critical sites, so one flaw cannot reach every site.	STRIDE E, D CAPEC – CWE CWE-1392 ATT&CK ICS T1694.001, T0883 CIE 7, 4
BKS-ST-J	**A rehearsal that tests the mechanism** A limited strike, on one sector or one night, tests that access, controls and timing work at scale and measures how fast operators and governments respond. It also sends a message about what could follow. Treated as a one-off incident, it gives the adversary its rehearsal for free. *Case: Supermarket refrigeration attacks, 2026; Bremanger dam, Norway, 2025.*	**A limited attack must be treated as evidence of a wider capability and trigger checks across the whole estate.** **1** After any incident affecting several sites, review every site that shares its platforms, vendors or design, not just those affected. **2** Share technical indicators quickly with sector peers and national authorities, across borders where operators span countries. **3** Assume the adversary learned the response timeline, and change procedures, contacts and fallback plans afterwards.	STRIDE I, D CAPEC – CWE – ATT&CK ICS T0888, T0826 CIE 6, 7, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-ST-10	**Cyber attack paired with physical sabotage †** A cyber attack can be coordinated with cut cables, drones over sites, arson or staged threats, so responders face both at once. Plans that assume an attack is either digital or physical send people to the wrong place and leave the other side undefended.	**Incident plans must cover combined cyber and physical attacks, with one picture of both.** 1 Bring physical security alarms and OT security monitoring into the same incident picture. 2 Exercise scenarios where site access is unsafe at the moment a cyber response needs someone on site. 3 Protect the routes that a cyber recovery depends on, such as fibre ducts, radio masts and depots.	STRIDE D CAPEC CAPEC-547 CWE – ATT&CK ICS T0826 CIE 10, 7
BKS-ST-9	**Struck when nobody is on site †** Attacks can be timed for nights, weekends and holidays, when sites are unstaffed, monitoring is thin and decisions wait for someone senior. Effects that would be stopped in minutes during the day run for hours before anyone acts. *Case: Supermarket refrigeration attacks, 2026.*	**Protection and response must work as well at 03:00 on a Sunday as at noon on a weekday.** 1 Put automatic limits in controllers that stop harmful conditions without waiting for a person to respond. 2 Staff or contract out-of-hours monitoring with authority to isolate sites without escalation. 3 Alarm on remote commands and configuration changes outside working hours by default.	STRIDE D CAPEC – CWE – ATT&CK ICS T0831, T0836 CIE 2, 6
BKS-ST-8	**Waves that exhaust responders** An adversary can strike in waves over days or weeks, each before the last is cleared. Engineers, vendor field staff, spare parts and decision makers run out, and fixes are rushed and incomplete, which leaves openings for the next wave. *Case: DDoS on US banks, 2011 to 2013.*	**Response capacity must be planned for a campaign lasting weeks, not one incident.** 1 Plan staffing rotations and mutual aid for an incident lasting weeks, with named people in each shift. 2 Keep pre-agreed surge capacity with vendors and integrators, with priority set by consequence, not contract value. 3 Track remediation completeness, so rushed fixes are rechecked before the next wave.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826, T0828 CIE 10, 12
BKS-ST-7	**Logic set to fire unattended †** Schedules, automation rules and timers can be planted in management platforms and building or site controllers, to act at a set time or condition without the adversary connected. The effect happens even if access is cut when a conflict starts, so network isolation after the fact does not stop it.	**The estate must be checked for planted logic before a crisis, not after its effect.** 1 Compare controller logic and platform schedules with approved baselines regularly, and investigate any unexplained timer or condition. 2 Review scheduled jobs and automation rules on management platforms as part of change control. 3 Prefer simple controller logic that engineers can review in full.	STRIDE T CAPEC CAPEC-441 CWE CWE-511, CWE-506 ATT&CK ICS T0821, T0889 CIE 4, 6

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-ST-6	**Operators that span borders** Multinational chains, grid interconnections and shared platforms run sites in several countries from one place. One action hits several states at once, while incident response is split between national authorities, regulators and legal regimes that do not share information quickly.	**Cross-border operations need incident response arrangements that work across the borders they span.** **1** Agree in advance which national authorities are informed of an incident affecting several countries, and how quickly. **2** Segment platforms by country so one compromise cannot act on every country at once. **3** Exercise cross-border incidents with the operating companies and authorities involved.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 7, 10
BKS-ST-5	**Small sites attacked in bulk †** Thousands of small water systems, pump stations, farms and shops have internet-exposed controllers, default passwords and no security staff. Each looks too small to matter, but attacked together they cause a widespread loss of service and a loss of public confidence. *Case: Unitronics PLCs at water utilities, 2023; Texas water systems, 2024; Bremanger dam, Norway, 2025.*	**Security for small sites must come from the design and the vendor, not from staff the site does not have.** **1** Ship devices that refuse to run with default credentials and are not reachable from the internet by default. **2** Offer small operators a managed, monitored remote access service instead of direct exposure. **3** Give regulators and sector bodies a way to find and notify exposed small sites.	STRIDE E, D CAPEC – CWE CWE-1393, CWE-1188 ATT&CK ICS T0883, T1694.001 CIE 4, 9
BKS-ST-4	**Effect long after the cause** The harmful change can be made weeks before its effect, through slow drift or a timed change. Investigators look in the wrong window, logs have rolled over, and the cause is never found, so the same access is used again.	**Records of changes must last longer than the time an adversary might wait.** **1** Retain configuration and command history for at least a year, off the systems it describes. **2** Investigate incidents against the full change history of affected devices, not just the hours before. **3** Keep periodic configuration snapshots so the date of a change can be found.	STRIDE R CAPEC CAPEC-268 CWE CWE-778 ATT&CK ICS T0872 CIE 6, 11
BKS-ST-3	**Timed to a political decision** Strikes follow a vote, a sanctions package, an arms delivery or a summit, so cause and message are linked in the public mind. Operators that do not follow the political calendar meet those days at normal readiness, with remote access open and the duty team at its thinnest.	**Readiness should rise with political risk, not only with technical warnings.** **1** Link government advisories and threat intelligence to defined readiness levels with set actions. **2** Raise posture around known trigger dates: more monitoring, remote access restricted, staff on call. **3** Agree in advance with the authorities how heightened alerts reach the operator and what they ask for.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 6, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-ST-2	**A decoy draws the responders away** A loud incident on one site, one sector or the corporate IT network takes up the responders, the vendor's support and management's attention. Meanwhile the real effect is prepared quietly elsewhere, against a team with nobody left to look.	**Incident response must keep capacity in reserve and treat a loud incident as a possible diversion.** 1 Keep a reserve team, or a duty to hunt elsewhere, that is never assigned to the visible incident. 2 During any major incident, check OT and other sites for quiet changes at the same time. 3 Agree with vendors and retained responders how support is prioritised when several incidents run at once.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 6, 12

RD · RECOVERY DENIAL

THE CAMPAIGN · BKS-RD-A TO BKS-RD-2 · https://ostering.com/taxonomies/critical-infrastructure/recovery-denial/

Making the outage last: what stops the operator restoring service, and what makes restored service untrustworthy.

BKS-RD-A Long-lead equipment destroyed †
BKS-RD-K Black start depends on the network †
BKS-RD-Q Reinstall needs the vendor's servers
BKS-RD-J Devices bricked with bad firmware
BKS-RD-10 Project files and workstations wiped
BKS-RD-9 Backups reachable from the attack
BKS-RD-8 Restores bring the adversary back
BKS-RD-7 Recovery cannot be verified
BKS-RD-6 Incident communications taken down
BKS-RD-5 Vendors overwhelmed at once
BKS-RD-4 Key people worn out or targeted
BKS-RD-3 Replacements arrive as weak as before
BKS-RD-2 Insurance and contracts fail in war

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RD-A	**Long-lead equipment destroyed †** Transformers, turbines, large pumps and compressors can be damaged by commands that drive them beyond their limits. Replacements take months to make and ship, so a few minutes of control turn into a regional outage measured in seasons.	**Equipment that cannot be replaced quickly must be protected by limits no command can override.** **1** Protect long-lead equipment with independent, non-networked protection that trips before damage occurs. **2** Hold strategic spares or share them through sector pools, sized for loss of several units together. **3** Identify every item with a replacement time over a month and record how it could be damaged digitally.	STRIDE D CAPEC CAPEC-547 CWE – ATT&CK ICS T0879, T0837 CIE 1, 10, 2
BKS-RD-K	**Black start depends on the network †** The systems needed to restart after total loss, such as black-start generators, their controls and their communications, share networks and accounts with the systems under attack. When the grid or plant goes down, the means of bringing it back is already compromised.	**Restart capability must be isolated and able to work without the systems it restores.** **1** Keep black-start plant and its controls on isolated networks with their own credentials and power. **2** Test black-start procedures with the normal control systems assumed unavailable. **3** Hold paper or offline copies of restart procedures, settings and contact lists at the sites that use them.	STRIDE D CAPEC – CWE CWE-653 ATT&CK ICS T0826, T0813 CIE 10, 7
BKS-RD-Q	**Reinstall needs the vendor's servers** Rebuilding HMIs, engineering tools and controllers needs software downloads, licence activation or a cloud account at the vendor. In a conflict those servers may be down, sanctioned, overwhelmed by every customer at once or attacked themselves, so recovery stalls at every site together.	**Every system needed to restore the critical functions must be rebuildable from material the operator holds, with no outside connection.** **1** Hold offline installers, licence files, firmware images and their hashes for every version in service. **2** Agree offline activation or licence escrow with each vendor in the contract. **3** Rehearse a full rebuild of a control system with the internet disconnected, and time it.	STRIDE D CAPEC – CWE CWE-1357 ATT&CK ICS T0826 CIE 10, 9
BKS-RD-J	**Devices bricked with bad firmware** Field devices, gateways and modems accept firmware remotely without signature checks or a protected recovery image. Overwritten with corrupt firmware, they stop working and must be replaced by hand, at every site, from spares that may not exist. *Case: Ukraine grid attack, 2015; Viasat KA-SAT modems, 2022.*	**Devices must refuse unsigned firmware and keep a recovery image an attacker cannot overwrite.** **1** Require signed firmware and reject updates that fail verification. **2** Keep a protected boot or recovery image that cannot be written remotely. **3** Hold spares of each critical device type, configured and ready, sized for loss at many sites.	STRIDE T, D CAPEC CAPEC-638 CWE CWE-494, CWE-1326 ATT&CK ICS T1693, T0800 CIE 2, 10

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RD-10	**Project files and workstations wiped** Engineering workstations hold the only current copies of controller programs, configurations and network settings. Wiped together with the HMIs and historians, they leave the operator unable to rebuild the plant as it was, and recovery means re-engineering from memory. *Case: Ukraine grid attack, 2015; NotPetya, 2017; Industroyer2 attempt, 2022.*	**The configuration of the plant must exist in protected copies that do not depend on the engineering workstations.** **1** Keep offline, versioned copies of every controller program and configuration, stored away from the control network. **2** Store engineering files in a managed repository with integrity checks, not on individual workstations. **3** Practise rebuilding an engineering workstation and reloading a controller from the offline copy.	STRIDE D, T CAPEC – CWE – ATT&CK ICS T0809 CIE 10, 11
BKS-RD-9	**Backups reachable from the attack** Backups sit on the same network and accounts as the systems they protect, or have never been restored. The adversary destroys or encrypts them first, and the operator discovers during the crisis that there is nothing to restore from. *Case: NotPetya, 2017.*	**At least one copy of every critical backup must be offline, immutable and proven by restore tests.** **1** Keep an offline or immutable copy of backups that the production accounts cannot delete or alter. **2** Test full restores on a schedule and record how long they take. **3** Separate backup administration credentials from the directory used to run the plant.	STRIDE D, T CAPEC – CWE CWE-530 ATT&CK ICS T0809 CIE 10
BKS-RD-8	**Restores bring the adversary back** Backups, golden images and project files may already contain the adversary's implant or altered logic. Restoring from them rebuilds the compromise, so the plant fails again soon after recovery and confidence in every later restore is lost.	**Anything restored must be checked against a known-good reference before it is trusted.** **1** Keep known-good hashes for firmware, images and logic, recorded at approval and stored offline. **2** Scan and compare restored systems before connecting them back to the control network. **3** Hold older restore points as well as recent ones, so a clean point predates any implant.	STRIDE T CAPEC CAPEC-441 CWE CWE-353 ATT&CK ICS T0873, T0889 CIE 10, 8
BKS-RD-7	**Recovery cannot be verified** Historians, logs and configuration records may have been altered, so there is no trusted record of what the plant looked like before. Operators cannot tell which settings and data are good, and restart is delayed while every value is checked by hand.	**There must be a trusted record of the plant's correct state that the adversary could not alter.** **1** Write key configuration and process records to write-once storage outside the control network. **2** Sign approved configurations so their integrity can be checked during recovery. **3** Define in advance which values must be checked by hand before restart, and who signs them off.	STRIDE T, R CAPEC CAPEC-268 CWE CWE-353, CWE-1293 ATT&CK ICS T0809, T0832 CIE 11, 10

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RD-6	**Incident communications taken down** Phone lines, email and chat used to coordinate response run on the same networks or providers as the systems under attack. Flooding call centres or compromising email cuts responders off from each other and from the public at the moment they need to talk. *Case: Ukraine grid attack, 2015.*	**Incident coordination must have channels that do not depend on the systems under attack.** 1 Provide out-of-band communications, such as radio, satellite phones or a separate messaging service, for incident teams. 2 Keep offline contact lists for staff, vendors, authorities and other sectors. 3 Prepare public messaging routes that work if the operator's own phone lines and website are unavailable.	STRIDE D CAPEC CAPEC-125 CWE – ATT&CK ICS – CIE 10, 7
BKS-RD-5	**Vendors overwhelmed at once** Many operators depend on the same vendor or integrator for recovery, and contracts assume one incident at a time. When every customer is hit together, the vendor's engineers, tools and spares are rationed, and recovery waits in a queue. *Case: Kaseya VSA and Coop Sweden, 2021; Supermarket refrigeration attacks, 2026.*	**Recovery must not depend on vendor capacity that every other customer will claim at the same moment.** 1 Build in-house capability to restore critical systems without the vendor on site. 2 Agree surge support and priority by consequence with vendors, and test it. 3 Hold the licences, tools and installation media needed to rebuild without the vendor's help.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 9, 10
BKS-RD-4	**Key people worn out or targeted** A few engineers know how the plant really works, and a long incident leaves them exhausted. They can also be targeted directly through intimidation, doxxing or attacks on their families. When they cannot continue, recovery stops.	**Knowledge needed for recovery must be shared across enough people to survive a long campaign.** 1 Document critical knowledge and train deputies for every role in the recovery plan. 2 Limit public information about the identities and roles of key OT staff. 3 Plan rest and rotation for incident staff from the first day.	STRIDE D, I CAPEC – CWE – ATT&CK ICS – CIE 12, 11
BKS-RD-3	**Replacements arrive as weak as before** Replacement devices and rebuilt systems come with default credentials, old firmware and factory settings. Restored in a hurry, the site is as exposed as it was before the attack, or more, and the adversary returns through the same route.	**Rebuilt systems must be hardened to the same standard as the original before they go back into service.** 1 Keep hardened build standards and configuration scripts ready to apply to replacements. 2 Update firmware on spares in storage, and record their versions. 3 Check credentials, remote access and firmware on every rebuilt site before reconnecting it.	STRIDE E CAPEC – CWE CWE-1188, CWE-1392 ATT&CK ICS T1694.001 CIE 10, 8
BKS-RD-2	**Insurance and contracts fail in war** Insurance, support contracts and service levels may exclude acts of war or state action, and attribution can take months. The operator finds that the money and support it planned for recovery are disputed, while repairs wait. *Case: NotPetya, 2017.*	**Recovery funding and support must be planned for an attack that may be classed as an act of war.** 1 Review insurance and supplier contracts for war, state-actor and force majeure exclusions. 2 Fund a recovery reserve, or agree public support arrangements, that do not depend on attribution. 3 Set out in contracts what vendors must do during a state-attributed incident.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 10

AD · AFTERMATH AND DENIABILITY

THE CAMPAIGN · BKS-AD-A TO BKS-AD-2 · https://ostering.com/taxonomies/critical-infrastructure/aftermath-and-deniability/

The cognitive and political layer: fronts, signals, false claims, disinformation and the loss of public trust.

BKS-AD-A False safety notices reach the public †
BKS-AD-K A limited strike is a warning
BKS-AD-Q Destruction disguised as ransomware
BKS-AD-J Response waits for attribution
BKS-AD-10 The public stops trusting the product
BKS-AD-9 Panic buying multiplies a small outage
BKS-AD-8 A hacktivist persona hides a state
BKS-AD-7 False claims force costly action
BKS-AD-6 Stolen engineering data is published
BKS-AD-5 Staff are named and targeted
BKS-AD-4 Planted evidence points elsewhere
BKS-AD-3 Disclosure teaches the adversary
BKS-AD-2 Taunts on public screens

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AD-A	**False safety notices reach the public †** The service has no authenticated way to tell the public what to do in an emergency, so a forged boil-water, evacuation or gas-leak notice spreads faster than the real one. People act on it and are harmed, and later genuine notices are not believed.	**Public safety instructions travel only through channels that the public has been taught to recognise and that can be verified.** **1** Agree in advance with the authorities which channels carry safety notices, and publish that list before any incident. **2** Protect official accounts, SMS sender IDs and alerting systems with phishing-resistant MFA and named owners. **3** Prepare holding statements and a rebuttal process that can go out within minutes of a forged notice appearing.	STRIDE S, T, D CAPEC CAPEC-148, CAPEC-151 CWE – ATT&CK ICS – CIE 10, 12
BKS-AD-K	**A limited strike is a warning** A small, contained attack is meant as a signal and a test of the mechanism. The organisation treats it as an isolated incident, restores service and closes the ticket, while the same path, at the same sites and their peers, stays open for a far larger strike later. *Case: Khuzestan steel plant, 2022.*	**Treat any effect an adversary has demonstrated once as a capability that can be repeated at full scale.** **1** After any physical effect, ask what the same mechanism would do across every site, vendor customer and peer operator at once. **2** Close the mechanism, not only the instance: remove the exposure fleet-wide and share indicators with the sector and national CERT. **3** Record demonstrated mechanisms in the threat model and test their removal in the next exercise.	STRIDE T, D CAPEC – CWE – ATT&CK ICS – CIE 1, 6, 10
BKS-AD-Q	**Destruction disguised as ransomware** A destructive attack is dressed up as criminal extortion. Responders follow the ransomware playbook, negotiate and wait for a decryptor that will never come, while the real aim, destruction and delay, is achieved and insurers may argue a war exclusion applies. *Case: NotPetya, 2017.*	**Plan recovery so that it never depends on the attacker's cooperation or on how the attack is labelled.** **1** Assume encrypted systems are destroyed: rebuild from offline, tested images rather than waiting for keys. **2** Escalate any attack on operational systems to national authorities early, whatever the ransom note says. **3** Check insurance cover for state-attributed and destructive attacks before an incident, not after.	STRIDE R, T, D CAPEC – CWE – ATT&CK ICS T0809, T0828 CIE 10, 6
BKS-AD-J	**Response waits for attribution** Plans tie escalation, mutual aid and national coordination to knowing who is behind an attack. Attribution takes weeks or months, so the organisation and its peers under-react while the attack is still unfolding and the same mechanism is reused elsewhere. *Case: Supermarket refrigeration attacks, 2026.*	**Decide escalation by effect and scope, not by who the attacker is believed to be.** **1** Write escalation triggers on observable effects: physical change, number of sites, sectors affected, public safety. **2** Pre-agree with peers and authorities what is shared and done when several operators are hit at once. **3** Keep attribution work separate from the response so neither waits for the other.	STRIDE D, R CAPEC – CWE – ATT&CK ICS – CIE 10, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AD-10	**The public stops trusting the product** After an attack on treatment, dosing or the cold chain, the operator cannot show that what reached people was safe, because quality records and process data could have been altered. Customers turn to riskier alternatives and confidence takes years to return.	**Keep evidence of product safety that an attacker on the control system cannot alter.** 1 Take independent quality samples and lab results through a path that does not touch the control network. 2 Write process and quality records to tamper-evident, write-once storage held off site. 3 Prepare a public explanation of how safety was verified, with figures, before it is needed.	STRIDE T, R CAPEC – CWE – ATT&CK ICS – CIE 2, 10
BKS-AD-9	**Panic buying multiplies a small outage** A disruption at a few sites, amplified on social media, sets off panic buying across a region. Replenishment, ordering and distribution are tuned for normal demand, so the shortage the attack only threatened becomes real. *Case: Colonial Pipeline, 2021.*	**Design supply and communications to absorb a demand surge triggered by fear, not only by real shortage.** 1 Hold surge stock and allocation rules for essentials, agreed with retailers and authorities in advance. 2 Publish factual stock and service updates early and often during an incident. 3 Model the demand spike that a visible outage at a few sites would cause, and plan for it.	STRIDE D CAPEC CAPEC-420 CWE – ATT&CK ICS T0828 CIE 7, 10
BKS-AD-8	**A hacktivist persona hides a state** Attacks are claimed by a self-styled volunteer group. Because the threat model rates hacktivists as low capability and opportunistic, the operator scopes the response narrowly and misses the resources, patience and intent behind it. *Case: Unitronics PLCs at water utilities, 2023; Texas water systems, 2024.*	**Judge a threat by what it did and could do, not by the name it chooses for itself.** 1 Assess every attack that changes a physical process as a capable adversary until evidence shows otherwise. 2 Track self-styled groups and their claims with the sector CERT, including links reported by government agencies. 3 Harden the exposure a persona used across the whole estate, not only the device it defaced.	STRIDE R, S CAPEC – CWE – ATT&CK ICS – CIE 12, 6
BKS-AD-7	**False claims force costly action** An adversary claims, without proof, to have tampered with water, food or fuel. The operator has no reliable way to show that nothing changed, so it shuts down, recalls or issues warnings it did not need to, and the claim works as well as an attack.	**Be able to show quickly and credibly that a process and its product were not changed.** 1 Keep a trusted baseline of logic, setpoints and firmware, and compare against it on demand. 2 Log every change to control logic and setpoints centrally, with who made it and when. 3 Agree with regulators in advance what evidence lets a claimed tampering be ruled out.	STRIDE R, D CAPEC CAPEC-417 CWE CWE-778 ATT&CK ICS – CIE 2, 8

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AD-6	**Stolen engineering data is published** Drawings, network diagrams, setpoints and passwords taken from the operator or its contractors are published to show reach and to help others attack. The operator cannot withdraw the information and must treat every design it described as known to everyone.	**Assume engineering information will leak, and design so that knowing it is not enough to cause harm.** 1 Classify engineering documents and limit who holds them, including contractors and bidders. 2 Rotate credentials and review exposures named in any leaked material immediately. 3 Rely on engineered limits and authentication rather than on the secrecy of drawings and settings.	STRIDE I CAPEC – CWE CWE-656 ATT&CK ICS T0882 CIE 11, 2
BKS-AD-5	**Staff are named and targeted** Operators, engineers and incident responders are identified online, doxxed, intimidated or approached to help. People under pressure make mistakes, leave, or are coerced, at the moment the organisation most needs them.	**Protect the people who run essential services as part of the system's security.** 1 Limit public exposure of names, roles and rotas of operational staff, including on professional networks. 2 Give staff a clear, confidential route to report approaches, threats or coercion. 3 Design critical actions so no single person can be pressured into causing harm alone.	STRIDE I, S CAPEC CAPEC-416 CWE – ATT&CK ICS – CIE 12, 11
BKS-AD-4	**Planted evidence points elsewhere** The attacker plants code, language and infrastructure traces that point to another actor. Investigators and decision makers who rely on a single source of evidence draw the wrong conclusion, and the response is aimed at the wrong party.	**Base conclusions on several independent lines of evidence that an attacker in one system cannot forge together.** 1 Keep network monitoring that is independent of the hosts it watches, with its own storage. 2 Preserve forensic images and logs with integrity protection before analysis starts. 3 Share raw evidence with the national CERT rather than conclusions alone.	STRIDE R, T CAPEC CAPEC-268, CAPEC-93 CWE – ATT&CK ICS – CIE 6, 8
BKS-AD-3	**Disclosure teaches the adversary** Detailed public statements and incident reports reveal which effects worked, how long recovery took and which controls failed. The adversary uses them to tune the next attack and to choose the next targets that share the same weaknesses.	**Share technical detail where it helps defenders, and keep what helps the attacker out of public reports.** 1 Share full technical detail through trusted sector channels and the national CERT. 2 Review public statements for detail that measures the attack's success, such as recovery times per site. 3 Fix shared weaknesses across peers before publishing them.	STRIDE I CAPEC – CWE – ATT&CK ICS – CIE 11, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AD-2	**Taunts on public screens** Fuel pumps, till screens, signs and HMIs that the public or staff can see are made to show the attacker's message. The defacement causes little damage but proves access, spreads fear and invites copycats. *Case: Iran fuel stations, 2021 and 2023; Unitronics PLCs at water utilities, 2023.*	**Treat any public-facing display linked to operational systems as part of the attack surface.** 1 Separate public displays from the systems that run the process, and restrict what can write to them. 2 Treat a defacement as proof of access and investigate what else the attacker could reach. 3 Prepare staff to switch displays off and explain the situation calmly.	STRIDE T CAPEC – CWE – ATT&CK ICS – CIE 3, 12

AS · AIR AND SPECTRUM

THE CAMPAIGN · BKS-AS-A TO BKS-AS-2 · https://ostering.com/taxonomies/critical-infrastructure/air-and-spectrum/

Drones and the electromagnetic spectrum as the adversary's tools: to watch, probe, deliver, jam, disrupt and close sites without touching the network.

BKS-AS-A Electromagnetic attack on protection and control †
BKS-AS-K Payloads delivered over the fence †
BKS-AS-Q Jammers carried over a region
BKS-AS-J Presence alone forces a shutdown
BKS-AS-10 Assets open to the sky †
BKS-AS-9 A radio left inside the fence
BKS-AS-8 Mapping the estate from above
BKS-AS-7 Probing the response from the air
BKS-AS-6 Listening from above the perimeter
BKS-AS-5 Countermeasures jam the defender too
BKS-AS-4 The site's own drones turned
BKS-AS-3 Nobody owns the sky overhead
BKS-AS-2 Sightings until nobody responds

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AS-A	**Electromagnetic attack on protection and control †** An adversary brings an intentional electromagnetic interference source close to a substation, pumping station or control building, by vehicle or drone. Protection relays, controllers and communications trip, freeze or fail together, with no network intrusion to detect, and the site loses control and protection at the same moment.	**Critical protection and control must keep working, or fail safe, under deliberate electromagnetic attack from the distances an adversary can reach.** **1** Assess critical sites for IEMI exposure, and test key protection and control equipment to IEC 61000-4-36 levels. **2** Shield and filter rooms and cabinets holding protection and control, following IEC TS 61000-5-10, with bonded entry points. **3** Prefer fibre for protection signalling, keep standoff from the perimeter, and make protection fail to a safe state.	STRIDE D, T CAPEC – CWE CWE-1384 ATT&CK ICS T0837, T0827, T0880 CIE 1, 2, 5 STANDARDS IEC 61000-4-36, IEC TS 61000-5-10
BKS-AS-K	**Payloads delivered over the fence †** A drone carries something over fences and gates designed against people on foot: an incendiary or explosive device, or equipment left beside transformers, aircraft or fuel. Perimeter security, patrols and access control are bypassed because they assume the threat arrives at ground level. *Case: Leipzig/Halle airport drone, 2026.*	**Sites must assume a threat can arrive from above and protect the assets whose loss is hardest to replace.** **1** Identify assets whose loss is catastrophic or slow to replace, and give them overhead protection or standoff. **2** Extend detection and patrol routines to objects that arrive from the air, including on roofs. **3** Plan isolation and safe shutdown for when a suspect object is found next to critical plant.	STRIDE D, T CAPEC CAPEC-390 CWE CWE-1263 ATT&CK ICS T0879 CIE 1, 5
BKS-AS-Q	**Jammers carried over a region** Jammers carried by drones or aircraft over a region drown out GNSS, cellular and private radio at many sites at once. Telemetry, alarms, timing and field crews' phones fail together, and the operator cannot tell which sites are affected, or why. *Case: GNSS interference, Baltic region.*	**Critical sites must keep timing, alarms and control when radio is denied across a whole region.** **1** Give critical links a wired or fibre path that does not depend on radio. **2** Hold local timing sources, such as holdover clocks, for when GNSS is lost. **3** Detect and report jamming, and plan how crews operate and communicate when radio fails.	STRIDE D CAPEC CAPEC-601, CAPEC-599 CWE – ATT&CK ICS T1695, T0815 CIE 7, 10
BKS-AS-J	**Presence alone forces a shutdown** Drones flown over an airport, power station or port trigger safety rules that stop operations until the airspace is clear. The adversary needs no payload and no intrusion: hours of closure, diverted traffic and public alarm come from presence alone, repeated night after night at low cost. *Case: Copenhagen and Oslo airport drones, 2025; Munich airport drones, 2025.*	**Operations must have a planned, graded response to drones that keeps essential functions running where it is safe to do so.** **1** Define graded responses by drone position, behaviour and site function, rather than a single full stop. **2** Agree in advance with aviation and police authorities who decides to stop and restart, and how fast. **3** Rehearse running essential functions under a drone alert, with protected staff positions.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826, T0828 CIE 10, 1

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AS-10	**Assets open to the sky †** Open reservoirs, treatment basins, outdoor switchyards, transformer bays, cooling towers and fuel farms are exposed from above. A drone can reach equipment or water that ground security protects well, so an attack bypasses the layers the design relies on.	**Design for exposure from above wherever interference with an asset would have severe consequences.** **1** List open-air assets with severe consequences, and assess their exposure from above. **2** Add cover, netting, standoff or monitoring where the consequence justifies it. **3** Increase water quality and equipment monitoring at open-air assets, and plan isolation if interference is suspected.	STRIDE T, D CAPEC CAPEC-390 CWE – ATT&CK ICS T0879 CIE 1, 5
BKS-AS-9	**A radio left inside the fence** A drone drops a small radio, cellular or Wi-Fi device on a roof or behind the fence, within reach of wireless controllers, sensors and site networks. The adversary gets a foothold inside the perimeter, with nobody passing the gate, and operates it from far away.	**Wireless networks inside the perimeter must not trust proximity, and unknown transmitters must be found.** **1** Authenticate every wireless device and link, so being within range gives no access. **2** Survey sites for unknown transmitters regularly and after every drone incursion. **3** Inspect roofs and inner areas after overflights, and treat any device found as a security incident.	STRIDE S, E CAPEC – CWE CWE-940 ATT&CK ICS T0860, T0848 CIE 3, 6
BKS-AS-8	**Mapping the estate from above** Drones film and photograph sites from above: equipment layout, cable routes, fuel and cooling, guard positions and gaps in fences. Thermal cameras show which units run and when. The adversary builds its target picture of what to hit, and where, without setting foot on site. *Case: Drones over Doel and Belgian airports, 2025.*	**Treat the view from above as public, and keep the most critical details out of it.** **1** Review what each critical site reveals from above, including heat, and screen or relocate what matters most. **2** Detect and log drone overflights, and share the patterns with peers and authorities. **3** Assume an overflown site has been mapped, and review its protection after each overflight.	STRIDE I CAPEC CAPEC-169 CWE – ATT&CK ICS – CIE 11, 6
BKS-AS-7	**Probing the response from the air** Repeated flights over civil and military sites test whether drones are detected, by which sensors and at what range, and who responds and how fast. Each response shows the adversary the blind spots and how long it has, ahead of a real strike. *Case: Munich airport drones, 2025; Drones over Doel and Belgian airports, 2025.*	**Drone response must give away as little as possible, and must change over time.** **1** Vary detection coverage, response times and procedures, and do not publicise them. **2** Record every incursion with sensor data and the response, and analyse them together for probing patterns. **3** Share incursion data with nearby operators and authorities so patterns across sites become visible.	STRIDE I CAPEC – CWE – ATT&CK ICS – CIE 6, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-AS-6	**Listening from above the perimeter** A drone hovering above or beside a site receives its Wi-Fi, telemetry radio and wireless sensor traffic far better than anyone at ground level. Unprotected links give away protocols, addresses, credentials and process values, which the adversary uses to plan control of the site.	**Wireless traffic must be protected as if anyone could receive it.** 1 Encrypt and authenticate every wireless link that carries control, telemetry or credentials. 2 Reduce transmit power and use directional antennas where links allow. 3 Rotate keys and credentials on a schedule, and at once after suspicious overflights.	STRIDE I CAPEC CAPEC-157 CWE CWE-319 ATT&CK ICS T0887 CIE 3, 2
BKS-AS-5	**Countermeasures jam the defender too** Jammers and spoofers brought in to stop drones also block the site's own wireless sensors, radio links, cellular alarms and GNSS timing. An adversary who triggers a drone alert can make the defenders degrade their own control, communications and protection.	**Counter-drone measures must be engineered together with the site, not added on top of it.** 1 Map which site systems use the bands counter-drone equipment affects, before it is deployed. 2 Agree with operators and authorities the rules for jamming or spoofing near critical sites. 3 Test essential systems with counter-drone equipment running, and keep a fallback for each one affected.	STRIDE D CAPEC – CWE – ATT&CK ICS T0815, T1695.003 CIE 7, 4
BKS-AS-4	**The site's own drones turned** Operators use drones and robots for inspection and patrol, controlled through vendor clouds and radio links. Hijacked or spoofed, they fly into plant, drop out when needed or return false inspection images, giving the adversary an aerial platform already trusted inside the perimeter.	**Inspection drones and robots are part of the control system and need the same protection.** 1 Authenticate and encrypt control links, and enforce flight limits and geofences on the aircraft itself. 2 Treat vendor cloud accounts for drones and robots as privileged, with MFA and monitoring. 3 Cross-check inspection findings with independent data before acting on them.	STRIDE S, T CAPEC – CWE CWE-940 ATT&CK ICS T0860 CIE 3, 9
BKS-AS-3	**Nobody owns the sky overhead** Operators have no authority to stop a drone, police and military take time to arrive, and responsibility between them is unclear. While they decide, the drone flies, and the adversary relies on that gap for every probe and strike.	**Who detects, decides and acts on drones at each critical site must be settled before the first incursion.** 1 Agree with police, military and aviation authorities who detects, who decides and who acts at each critical site. 2 Give operators the detection, reporting channels and training to support a fast decision. 3 Exercise the arrangement with all parties at least once a year.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 12, 10
BKS-AS-2	**Sightings until nobody responds** Frequent drone sightings, real or false, wear out responders and teach staff that alerts lead nowhere. Response slows, procedures are skipped, and the alert that matters is treated like all the others. *Case: Copenhagen and Oslo airport drones, 2025.*	**Drone alerts must stay credible: triaged, verified and closed with a finding.** 1 Verify sightings with sensors before raising site-wide alerts, and grade the response. 2 Close every alert with what was found, and feed the result back to staff. 3 Rotate and support responders during sustained periods of incursions.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 12, 6

FD · FIELD DEVICES AND CONTROLLERS

THE ESTATE · BKS-FD-A TO BKS-FD-2 · https://ostering.com/taxonomies/critical-infrastructure/field-devices-and-controllers/

The devices that touch the process: PLCs, RTUs, protection relays, refrigeration and building controllers, drives and sensors.

BKS-FD-A Control and safety share one box †
BKS-FD-K Protection relays can be switched off †
BKS-FD-Q Controllers obey any well-formed command †
BKS-FD-J Sensors report what they are told †
BKS-FD-10 Unsigned firmware is accepted
BKS-FD-9 Default credentials ship in the field
BKS-FD-8 A web panel runs the process †
BKS-FD-7 Logic can change while it runs †
BKS-FD-6 Devices cannot prove what they run
BKS-FD-5 Hidden test and debug modes
BKS-FD-4 The controller cannot be patched
BKS-FD-3 Maintenance ports at unattended sites
BKS-FD-2 Wireless links to field devices

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FD-A	**Control and safety share one box †** Control and safety functions run on the same controller, network or engineering tool, so whoever can change the control logic can also reach the safety system. One compromise removes both the process and its last automatic protection against explosion, release or fire. *Case: TRITON safety system attack, 2017.*	**The safety system must be independent of the control system in hardware, network and engineering access, so no single compromise reaches both.** **1** Run safety functions on separate controllers and networks, with no routable path from control or business networks. **2** Use a separate engineering workstation and credentials for safety programming, held offline when not in use. **3** Require a physical key for program mode, alarm whenever it leaves run, and back critical trips with hard-wired protection.	STRIDE T, E, D CAPEC – CWE CWE-653 ATT&CK ICS T0880, T0837, T0858 CIE 2, 4, 1
BKS-FD-K	**Protection relays can be switched off †** Protection relays and their settings can be changed, disabled or crashed remotely. An attacker can remove protection before switching, so faults are not cleared and equipment such as transformers is damaged, turning a short outage into a long one. *Case: Kyiv substation attack, 2016; Industroyer2 attempt, 2022.*	**Protection must keep working, and stay set correctly, whatever happens to the communications around it.** **1** Make protection settings read-only remotely, with changes only by an authorised person on site. **2** Test that relays keep protecting when their communication port is flooded or attacked. **3** Alarm on any change to protection settings or relay state, at a monitoring point independent of SCADA.	STRIDE T, D CAPEC – CWE CWE-306 ATT&CK ICS T0837, T0814, T0816 CIE 2, 1
BKS-FD-Q	**Controllers obey any well-formed command †** Field protocols such as Modbus, DNP3 and IEC 60870-5-104 are used without authentication, so a controller executes any correctly formatted command from anything that can reach it. Whoever gets onto the network can operate the plant. *Case: FrostyGoop, Lviv, 2024; Kyiv substation attack, 2016.*	**Only commands from an authenticated, authorised source, within a defined set, should change the process.** **1** Use the secure versions of field protocols where devices support them, such as DNP3 Secure Authentication. **2** Restrict which hosts may send write commands, using allow-lists at a protocol-aware firewall. **3** Alarm on write commands from any source other than the expected masters.	STRIDE S, T, E CAPEC CAPEC-151 CWE CWE-306 ATT&CK ICS T1692.001, T0831 CIE 3, 2
BKS-FD-J	**Sensors report what they are told †** Transmitters and sensors accept range, calibration and configuration changes over the network, or can be fed false signals at the cable. Control and safety logic then act on a measurement the adversary chose, and every system above them agrees the plant is fine.	**The measurements that control and safety act on must be protected from change and checked against an independent source.** **1** Write-protect sensor configuration and calibration, with a local switch or key for changes. **2** Give critical variables a second, independent measurement and alarm when the two disagree. **3** Check readings against what the physics allows, and treat impossible values as an attack until proved otherwise.	STRIDE T, S CAPEC – CWE CWE-1314 ATT&CK ICS T0836, T0832 CIE 2, 5

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FD-10	**Unsigned firmware is accepted** Devices accept firmware without checking a signature, or let the update mode be entered remotely. An attacker can load malicious firmware or overwrite it with garbage, leaving devices that run the attacker's code or never work again. *Case: Ukraine grid attack, 2015.*	**A device should run only firmware its maker signed, and only enter update mode with a person's approval.** **1** Buy devices that verify firmware signatures from a hardware root of trust, and make this a procurement requirement. **2** Block remote entry to firmware update mode, or alarm on it, and require local approval. **3** Prevent rollback to older, vulnerable firmware versions.	STRIDE T, D CAPEC CAPEC-638, CAPEC-186 CWE CWE-494, CWE-347 ATT&CK ICS T1693, T0800 CIE 9, 2
BKS-FD-9	**Default credentials ship in the field** Devices are installed with default or hard-coded passwords that are listed in public manuals. Anyone who can reach a device can log in, and the same credentials open every unit of that model across the fleet. *Case: Unitronics PLCs at water utilities, 2023.*	**No device should go into service with a credential that anyone else knows.** **1** Require unique per-device credentials, or a forced change at commissioning, in every purchase. **2** Check commissioning records and scan the estate for devices still accepting default logins. **3** Reject products with hard-coded credentials that cannot be changed.	STRIDE S, E CAPEC CAPEC-70 CWE CWE-1392, CWE-798 ATT&CK ICS T1694.001, T1694.002 CIE 9, 3
BKS-FD-8	**A web panel runs the process †** Controllers and site managers carry embedded web interfaces that can change settings, and these end up reachable from the internet or the business network. Weak or missing authentication on the panel gives direct control of the process to anyone who finds it. *Case: Bremanger dam, Norway, 2025; Supermarket refrigeration attacks, 2026.*	**Remove device features that are not needed to run the process, and never expose control interfaces directly.** **1** Disable embedded web and remote configuration services that the operating design does not need. **2** Place any remaining interfaces behind authenticated remote access, never on a public address. **3** Scan regularly for estate devices visible from the internet, using the same search engines attackers use.	STRIDE S, E, T CAPEC – CWE CWE-306, CWE-1188 ATT&CK ICS T0883, T0819 CIE 4, 3
BKS-FD-7	**Logic can change while it runs †** Controllers allow programs to be downloaded or edited online while the process runs, with no physical key or local approval. An attacker who reaches the engineering protocol can change what the plant does without stopping it or being seen. *Case: Stuxnet, 2010.*	**Changing control logic should need a deliberate, local, visible act.** **1** Use a physical run/program key or switch, kept in run, and alarm when it changes. **2** Restrict online edits and downloads to named engineering workstations at set times. **3** Compare running logic with an approved copy on a schedule.	STRIDE T, E CAPEC CAPEC-441 CWE CWE-862 ATT&CK ICS T0843.002, T0889, T0858 CIE 2, 3
BKS-FD-6	**Devices cannot prove what they run** There is no way to ask a controller what logic and firmware it is really running and trust the answer. A tampered device reports whatever the attacker chooses, so changes go unnoticed and recovery cannot confirm a device is clean. *Case: Stuxnet, 2010.*	**Be able to verify a device's logic and firmware from a trusted source the device itself does not control.** **1** Prefer devices with measured boot and attestation that a separate system can check. **2** Keep approved copies and hashes of logic and firmware offline, and compare periodically. **3** During recovery, re-flash from trusted images rather than trusting a device's own report.	STRIDE T, R CAPEC CAPEC-440 CWE CWE-1283, CWE-1326 ATT&CK ICS T0851, T0835 CIE 8, 2

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FD-5	**Hidden test and debug modes** Firmware ships with debug commands, test modes, undocumented accounts or factory functions left active. They bypass normal checks and let an attacker run the device in ways the operator never sees in the manual.	**Ship devices with only the functions the operator knows about, and disable the rest.** 1 Ask suppliers to declare all debug, test and maintenance functions, and to show how they are disabled in production. 2 Test devices before purchase for undocumented services and accounts. 3 Remove or lock maintenance modes before commissioning.	STRIDE E, T CAPEC CAPEC-121 CWE CWE-489, CWE-912 ATT&CK ICS T0858 CIE 9, 4
BKS-FD-4	**The controller cannot be patched** Controllers built to last decades run firmware the vendor no longer updates, or cannot be updated without a long outage. Known weaknesses stay open for the life of the plant, and the same unpatched model sits at many sites.	**Plan for the life of the plant, not of the software, and put protection around what cannot be fixed.** 1 Require in contracts a support period and update path that match the asset's expected life. 2 Keep a register of devices that can no longer be patched, and put compensating controls around each. 3 Budget replacement of unsupported controllers in the capital plan.	STRIDE T, E, D CAPEC – CWE CWE-1329, CWE-1277, CWE-1104 ATT&CK ICS – CIE 8, 10, 4
BKS-FD-3	**Maintenance ports at unattended sites** Serial, USB, debug and local panel ports on devices at remote, unmanned sites are open to anyone who can get through a fence or cabinet door. A brief visit can change logic, extract credentials or plant an implant.	**Treat physical access to an unattended site as access to the network.** 1 Lock and seal cabinets, and alarm door and port use to the control centre. 2 Disable unused ports in device configuration and cover the rest physically. 3 Inspect and record what is connected to each device on every site visit.	STRIDE T, I, E CAPEC CAPEC-401 CWE CWE-1191, CWE-1263 ATT&CK ICS T0864, T0847 CIE 2, 5
BKS-FD-2	**Wireless links to field devices** Field devices and sensors that report or are configured over radio, Wi-Fi or Bluetooth can be listened to, impersonated or reconfigured from outside the site. Encryption is weak or off and pairing is open.	**Treat every radio link to the field as an untrusted network.** 1 Use authenticated encryption on wireless field links, with keys unique to each site. 2 Disable wireless configuration interfaces after commissioning. 3 Monitor for unknown devices and unusual traffic on field radio networks.	STRIDE I, S, T CAPEC CAPEC-157 CWE CWE-319 ATT&CK ICS T0860, T0887 CIE 3, 5

CC · CONTROL CENTRE AND SCADA

THE ESTATE · BKS-CC-A TO BKS-CC-2 · https://ostering.com/taxonomies/critical-infrastructure/control-centre-and-scada/

Where operators see and steer the process: HMIs, historians, engineering workstations, alarms and the people at the desk.

BKS-CC-A The screen is the only witness †
BKS-CC-K The operator's tools do the damage †
BKS-CC-Q One directory for IT and OT
BKS-CC-J The engineering workstation holds every key †
BKS-CC-10 Alarm floods bury the critical one †
BKS-CC-9 A flat network behind the firewall
BKS-CC-8 The historian is a bridge
BKS-CC-7 Nobody has rehearsed manual operation †
BKS-CC-6 The backup centre fails too
BKS-CC-5 Shared operator accounts
BKS-CC-4 Legacy operating systems on HMIs
BKS-CC-3 Too little logging in OT
BKS-CC-2 Data crosses on USB sticks

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-CC-A	**The screen is the only witness †** Control rooms have removed local gauges, panel indicators and independent instruments, so the HMI is the only way to know the state of the plant. When its values are replayed or altered, operators see a normal plant while the process is driven out of control, and nothing tells them otherwise. *Case: Stuxnet, 2010.*	**Critical process states must be visible through a path the control system cannot falsify.** **1** Install independent instruments for the most critical variables, with their own display or alarm. **2** Cross-check SCADA values against physics and independent sensors, and alarm on disagreement. **3** Train operators to trust local readings and plant behaviour over the screen when they conflict.	STRIDE S, T CAPEC CAPEC-148 CWE CWE-451 ATT&CK ICS T0832, T0829 CIE 2, 5
BKS-CC-K	**The operator's tools do the damage †** The control system lets an operator session open breakers, stop pumps or change modes across many sites in a few clicks, with no second check. An attacker who takes over a session uses the operator's own HMI to cause the outage. *Case: Ukraine grid attack, 2015.*	**Wide-area and irreversible commands should need more than one person and more than one session.** **1** Require a second authorised person to confirm commands that affect many sites or critical assets. **2** Limit how many sites or assets one command or one session can change in a period. **3** Show operators who else is connected and what they are doing in real time.	STRIDE E, T CAPEC – CWE – ATT&CK ICS T0823, T0831, T0886 CIE 2, 4
BKS-CC-Q	**One directory for IT and OT** The control environment trusts the corporate directory, so compromising the business domain grants accounts and administrative rights on SCADA servers and workstations. The boundary between IT and OT exists on the diagram only. *Case: Volt Typhoon pre-positioning, 2024 advisory; NotPetya, 2017.*	**Operational systems must not depend on the business identity system to decide who is trusted.** **1** Run a separate directory for OT with no trust relationship to the corporate domain. **2** Use separate, MFA-protected accounts for OT administration, never reused from IT. **3** Test whether a fully compromised corporate domain can reach any OT system.	STRIDE E, S CAPEC CAPEC-560 CWE CWE-653 ATT&CK ICS T0859 CIE 3, 5
BKS-CC-J	**The engineering workstation holds every key †** One engineering workstation holds the project files, programming software and passwords for every controller in the plant. Compromise it, or infect its project files, and the attacker can reprogram the whole estate with the engineers' own tools. *Case: Stuxnet, 2010.*	**Engineering capability should be split, protected and used only when needed.** **1** Keep engineering workstations off the network except during planned work, and log every session. **2** Store controller credentials in a protected vault, not in project files or on the desktop. **3** Check project files against approved versions before downloading them to controllers.	STRIDE E, T, I CAPEC CAPEC-441 CWE CWE-256, CWE-653 ATT&CK ICS T0873, T0843 CIE 3, 11

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-CC-10	**Alarm floods bury the critical one †** Alarm management is weak, and false or nuisance alarms can be generated from the control network. An adversary floods operators with alarms during the attack, so the one that matters is missed, acknowledged in bulk or shelved.	**Operators must be able to see the critical alarm whatever else is happening.** **1** Rationalise alarms to a load operators can handle in a serious incident, with clear priorities. **2** Route the most critical alarms through an independent path and display that bulk acknowledgement cannot clear. **3** Detect abnormal alarm rates and treat a flood as a possible attack.	STRIDE D, S CAPEC – CWE – ATT&CK ICS T1692.002 CIE 2, 6
BKS-CC-9	**A flat network behind the firewall** Inside the control centre, servers, HMIs, engineering workstations and controllers share one network with no zones. A single foothold reaches everything, and nothing slows or reveals lateral movement.	**Divide the control network into zones by function and consequence, with controlled conduits between them.** **1** Zone the control network following IEC 62443 zones and conduits, with the most critical assets in the smallest zones. **2** Allow only the protocols and hosts each conduit needs, and deny the rest. **3** Monitor traffic between zones and alarm on new connections.	STRIDE E, T CAPEC CAPEC-700 CWE CWE-653 ATT&CK ICS T0886, T0867 CIE 3, 5
BKS-CC-8	**The historian is a bridge** Historians, reporting servers and data links that copy process data to the business network are two-way or dual-homed. The route built to let data out becomes the route the attacker uses to get in.	**Data should leave the control network by a path that cannot carry traffic back in.** **1** Use a DMZ with a replica historian, so business users never connect to the OT historian. **2** Use one-way data diodes for data that only needs to leave. **3** Remove dual-homed hosts and document every link between IT and OT.	STRIDE E, I CAPEC CAPEC-700 CWE CWE-669 ATT&CK ICS T0886 CIE 3
BKS-CC-7	**Nobody has rehearsed manual operation †** Procedures, staffing and training assume the SCADA system works. When it must be switched off because it cannot be trusted, operators do not know how to run the plant by hand, so a cyberattack becomes a total outage. *Case: Norsk Hydro, 2019; Ukraine grid attack, 2015.*	**Be able to run essential functions safely without the control system, for long enough to rebuild it.** **1** Write and rehearse manual operating procedures for the essential functions, with field staff. **2** Keep the local controls, gauges and hand tools that manual operation needs, and test them. **3** Plan staffing for sustained manual operation, which takes many more people.	STRIDE D CAPEC – CWE – ATT&CK ICS T0827 CIE 10, 12
BKS-CC-6	**The backup centre fails too** The backup control centre replicates the primary in real time, with the same accounts, software and connections. A wiper or malicious change in the primary reaches the backup in seconds, so it fails at the same moment.	**A backup control centre must be able to survive what destroys the primary.** **1** Use separate credentials and administration for the backup centre. **2** Delay or check replication of configuration and software changes, so damage can be stopped. **3** Exercise switching to the backup after a simulated destructive attack on the primary.	STRIDE D, T CAPEC – CWE – ATT&CK ICS T0809 CIE 10, 5

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-CC-5	**Shared operator accounts** Operators share generic accounts on HMIs and servers, so no action can be tied to a person. An attacker using the same account looks like a shift worker, and investigators cannot tell which actions were legitimate.	**Every action on the control system should be traceable to one person.** **1** Give each operator and engineer a named account, with quick log-on at the HMI. **2** Log commands and setpoint changes with the named user, and keep the logs off the HMI. **3** Review use of any remaining shared or service accounts.	STRIDE S, R CAPEC – CWE CWE-778 ATT&CK ICS T0859 CIE 12, 3
BKS-CC-4	**Legacy operating systems on HMIs** HMIs and SCADA servers run operating systems the vendor no longer supports, because the control software is certified only for them. They cannot run current protection and carry known weaknesses for years.	**Contain what cannot be updated, and plan its replacement.** **1** Isolate unsupported hosts in their own zone, with application allow-listing. **2** Require vendors to certify current operating systems within an agreed period. **3** Track unsupported systems in the risk register with an owner and a date.	STRIDE T, E CAPEC – CWE CWE-1104 ATT&CK ICS T0866 CIE 8, 10
BKS-CC-3	**Too little logging in OT** Control systems keep few logs, store them on the device or host, and nobody watches OT network traffic. An adversary can live in the environment for years, clearing what traces there are, and leave no record to investigate. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**Collect OT security logs and network data centrally, where the adversary cannot erase them.** **1** Send logs from OT hosts and devices to a protected collector with retention measured in years. **2** Deploy passive OT network monitoring that understands industrial protocols. **3** Alarm when a log source falls silent.	STRIDE R, I CAPEC CAPEC-571 CWE CWE-778 ATT&CK ICS T0872 CIE 6, 8
BKS-CC-2	**Data crosses on USB sticks** Patches, recipes, backups and reports move in and out of the control network on removable media because there is no other path. Malware rides in on them and reaches hosts that have no network route to the outside. *Case: Stuxnet, 2010.*	**Data crosses into the control network only through one controlled, checked point.** **1** Provide a single transfer point, such as a scanning kiosk or one-way gateway, for all files entering OT. **2** Block unknown USB storage on OT hosts and issue checked, company-owned media for the rest. **3** Log every file transfer into OT with who, what and why.	STRIDE T, E CAPEC – CWE – ATT&CK ICS T0847, T0864 CIE 9, 5

FM · FLEET MANAGEMENT PLATFORMS

THE ESTATE · BKS-FM-A TO BKS-FM-2 · https://ostering.com/taxonomies/critical-infrastructure/fleet-management-platforms/

One console running many sites: retail refrigeration, building management, charging, distributed energy, meters and telemetry.

BKS-FM-A One command reaches every site †
BKS-FM-K The platform is the master key †
BKS-FM-Q Every controller function is remote †
BKS-FM-J Sites cannot say no †
BKS-FM-10 A firmware push bricks the fleet †
BKS-FM-9 One vendor cloud, many operators
BKS-FM-8 The platform is the only view †
BKS-FM-7 Commands unsigned end to end †
BKS-FM-6 Integrations hold command rights
BKS-FM-5 No plan to cut the cord †
BKS-FM-4 Alarms only travel through the platform †
BKS-FM-3 Nobody can say who sent what
BKS-FM-2 Nobody knows what the fleet runs

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FM-A	**One command reaches every site †** The platform lets one operator, or one stolen session, send a dangerous command to every site at once: a setpoint, a mode change, a forced defrost or a shutdown. Nothing in the design limits how many sites a single action can touch, so one decision becomes a national event. *Case: Supermarket refrigeration attacks, 2026.*	**The blast radius of any single command is bounded by design, not by who happens to be logged in.** **1** Cap the number of sites one command can reach, and require a second named approver above the cap. **2** Roll fleet-wide changes out in waves that halt automatically when site telemetry moves away from normal. **3** Enforce each site's engineered safe envelope in the site controller, so out-of-range commands are refused locally.	STRIDE T, D, E CAPEC CAPEC-212 CWE CWE-1220, CWE-799 ATT&CK ICS T0831, T0836, T0858 CIE 1, 4, 2
BKS-FM-K	**The platform is the master key †** The central console or vendor cloud holds standing authority over every connected site. Compromising the platform, its administrators or its hosting gives direct control of the whole estate without touching a single site's own defences. *Case: Supermarket refrigeration attacks, 2026; Kaseya VSA and Coop Sweden, 2021.*	**No single system, account or provider holds unbroken authority over every site.** **1** Split the estate into independently administered cells, so one compromised cell cannot command the others. **2** Keep platform administration on separate identities, devices and networks from day-to-day operation. **3** Treat the platform as a crown-jewel asset: dedicated monitoring, privileged access review and tested compromise playbooks.	STRIDE S, T, E CAPEC CAPEC-122 CWE CWE-653, CWE-250 ATT&CK ICS T0822, T0859, T0886 CIE 3, 1, 5
BKS-FM-Q	**Every controller function is remote †** The platform exposes every function the site controllers support, including defrost, test modes, factory reset, flushing and limit overrides, because exposing everything was easiest. Functions only an engineer standing at the plant should ever use become commands anyone on the platform can send. *Case: Supermarket refrigeration attacks, 2026.*	**Expose remotely only the functions remote operation needs; dangerous functions stay local or need local confirmation.** **1** Classify every controller function by consequence and disable remote access to the dangerous class by default. **2** Require a physical action at the site, such as a key switch or button, before hazardous modes start. **3** Limit how long, how often and how far any built-in cycle such as defrost can run, in the controller itself.	STRIDE T, E CAPEC CAPEC-212, CAPEC-36 CWE CWE-749, CWE-1188 ATT&CK ICS T0858, T0836, T0821 CIE 4, 2, 1
BKS-FM-J	**Sites cannot say no †** Site controllers execute whatever the platform sends. They have no local check of whether a command is safe now (store open, tank low, demand peaking) and no local override that the platform itself cannot switch off, so the site's own knowledge never gets a vote.	**The site that bears the consequence keeps a veto over commands that would harm it.** **1** Give each site controller interlocks that reject commands unsafe for its current process state. **2** Provide a hard-wired local override that returns the site to safe standalone control and cannot be disabled remotely. **3** Report every refused command back to the platform and to the site operator as a security event.	STRIDE T, E CAPEC CAPEC-212 CWE CWE-807, CWE-863 ATT&CK ICS T1692.001, T0831 CIE 2, 1, 5

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FM-10	**A firmware push bricks the fleet †** The platform can push firmware and configuration to every device it manages. A malicious, corrupted or wiping image sent through that channel disables the fleet in one operation, and recovery means a person visiting every site with replacement hardware. *Case: Viasat KA-SAT modems, 2022.*	**Mass updates are signed, staged and reversible, and no single push can reach the whole fleet.** **1** Accept only firmware signed by keys held off the platform, and verify the signature on the device. **2** Deploy updates in rings with a hold period, and stop automatically when early rings report failures. **3** Keep a protected recovery image on every device that a remote push cannot overwrite.	STRIDE T, D CAPEC CAPEC-186, CAPEC-669 CWE CWE-494, CWE-347 ATT&CK ICS T1693, T0800 CIE 9, 10, 4
BKS-FM-9	**One vendor cloud, many operators** A single vendor platform serves many operators: competing retailers, several water companies, utilities in different countries. A failure of tenant isolation, or a compromise of the vendor's own administration plane, reaches every customer at once and across borders, which looks like a coordinated campaign against a whole sector. *Case: Supermarket refrigeration attacks, 2026.*	**An operator's sites are isolated from other customers and from the vendor's own administrators by default.** **1** Require contractual and technical tenant isolation, with vendor administrative access to your tenant off unless you grant it. **2** Ask vendors for evidence of how their administration plane is separated, monitored and tested. **3** Map which suppliers' platforms are shared with others in your sector, and plan for losing each one.	STRIDE E, I, D CAPEC CAPEC-122, CAPEC-180 CWE CWE-653, CWE-863 ATT&CK ICS T0859 CIE 9, 7, 3
BKS-FM-8	**The platform is the only view †** Operators see temperatures, pressures and levels only through the fleet dashboard. If the platform is compromised it can show normal values while sites fail; if it is down, nobody can see the sites at all. There is no second, independent way to know what is happening. *Case: Stuxnet, 2010.*	**Critical process state can be confirmed through a path the platform does not control.** **1** Fit independent alarm sensors at each site that report through a separate channel. **2** Cross-check platform readings against independent measurements and alarm on disagreement. **3** Write procedures for verifying site state locally when the dashboard cannot be trusted.	STRIDE T, D CAPEC CAPEC-148 CWE CWE-1293 ATT&CK ICS T0832, T0815, T0829 CIE 5, 10, 1
BKS-FM-7	**Commands unsigned end to end †** Commands travel from the console through brokers, gateways and cloud relays before reaching the site, and the site trusts whatever arrives from the last hop. Anyone who controls a relay can inject, alter or replay commands that the site accepts as genuine.	**A site acts only on commands it can verify came, unaltered and fresh, from an authorised operator.** **1** Sign commands at the point of authorisation and verify them in the site controller, not in an intermediate gateway. **2** Include sequence numbers and expiry in every command so replays and delayed commands are rejected. **3** Bind each command to the operator identity that approved it, and log that identity at the site.	STRIDE S, T CAPEC CAPEC-94, CAPEC-148 CWE CWE-924, CWE-940 ATT&CK ICS T0830, T1692.001 CIE 3, 2

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FM-6	**Integrations hold command rights** Energy optimisation, analytics, ticketing and ERP integrations call the platform API with long-lived keys or service accounts that can change setpoints or send commands. Nobody watches them as closely as human operators, and one leaked key works against every site the integration can reach.	**Machine accounts get the least authority their purpose needs, and command rights are never granted for convenience.** **1** Give integrations read-only access unless a named owner justifies each write or command scope. **2** Use short-lived, rotated credentials for API access, scoped to specific sites and functions. **3** Alert on any command issued by a service account outside its expected pattern or hours.	STRIDE S, E CAPEC CAPEC-21, CAPEC-122 CWE CWE-272, CWE-522 ATT&CK ICS T0871, T0859 CIE 3, 8
BKS-FM-5	**No plan to cut the cord †** When an advisory says to disconnect affected controllers, the operator finds there is no tested way to take sites off the platform quickly and run them safely standalone. Sites stay connected while the attack continues, or are disconnected into an unsafe state. *Case: Supermarket refrigeration attacks, 2026.*	**Every site can be isolated from central management quickly and continue in a safe, known local mode.** **1** Design and document a standalone mode for each site type that keeps the process safe without the platform. **2** Provide a single, tested action that severs a site or a whole region from the platform. **3** Rehearse fleet disconnection at least yearly and time how long it takes.	STRIDE D CAPEC – CWE – ATT&CK ICS T0827 CIE 10, 1
BKS-FM-4	**Alarms only travel through the platform †** Site alarms are routed to people only through the fleet platform's notification service. When the platform is attacked, overloaded or switched off, alarms stop reaching anyone, often at night when sites are unattended and damage builds for hours unnoticed. *Case: Supermarket refrigeration attacks, 2026.*	**Critical alarms reach a person even when central management is unavailable.** **1** Send high-priority alarms over a second path that does not depend on the platform. **2** Treat a silent site as an alarm: raise an alert when expected heartbeats stop arriving. **3** Test end-to-end alarm delivery regularly, including at night and at weekends.	STRIDE D CAPEC CAPEC-603 CWE CWE-1320 ATT&CK ICS T0878, T0815 CIE 5, 7, 10
BKS-FM-3	**Nobody can say who sent what** The platform logs commands without the human operator's identity, source location or approval trail, and keeps the logs only in the vendor's cloud. After an incident the operator cannot tell which commands were legitimate, which sites were touched or when the attack began.	**Every command is attributable to a person and recorded where the operator can keep and query it.** **1** Log operator identity, source address, target sites and the before and after values for every command. **2** Stream platform logs to the operator's own monitoring, outside the vendor's control. **3** Protect logs against deletion and alteration by platform administrators.	STRIDE R CAPEC CAPEC-268 CWE CWE-778, CWE-223 ATT&CK ICS T0872 CIE 6, 8

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-FM-2	**Nobody knows what the fleet runs** The platform's inventory does not reliably record which firmware, model and exposure each site has. When a vulnerability is announced, the operator cannot say which sites are affected, so it either disconnects everything or guesses, and the guess is slower than the attacker. *Case: Supermarket refrigeration attacks, 2026.*	**The operator can answer which sites run what, and how they are reached, within an hour.** 1 Keep an authoritative inventory of model, firmware and connectivity per site, reconciled automatically against the devices. 2 Subscribe to advisories for every model in the fleet and match them to the inventory automatically. 3 Record which sites are reachable from the internet, and why, as part of the inventory.	STRIDE I CAPEC – CWE CWE-1104 ATT&CK ICS – CIE 8

RA · REMOTE AND VENDOR ACCESS

THE ESTATE · BKS-RA-A TO BKS-RA-2 · https://ostering.com/taxonomies/critical-infrastructure/remote-and-vendor-access/

Every way in from outside: VPNs, remote desktop tools, vendor tunnels, modems and exposed interfaces.

BKS-RA-A Control panels on the internet †
BKS-RA-K Edge appliances are the front door
BKS-RA-Q Vendor tunnels are always open †
BKS-RA-J Remote sessions land on the controls †
BKS-RA-10 Remote access is all or nothing
BKS-RA-9 Cellular modems bypass the perimeter
BKS-RA-8 Single-factor remote access
BKS-RA-7 Ad hoc desktop-sharing tools †
BKS-RA-6 Sessions nobody approves or records
BKS-RA-5 Leavers and subcontractors keep access
BKS-RA-4 Break-glass weaker than the front door
BKS-RA-3 OT can call out to anywhere
BKS-RA-2 Access granted once, kept forever

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RA-A	**Control panels on the internet †** Controller web panels, site managers and HMIs are reachable directly from the internet so engineers and vendors can reach them from anywhere. Anyone who finds the address meets only a login page, or nothing, between them and the physical process. *Case: Bremanger dam, Norway, 2025; Unitronics PLCs at water utilities, 2023; Supermarket refrigeration attacks, 2026.*	**No control interface is directly reachable from the internet.** **1** Place every control interface behind brokered remote access, and verify from outside that none answers. **2** Scan your own address ranges continuously, and use exposure-search services to find what others can see. **3** Make suppliers declare and justify any internet path into a site before installation.	`STRIDE` S, E `CAPEC` CAPEC-115 `CWE` CWE-306 `ATT&CK ICS` T0883, T0819 `CIE` 3, 4, 8
BKS-RA-K	**Edge appliances are the front door** The VPN concentrators, firewalls and remote access gateways that guard control networks are themselves internet-facing devices, often unpatched and unmonitored. They are the first thing a patient adversary compromises, and access through them looks like normal remote working. *Case: Volt Typhoon pre-positioning, 2024 advisory; Danish energy sector, 2023.*	**The devices that guard remote access are maintained and watched as closely as the systems they protect.** **1** Patch internet-facing edge devices on an emergency timetable, and replace any the vendor no longer supports. **2** Send edge device logs to monitoring that is independent of the device itself. **3** Plan for edge compromise: remote access lands in a broker zone, never directly on the control network.	`STRIDE` S, E `CAPEC` CAPEC-555 `CWE` CWE-1104, CWE-1329 `ATT&CK ICS` T0819, T0866 `CIE` 5, 6, 8
BKS-RA-Q	**Vendor tunnels are always open †** Vendors keep a permanent VPN or tunnel into the site, live day and night whether or not any work is scheduled. A compromise of the vendor, or of one of its engineers, becomes standing entry to every customer site that tunnel reaches. *Case: Ukraine grid attack, 2015.*	**Remote access exists only for approved work, for as long as the work lasts.** **1** Keep vendor access disabled by default and enable it per job, with the site operator's approval. **2** Expire every remote session automatically after a set time. **3** Terminate vendor connections in a broker you control, not on equipment the vendor manages.	`STRIDE` S, E `CAPEC` CAPEC-555 `CWE` CWE-923 `ATT&CK ICS` T0822, T0886 `CIE` 3, 9
BKS-RA-J	**Remote sessions land on the controls †** A remote user lands on an HMI or engineering workstation with full operating authority, able to open breakers, change dosing or rewrite logic, when the job only needed to read a log. Whoever holds the session can drive the process as if sitting in the control room. *Case: Ukraine grid attack, 2015.*	**Remote access is scoped to the task, and operating authority from outside is the exception.** **1** Broker remote sessions through a jump host that grants read-only access unless operating rights are approved. **2** Require a local operator to watch, and be able to end, any remote session with operating rights. **3** Block remote use of the most hazardous operations entirely; they need someone on site.	`STRIDE` E, T `CAPEC` CAPEC-122 `CWE` CWE-250, CWE-1220 `ATT&CK ICS` T0886, T0823 `CIE` 3, 2, 1

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RA-10	**Remote access is all or nothing** Once a remote user is connected, they can reach every device on the site with full rights, whatever the job. A technician sent to read a fault log could rewrite logic or change setpoints, and so can anyone who takes over their session or account.	**Remote access is scoped to the task: the devices, the functions and the time the job needs, and no more.** **1** Grant remote sessions per job, limited to named devices and a time window, through a broker that enforces it. **2** Offer a read-only mode for diagnostics, and require a second approval to move to write access. **3** Block engineering protocols and download functions in remote sessions unless the job requires them.	STRIDE E CAPEC – CWE CWE-250 ATT&CK ICS T0822, T0859 CIE 3, 2
BKS-RA-9	**Cellular modems bypass the perimeter** A vendor fits a 4G router in the cabinet so it can reach its equipment without the operator's network team. The site now has a path into the control network that the firewall, monitoring and remote access policy never see.	**Every path into a control network is known, approved and monitored.** **1** Prohibit independent connectivity in supply contracts, and survey cabinets for cellular and radio modems. **2** Route any approved cellular link through the same brokered access and monitoring as wired links. **3** Watch for unexpected wireless devices and new routes from control networks.	STRIDE S, E CAPEC CAPEC-616 CWE CWE-420 ATT&CK ICS T0883, T0822 CIE 8, 3
BKS-RA-8	**Single-factor remote access** Remote access to control networks relies on a password alone, or on a second factor that can be phished, pushed until accepted, or reset by a help desk on request. Stolen or guessed credentials are all an adversary needs. *Case: Marks & Spencer and Co-op, 2025.*	**Remote access to control systems requires strong, phishing-resistant authentication.** **1** Require phishing-resistant multi-factor authentication for every remote route into control networks. **2** Make resets of remote access credentials need verification through an independent channel. **3** Alert on remote logins from new locations, devices or hours.	STRIDE S CAPEC CAPEC-560, CAPEC-600 CWE CWE-308, CWE-654 ATT&CK ICS T0859, T0822 CIE 3, 12
BKS-RA-7	**Ad hoc desktop-sharing tools †** Staff and vendors install desktop-sharing tools on HMIs and workstations to get help quickly, set for unattended access. Nobody manages them centrally, they reach out through the firewall, and their credentials live in personal accounts.	**Only approved, centrally managed remote access tools run on control systems.** **1** Allow-list remote access software on control workstations and remove everything else. **2** Block outbound connections from control networks to remote-access services you have not approved. **3** Check control workstations regularly for remote-access tools and unattended-access settings.	STRIDE S, E CAPEC CAPEC-555 CWE CWE-420, CWE-1188 ATT&CK ICS T0822, T0886 CIE 8, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RA-6	**Sessions nobody approves or records** Remote sessions start without the site operator knowing and leave no recording of what was done. During an incident, nobody can tell a vendor's routine maintenance from an adversary, and afterwards nobody can prove what changed.	**Every remote session is approved, visible while it runs and recorded.** 1 Require approval from the site operator before a remote session starts. 2 Show active remote sessions on the operator's screen, with a way to end them. 3 Record sessions with operating rights and keep the recordings outside the vendor's reach.	STRIDE R CAPEC CAPEC-268 CWE CWE-778 ATT&CK ICS T0886 CIE 6, 12
BKS-RA-5	**Leavers and subcontractors keep access** Vendor staff turn over and work is subcontracted again and again, but remote accounts are not tied to named people or reviewed. Former engineers, and the firms they move to, still hold working access years later.	**Remote access belongs to named, current people, and is removed when they leave or the contract ends.** 1 Require vendors to tell you about leavers, and suspend accounts not used for a set period. 2 Review every remote account against a named, current person at least quarterly. 3 Put subcontractor access in the contract chain, with the same rules as the prime supplier.	STRIDE S, E CAPEC CAPEC-560 CWE – ATT&CK ICS T0859 CIE 9, 12
BKS-RA-4	**Break-glass weaker than the front door** An emergency path exists for when normal remote access fails: a shared local administrator, an old dial-up modem, a spare account in an envelope. It bypasses the controls on the main path, so an adversary uses it, or in a real crisis it does not work.	**Emergency access is as strong as normal access, and is tested and monitored.** 1 Inventory every emergency access path and remove the ones that are not needed. 2 Protect break-glass accounts with strong credentials, alerting on every use, and review after each use. 3 Test emergency access in exercises so it works when the main path is down.	STRIDE S, E CAPEC CAPEC-115 CWE CWE-288 ATT&CK ICS T0859 CIE 10, 3
BKS-RA-3	**OT can call out to anywhere** Control networks allow outbound connections to the internet for updates, telemetry and remote tools. Implants and ad hoc remote tools reach their operators through ordinary web traffic, and data leaves without anyone noticing, because nobody defined where OT is allowed to talk.	**Outbound traffic from control networks is denied by default and allowed only to named destinations for named purposes.** 1 Deny outbound internet access from control networks and allow only listed destinations through a proxy. 2 Alert on any new outbound destination, protocol or volume from OT hosts. 3 Bring vendor updates and telemetry through a controlled relay in a DMZ rather than direct connections.	STRIDE I, E CAPEC – CWE CWE-923 ATT&CK ICS T0885, T0869 CIE 3, 6

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-RA-2	**Access granted once, kept forever** Firewall rules and accounts opened for one commissioning job or emergency are never closed. Over the years remote access grows broader than any current task needs, and nobody can say why each path exists.	**Every remote access rule has an owner, a purpose and an end date.** 1 Give every firewall rule and remote account an owner, a reason and an expiry date. 2 Remove rules and accounts automatically at expiry unless the owner renews them. 3 Review remote access paths against current maintenance needs every year.	STRIDE E CAPEC CAPEC-180 CWE CWE-272 ATT&CK ICS – CIE 4, 8

TT · TELECOMS AND TIMING

THE ESTATE · BKS-TT-A TO BKS-TT-2 · https://ostering.com/taxonomies/critical-infrastructure/telecoms-and-timing/

The links and clocks the estate runs on: GNSS, private radio, cellular, satellite, leased lines and time sources.

BKS-TT-A One bearer, a region goes dark †
BKS-TT-K The provider can brick the terminals
BKS-TT-Q Anyone can send the radio command †
BKS-TT-J GNSS is the only clock †
BKS-TT-10 The carrier's network is the target
BKS-TT-9 Network time can be moved
BKS-TT-8 Cellular devices on the open network
BKS-TT-7 SMS commands and alarms are trusted
BKS-TT-6 Telemetry readable in the clear
BKS-TT-5 Wireless field networks can be jammed †
BKS-TT-4 Rogue base stations and downgrades
BKS-TT-3 Private circuits that aren't private
BKS-TT-2 Nobody gets the 3 a.m. call

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TT-A	**One bearer, a region goes dark †** Telemetry and remote control for a whole region ride a single carrier, satellite service or cellular network. When that bearer is wiped, jammed or cut, operators lose sight and control of every site on it at once, and monitoring is lost far beyond the original target. *Case: Viasat KA-SAT modems, 2022.*	**No single communications bearer carries all monitoring and control for a region.** 1 Give critical sites two diverse bearers from different providers and technologies. 2 Design sites to fail safe and continue locally when all communications are lost. 3 Map which sites depend on each carrier and satellite service, and plan for losing each.	STRIDE D CAPEC CAPEC-603, CAPEC-582 CWE – ATT&CK ICS T0829, T0827 CIE 7, 10, 5
BKS-TT-K	**The provider can brick the terminals** Satellite terminals, routers and modems are managed by the communications provider, which can push configuration and firmware to all of them. If its management system is compromised, terminals across many customers can be disabled at once, and each one needs a visit to replace. *Case: Viasat KA-SAT modems, 2022.*	**The operator can recover connectivity without depending on the provider's management system.** 1 Ask providers how terminal management is secured and segmented, and what a fleet-wide wipe would take to recover. 2 Keep spare terminals and pre-configured replacements for critical sites. 3 Prefer terminals with protected recovery images that remote management cannot overwrite.	STRIDE D, T CAPEC CAPEC-186 CWE CWE-494 ATT&CK ICS T1693, T0826 CIE 9, 10
BKS-TT-Q	**Anyone can send the radio command †** Operational radio systems accept commands from anyone transmitting on the right frequency: emergency stops on rail radio, telemetry and commands on utility radio. The command was designed for safety and convenience, not authenticated, so cheap equipment can stop or start operations across a network. *Case: Polish rail radio stops, 2023.*	**Commands sent over radio are authenticated before they are acted on.** 1 Add authentication to radio commands, or move them to authenticated digital systems. 2 Detect and locate unexpected transmissions on operational frequencies. 3 Where legacy radio cannot change, limit what a radio command can do and require confirmation through another channel.	STRIDE S, D CAPEC CAPEC-151 CWE CWE-306, CWE-940 ATT&CK ICS T0860, T1692.001 CIE 2, 6
BKS-TT-J	**GNSS is the only clock †** Protection relays, synchrophasors, telecoms synchronisation and event logs take their time from satellite navigation signals. Jamming or spoofing those signals shifts or removes time, which can upset protection, corrupt the sequence of events and break network synchronisation over a wide area. *Case: GNSS interference, Baltic region.*	**Critical timing has a holdover and a second source that do not depend on satellite signals.** 1 Fit timing equipment with holdover oscillators sized for the longest credible outage. 2 Use a terrestrial time source, such as a network time service, as a cross-check and backup. 3 Detect jamming and spoofing at receivers and alarm when time sources disagree.	STRIDE T, D CAPEC CAPEC-627, CAPEC-599 CWE CWE-348, CWE-1293 ATT&CK ICS – CIE 5, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TT-10	**The carrier's network is the target** A state adversary compromises the telecommunications operator itself: its core, its management systems, its lawful-intercept and its staff. From there it can read, reroute or cut the utility traffic that crosses the carrier, without touching the utility at all.	**Control traffic stays confidential and authenticated even if the carrier is compromised.** 1 Encrypt and authenticate control and telemetry traffic end to end, so the carrier sees only ciphertext. 2 Avoid relying on the carrier's network for authentication or trust between sites. 3 Agree with carriers how they will notify you of compromise, and rehearse running without them.	STRIDE I, T, D CAPEC CAPEC-94, CAPEC-117 CWE CWE-319, CWE-924 ATT&CK ICS T0830 CIE 3, 7, 9
BKS-TT-9	**Network time can be moved** Servers, controllers and logs take time from unauthenticated network time services. Whoever can shift the clock can expire certificates, fire schedules at the wrong moment, break authentication tokens and scramble the evidence of what happened when.	**Time used for security, scheduling and evidence comes from authenticated, cross-checked sources.** 1 Use authenticated network time protocols and internal time servers for control networks. 2 Reject clock changes larger than a set limit without operator approval. 3 Alarm when internal clocks drift apart or jump.	STRIDE T CAPEC CAPEC-94 CWE CWE-924 ATT&CK ICS – CIE 3, 5
BKS-TT-8	**Cellular devices on the open network** Field devices connect through public cellular networks with addresses reachable from the internet or from other subscribers. Anyone who can reach the address can talk to the device, and the operator often does not know which devices are exposed this way.	**Cellular field devices are reachable only from the operator's own systems.** 1 Use a private access point name or private cellular network with no internet routing. 2 Block inbound connections to field devices at the carrier, and test that the block works. 3 Keep a register of every SIM, its device and its permitted destinations.	STRIDE S, E CAPEC CAPEC-616 CWE CWE-923 ATT&CK ICS T0883 CIE 3, 8
BKS-TT-7	**SMS commands and alarms are trusted** Pumping stations, generators and alarm panels accept commands by text message, or send alarms only by SMS. Sender numbers can be spoofed, messages delayed or blocked, and the gateway that sends alarms becomes a single point of failure.	**Text messaging is never the only path for alarms and never authorises control actions on its own.** 1 Remove SMS command functions, or require authentication that does not rely on the sender's number. 2 Send critical alarms over at least two independent channels and confirm delivery. 3 Monitor SMS gateways for failure and treat silence as an alarm.	STRIDE S, D CAPEC CAPEC-151 CWE CWE-290, CWE-940 ATT&CK ICS T1692.001, T0878 CIE 2, 5
BKS-TT-6	**Telemetry readable in the clear** Telemetry and commands cross radio links, leased lines and shared networks without encryption. Anyone listening learns how the process works and where the critical points are, and can record traffic to replay or imitate later.	**Telemetry and commands are protected wherever they leave a physically secured site.** 1 Encrypt and authenticate telemetry on radio, leased-line and shared network links. 2 Where legacy links cannot be encrypted, wrap them in protected tunnels at both ends. 3 Treat captured telemetry as sensitive engineering information when planning protection.	STRIDE I, T CAPEC CAPEC-157 CWE CWE-319 ATT&CK ICS T0887, T0842 CIE 3, 11

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TT-5	**Wireless field networks can be jammed †** Sensors and controllers on Wi-Fi, low-power radio or licensed radio links can be silenced by a jammer near the site. The process loses its inputs, alarms stop arriving, and the system may treat silence as normal.	**Loss of a wireless link is detected at once and leads to a safe state.** 1 Detect loss of wireless updates within seconds and drive the process to a safe state. 2 Keep safety-critical signals on wired links. 3 Monitor the radio spectrum at critical sites for jamming.	STRIDE D CAPEC CAPEC-601, CAPEC-604 CWE – ATT&CK ICS T1695.003, T0815 CIE 2, 5
BKS-TT-4	**Rogue base stations and downgrades** Cellular devices can be lured onto a fake base station or forced down to older, weaker network generations. The adversary can then intercept, block or alter their traffic close to the site, without touching the carrier or the operator.	**Field devices do not depend on the cellular network for confidentiality or authenticity.** 1 Disable older network generations on field modems where coverage allows. 2 Protect device traffic end to end, so a rogue base station gains nothing. 3 Alert when devices change network generation or cell unexpectedly.	STRIDE S, I, T CAPEC CAPEC-617, CAPEC-606 CWE – ATT&CK ICS T0830 CIE 3
BKS-TT-3	**Private circuits that aren't private** The operator believes its telemetry runs on dedicated leased lines, but the carrier has long since migrated them onto shared IP networks. The assumptions behind the security design, physical separation and no third party in the path, are no longer true.	**Assumptions about how communications are carried are checked, not inherited.** 1 Ask carriers in writing how each circuit is delivered today, and repeat the question after migrations. 2 Protect traffic on every circuit as if it crossed a shared network. 3 Record bearer technology in the asset inventory and review it each year.	STRIDE I, T CAPEC – CWE – ATT&CK ICS – CIE 8, 7
BKS-TT-2	**Nobody gets the 3 a.m. call** Out-of-hours alarms reach on-call staff through one paging or notification service. If it fails, is jammed or is attacked at night or at a weekend, damage builds unnoticed until staff arrive in the morning. *Case: Supermarket refrigeration attacks, 2026.*	**Out-of-hours alarms reach a person through more than one route, and failures are noticed.** 1 Use two independent notification routes for critical alarms and require acknowledgement. 2 Escalate automatically when an alarm is not acknowledged within a set time. 3 Test out-of-hours alarm delivery regularly, unannounced.	STRIDE D CAPEC CAPEC-603 CWE CWE-1320 ATT&CK ICS T0878 CIE 5, 10

LS · LOGISTICS AND SUPPLY

THE ESTATE · BKS-LS-A TO BKS-LS-2 · https://ostering.com/taxonomies/critical-infrastructure/logistics-and-supply/

How food, fuel, medicines and goods get from warehouse to shelf, pump and pharmacy.

BKS-LS-A Cold-chain records cannot be trusted †
BKS-LS-K One distribution centre feeds a region
BKS-LS-Q Product data changes the label †
BKS-LS-J Medicines stop at the wholesaler †
BKS-LS-10 Fuel stops at the pump
BKS-LS-9 Tills fail and shops close
BKS-LS-8 Warehouse machines obey false orders †
BKS-LS-7 Port terminal stops moving boxes
BKS-LS-6 Ordering data quietly corrupted
BKS-LS-5 Fleet telematics immobilise the lorries
BKS-LS-4 Just-in-time leaves no buffer
BKS-LS-3 Tracking reveals what matters
BKS-LS-2 Delivery slots and yard bookings jammed

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-LS-A	**Cold-chain records cannot be trusted †** Temperature logs for food and medicines are stored and reported by systems that can be edited remotely. An adversary hides an excursion so unsafe stock is sold or dispensed, or fakes one so safe stock is destroyed, and nobody can tell which records are true.	**Cold-chain evidence is produced and kept where the system that controls the temperature cannot rewrite it.** **1** Log temperatures from independent sensors that the refrigeration controller and fleet console cannot configure or write to. **2** Sign readings at the logger and keep them in append-only storage held by a different party. **3** Define a release rule: stock whose record is missing or inconsistent is held for inspection, never sold by default.	STRIDE T, R CAPEC CAPEC-268, CAPEC-194 CWE CWE-353, CWE-1293 ATT&CK ICS T0832, T0836 CIE 1, 2, 3
BKS-LS-K	**One distribution centre feeds a region** A regional distribution centre's warehouse management and control systems decide what reaches hundreds of stores, pharmacies or depots. Stopping or wiping them empties shelves within days, because stores hold little stock and nothing else knows what to pick, where it is or where it goes. *Case: United Natural Foods, 2025; Marks & Spencer and Co-op, 2025.*	**No single site's systems should be able to stop supply to a whole region, and each site can pick and ship without them.** **1** Design a degraded mode: printed or locally cached pick lists, location maps and route sheets refreshed daily. **2** Keep enough spare capacity and current data at a second site to serve priority stores and pharmacies. **3** Separate the warehouse control network from corporate IT so a ransomware or wiper outbreak in one does not reach the other.	STRIDE D CAPEC – CWE – ATT&CK ICS T0828, T0826 CIE 7, 10, 1
BKS-LS-Q	**Product data changes the label †** Ingredient, allergen, use-by and dosage data flows from a central product database to label printers, shelf labels and websites. An adversary who alters it can put wrong allergen or dosage information on goods at scale, harming people and forcing mass recalls.	**Safety-critical product data is changed only with independent approval, and what is printed is checked against an approved source.** **1** Require two-person approval for changes to allergen, use-by and dosage fields, with alerts on bulk edits. **2** Keep a signed reference copy of safety-critical product data and compare label output against it before release. **3** Make recall of a batch fast: trace every label run to the data version that produced it.	STRIDE T, R CAPEC CAPEC-148, CAPEC-385 CWE CWE-353, CWE-862 ATT&CK ICS – CIE 1, 2, 11
BKS-LS-J	**Medicines stop at the wholesaler †** Pharmacies and hospitals depend on a few wholesalers' ordering, picking and pack-verification systems. If those stop, or the national verification service that checks each pack goes down, dispensing stops even though medicines sit in the warehouse.	**Medicine supply has a planned way to keep dispensing when ordering or verification systems are unavailable.** **1** Agree and test an emergency ordering route with each wholesaler that works by phone and paper for critical medicines. **2** Define in advance how dispensing continues when pack verification is unreachable, with a reconciliation step afterwards. **3** Hold buffer stock of critical medicines at hospitals and at more than one wholesaler site.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 10, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-LS-10	**Fuel stops at the pump** Forecourt pumps, fleet fuel cards and subsidy schemes are authorised by central systems. Disabling them stops fuel for ambulances, generators, lorries and the public across a country at once, and messages on pump screens can be used to taunt or alarm. *Case: Iran fuel stations, 2021 and 2023.*	**Fuel can be dispensed to priority users when central authorisation is unavailable.** 1 Give forecourts a local offline mode with limits per card and later reconciliation. 2 Keep designated priority sites for emergency services and utilities that can dispense without the central system. 3 Control who can change pump display messages, and alert on fleet-wide display changes.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826, T0828 CIE 10, 1
BKS-LS-9	**Tills fail and shops close** Point-of-sale systems are managed, updated and authorised through a central platform or managed service provider. When that platform is used to push malware or simply stops, every store using it closes, though the food is on the shelves. *Case: Kaseya VSA and Coop Sweden, 2021.*	**Stores can sell essentials when central till management and authorisation are down.** 1 Design an offline sales mode with local price files and deferred card authorisation within set limits. 2 Keep the till management tool on its own network, accounts and approval workflow, not a general remote management tool. 3 Stage updates to tills in waves so one bad push cannot reach every store.	STRIDE D CAPEC CAPEC-186 CWE CWE-494 ATT&CK ICS T0862 CIE 10, 9, 5
BKS-LS-8	**Warehouse machines obey false orders †** Conveyors, shuttles, cranes and robots in automated warehouses take their moves from the warehouse control system. False commands can crash equipment, drop loads or move machines while people are in the aisles, and repairs to bespoke automation take weeks.	**Machine safety in automated warehouses does not depend on the commands being honest.** 1 Keep personnel protection (light curtains, area locks, emergency stops) in hard-wired safety circuits the control system cannot override. 2 Validate commands at the machine controller against physical limits for speed, load and position. 3 Hold spares and recovery images for bespoke automation controllers off site.	STRIDE T, D CAPEC CAPEC-153 CWE CWE-1284, CWE-807 ATT&CK ICS T0831, T0879, T1692.001 CIE 2, 1
BKS-LS-7	**Port terminal stops moving boxes** A container terminal's operating system tracks every box, gate booking and crane move. When it stops, the terminal stops, ships wait offshore and food, fuel components and medicines pile up, with backlogs that take far longer to clear than the outage lasted. *Case: DP World Australia, 2023; Port of Nagoya, 2023; NotPetya, 2017.*	**A terminal can keep moving priority cargo when its operating system is unavailable.** 1 Rehearse a manual mode for priority cargo with printed stowage and yard positions taken at least daily. 2 Isolate the terminal operating system from corporate IT and from remote access used by its vendor. 3 Keep an offline restorable copy of the yard inventory so recovery does not start from nothing.	STRIDE D CAPEC – CWE – ATT&CK ICS T0828, T0826 CIE 10, 3

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-LS-6	**Ordering data quietly corrupted** Replenishment depends on sales data, forecasts and supplier messages. Small, plausible changes cause under-ordering of staples or over-ordering that blocks storage, producing shortages that look like panic buying or supplier failure rather than an attack.	**Ordering systems detect implausible changes and cannot drift far from physical reality unnoticed.** 1 Set bounds on order changes per product and store, with human review outside them. 2 Reconcile system stock against periodic physical counts for essential lines. 3 Authenticate supplier and partner messages and keep a log that shows who changed forecasts and parameters.	STRIDE T CAPEC CAPEC-385, CAPEC-153 CWE CWE-1284 ATT&CK ICS – CIE 1, 6
BKS-LS-5	**Fleet telematics immobilise the lorries** Hauliers manage fleets through telematics platforms that can track, limit or immobilise vehicles and change their routes. One compromised platform or account can stop thousands of lorries and tankers at once, or send them to the wrong place.	**No remote platform can stop or redirect a whole fleet without local consent.** 1 Disable remote immobilisation, or limit it to one vehicle at a time with a second approval. 2 Make drivers and depots able to override remote limits safely, and confirm route changes by an independent channel. 3 Give the telematics vendor's administrators no standing access to customer fleets.	STRIDE T, E CAPEC CAPEC-122 CWE CWE-862, CWE-1220 ATT&CK ICS T0831, T0859 CIE 2, 4
BKS-LS-4	**Just-in-time leaves no buffer** Stock levels for food, fuel and medicines are tuned for cost, holding a day or two of supply. A disruption of a few days in any link becomes an outage for consumers, which is exactly the effect an adversary wants.	**Buffers for essential goods are sized for a deliberate disruption, not only for normal variation.** 1 Identify essential lines and set minimum stock in days of supply, reviewed against realistic outage durations. 2 Pre-position emergency stock away from the systems and sites most likely to be attacked together. 3 Agree in advance which goods and customers get priority when stock runs short.	STRIDE D CAPEC – CWE – ATT&CK ICS T0828 CIE 1, 10
BKS-LS-3	**Tracking reveals what matters** Shipment tracking, telematics and booking portals show where fuel tankers, medicine consignments and critical spares are and when they will arrive. Leaked or scraped, that data lets an adversary choose targets and time disruption for maximum effect.	**Location and schedule data for critical consignments is treated as sensitive and shared only with those who need it.** 1 Restrict who can see real-time position and schedule data for critical goods, and log every query. 2 Delay or coarsen tracking shown to customers and partners for sensitive loads. 3 Rate-limit and monitor portal and API access for bulk collection.	STRIDE I CAPEC CAPEC-169 CWE CWE-1220 ATT&CK ICS T0882 CIE 11, 3
BKS-LS-2	**Delivery slots and yard bookings jammed** Booking systems for delivery slots, gates and yards are reachable by many suppliers and hauliers. Flooding or falsifying bookings causes queues, missed slots and wasted refrigerated loads, a cheap way to degrade supply without touching the warehouse.	**Booking systems resist bulk abuse and fall back to a simple manual process.** 1 Require authenticated accounts per haulier with limits on bookings and changes. 2 Alert on unusual booking patterns and freeze changes when they occur. 3 Keep a manual gate procedure with a printed slot list for the next shift.	STRIDE S, D CAPEC CAPEC-125 CWE CWE-770, CWE-799 ATT&CK ICS – CIE 10, 5

TN · TRANSPORT NETWORKS

THE ESTATE · BKS-TN-A TO BKS-TN-2 · https://ostering.com/taxonomies/critical-infrastructure/transport-networks/

How people and goods move: rail signalling, level crossings, road tunnels, traffic control, airports, shipping lanes and the information that travellers act on.

BKS-TN-A Signalling obeys any well-formed command †
BKS-TN-K Level crossings fail open †
BKS-TN-Q Tunnel safety systems on the network †
BKS-TN-J Traction power switched off remotely †
BKS-TN-10 Signal cables share one route
BKS-TN-9 One centre times every junction †
BKS-TN-8 Motorway signs and lanes lie †
BKS-TN-7 Airports share one passenger platform
BKS-TN-6 Supplier app failure stops trains
BKS-TN-5 Vessel traffic trusts what ships report †
BKS-TN-4 Navigation data sends traffic astray
BKS-TN-3 Station boards speak for the attacker †
BKS-TN-2 Ticketing and gates fail badly

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TN-A	**Signalling obeys any well-formed command †** Interlockings, radio block centres and metro train control accept commands and movement authorities from their networks without checking where they came from. Anyone who reaches those networks, or the trackside points, can set routes, release locks or grant authorities the safety logic would refuse, and trains move on false permission. *Case: Łódź tram points, 2008.*	**Every command that moves points, sets routes or grants movement authority must be authenticated and must pass the interlocking's safety logic.** **1** Authenticate and integrity-protect every message between control centre, interlocking, radio block centre and train. **2** Keep route-setting and locking logic in the vital interlocking, so no network command can bypass it. **3** Zone signalling networks per CLC/TS 50701, with no path from business, passenger or maintenance networks.	`STRIDE` S, T, E `CAPEC` CAPEC-151 `CWE` CWE-306, CWE-940 `ATT&CK ICS` T1692.001, T0831, T0880 `CIE` 2, 3, 1 `STANDARDS` CLC/TS 50701, IEC 62443
BKS-TN-K	**Level crossings fail open †** Barriers, warning lights and the train detection that closes them are increasingly monitored and controlled remotely. If the controller can be told the line is clear, or fails with barriers raised, road traffic crosses in front of an approaching train.	**A level crossing must fail closed, and its closing must depend only on local train detection.** **1** Close barriers and stop road traffic on any loss of detection, power or communication. **2** Keep the closing logic local and vital, with remote links able to monitor but not to raise barriers. **3** Alarm the signaller and stop approaching trains when a crossing reports a fault or an unexpected state.	`STRIDE` T, D `CAPEC` – `CWE` CWE-636, CWE-306 `ATT&CK ICS` T0880, T0837, T0836 `CIE` 2, 1 `STANDARDS` CLC/TS 50701
BKS-TN-Q	**Tunnel safety systems on the network †** Road and rail tunnel ventilation, fire suppression, emergency lighting, barriers and evacuation signs are run by a tunnel control system linked to a remote centre. Changing them during a fire turns smoke towards people, closes exits or opens the tunnel to traffic that should be held outside.	**Tunnel life-safety functions must keep working, and stay in safe modes, whatever happens to the control network.** **1** Pre-program fire scenarios in the local controllers, started by local detection, and locked against remote change. **2** Give firefighters a local panel at each portal that overrides remote control. **3** Separate life-safety control from traffic management and monitoring networks, and alarm any remote change to safety modes.	`STRIDE` T, D, E `CAPEC` – `CWE` CWE-306, CWE-15 `ATT&CK ICS` T0880, T0831, T0836 `CIE` 1, 2, 3 `STANDARDS` IEC 62443
BKS-TN-J	**Traction power switched off remotely †** Substations that feed rail and metro lines are switched from a remote control room. Cutting traction power strands trains between stations and in tunnels, stops ventilation fed from the same supply, and can leave passengers walking along the track in the dark.	**Losing traction power must leave trains and passengers safe, and restoring it must not depend on the control network alone.** **1** Require local confirmation for switching that would de-energise sections with trains in tunnels. **2** Supply tunnel ventilation, lighting and communications from a source independent of traction power. **3** Rehearse local, manual restoration of traction power at each substation.	`STRIDE` D, T `CAPEC` – `CWE` CWE-306 `ATT&CK ICS` T0816, T0831, T0827 `CIE` 1, 10, 7 `STANDARDS` CLC/TS 50701, IEC 62443

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TN-10	**Signal cables share one route** Fibre and copper for signalling, points motors, train detection and line telecoms run in the same trackside conduits, for long distances, with little monitoring. Fire or cutting at a few points stops a line for days, because each cable must be found and repaired by hand. *Case: French high-speed rail arson, 2024.*	**No single cut or fire should take signalling, detection and communications off a whole line.** **1** Route critical signalling and telecom cables on separate paths where the line allows, or protect shared conduits. **2** Monitor conduits and cable integrity, and alarm on intrusion, heat or loss of continuity. **3** Keep repair kits, spare cable and degraded working rules ready for each line, and rehearse them.	STRIDE D CAPEC CAPEC-547 CWE – ATT&CK ICS T0826, T0828 CIE 7, 10, 1 STANDARDS CLC/TS 50701
BKS-TN-9	**One centre times every junction †** Urban traffic control centres push signal timings, priorities and plans to thousands of junction controllers, which also accept local maintenance access. A changed plan can gridlock a city, block emergency routes or, where safety checks are in software, show conflicting greens.	**Junction safety must be enforced locally in hardware, and central changes must be limited in scope and reversible.** **1** Keep conflicting-green protection in an independent hardware monitor at every junction, not in the timing plan. **2** Sign and approve timing plans before they reach controllers, and stage changes area by area. **3** Let controllers fall back to safe fixed timings when central control is lost or untrusted.	STRIDE T, D CAPEC – CWE CWE-1220, CWE-306 ATT&CK ICS T0836, T0831, T0813 CIE 2, 4, 10 STANDARDS IEC 62443
BKS-TN-8	**Motorway signs and lanes lie †** Lane signals, speed limits, variable message signs and ramp meters are set from a regional control centre. False closures send traffic into incidents or onto unsuitable roads, false messages cause panic, and open lanes can be shown where a crash or roadworks lie ahead.	**What drivers are told must come from authorised operators and match what the roadside detects.** **1** Authenticate every setting sent to roadside equipment, and log who set what. **2** Cross-check signals against incident detection, and alarm when signs and detected conditions disagree. **3** Limit sign messages to approved templates, with free text needing a second approver.	STRIDE S, T CAPEC CAPEC-148 CWE CWE-306, CWE-1293 ATT&CK ICS T0831, T0832 CIE 2, 6
BKS-TN-7	**Airports share one passenger platform** Check-in, bag drop, boarding and baggage systems at many airports run on shared platforms from a few vendors. One compromise stops processing at all of them at once, and manual fallback handles only a fraction of normal traffic. *Case: Collins Aerospace MUSE, 2025.*	**Passenger and baggage processing must keep running, at reduced scale, without the shared platform.** **1** Rehearse manual check-in, boarding and baggage handling at full shift scale, with printed materials ready. **2** Segment the airport's own systems from the vendor platform so one compromise does not reach both. **3** Agree recovery priorities and support capacity with the vendor for incidents that hit many airports at once.	STRIDE D CAPEC – CWE CWE-1357 ATT&CK ICS T0862, T0826, T0828 CIE 9, 10, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TN-6	**Supplier app failure stops trains** Crew, dispatch and maintenance systems from suppliers carry speed restrictions, work zones and safety notices to drivers and conductors. When the supplier is attacked, staff cannot run trains safely, so the operator stops the network even though signalling is untouched. *Case: DSB trains and Supeo, 2022.*	**Safety-critical operating information must reach crews by a fallback path when a supplier's system is lost.** **1** Identify supplier systems that carry safety information, and treat them as critical in contracts and testing. **2** Keep a fallback channel, such as printed notices or radio, for speed restrictions and work zones. **3** Hold current copies of rosters and restrictions so services can restart without the supplier.	STRIDE D CAPEC – CWE CWE-1357 ATT&CK ICS T0862, T0828 CIE 9, 7, 10 STANDARDS CLC/TS 50701
BKS-TN-5	**Vessel traffic trusts what ships report †** Vessel traffic services and ships rely on the Automatic Identification System, which carries unauthenticated position and identity reports. False tracks can hide a ship, invent one, or show vessels where they are not, so traffic is closed, routed wrongly or put at risk of collision.	**Traffic decisions must not rest on unauthenticated reports alone.** **1** Fuse AIS with radar and other sensors, and alarm when a reported track has no radar match. **2** Flag tracks with impossible movements, duplicate identities or sudden jumps for operator review. **3** Train operators to treat AIS as a claim, and give them procedures for when it cannot be trusted.	STRIDE S, T CAPEC CAPEC-194 CWE CWE-290, CWE-1293 ATT&CK ICS T0832 CIE 2, 6
BKS-TN-4	**Navigation data sends traffic astray** Navigation apps, ride-hailing platforms and live traffic feeds steer thousands of vehicles at once. False congestion, false closures or mass bookings can send traffic into one street, block emergency routes or empty the roads an evacuation needs. *Case: Yandex Taxi gridlock, Moscow, 2022.*	**Platforms that steer traffic must detect and limit coordinated, implausible demand or data.** **1** Rate-limit bookings and route changes that converge on one place, and alarm on sudden concentrations. **2** Authenticate official closure and incident data feeds, and cross-check them against observed traffic. **3** Agree with road authorities how routing is constrained during emergencies and evacuations.	STRIDE T, D CAPEC CAPEC-153 CWE CWE-807 ATT&CK ICS – CIE 6, 7
BKS-TN-3	**Station boards speak for the attacker †** Passenger information displays, apps and public address are fed from central systems with weak access control. False delays, cancellations or evacuation messages send crowds the wrong way, overload stations and staff, and make passengers doubt real instructions. *Case: Iran railway, 2021.*	**Only authorised staff can publish to passengers, and emergency messages need a protected path.** **1** Restrict who and what can publish, and require approval for messages beyond routine updates. **2** Give emergency and evacuation messages a separate, authenticated path that staff can verify. **3** Let station staff override or blank displays locally when content cannot be trusted.	STRIDE S, T CAPEC CAPEC-148 CWE CWE-862 ATT&CK ICS T0832 CIE 3, 6

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TN-2	**Ticketing and gates fail badly** Ticket gates, validators and the back-office systems that settle fares depend on central services. When those fail, gates either lock passengers in or out or are left open, refunds and passes stop, and revenue and passenger data are exposed. *Case: Transport for London, 2024.*	**Gates must fail safely for people, and travel must continue when back-office systems are lost.** 1 Make gates fail open for evacuation, with local staff control, whatever the back office does. 2 Let validators keep working offline for a set period, with fares settled later. 3 Separate ticketing back offices from operational networks, and protect customer data in them.	STRIDE D, I CAPEC – CWE CWE-636 ATT&CK ICS T0828 CIE 10, 3

IX · INTERDEPENDENCIES

THE ESTATE · BKS-IX-A TO BKS-IX-2 · https://ostering.com/taxonomies/critical-infrastructure/interdependencies/

Where one service's failure becomes another's, and the dependencies nobody wrote down.

BKS-IX-A No power, then no water †
BKS-IX-K Telecoms die when batteries do †
BKS-IX-Q Gas and power fail together †
BKS-IX-J Generators need fuel that needs power †
BKS-IX-10 Treatment chemicals run out †
BKS-IX-9 Many sectors, one cloud
BKS-IX-8 Payment fails, food and fuel stop
BKS-IX-7 The cascade crosses borders
BKS-IX-6 Mutual aid assumes neighbours are fine
BKS-IX-5 Restoration waits on everyone else
BKS-IX-4 Staff cannot get to work
BKS-IX-3 Cooling depends on water
BKS-IX-2 Shared sites, shared fate

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-IX-A	**No power, then no water †** Water pumping and treatment depend on the grid, and standby generators cover hours, not days. A long outage drops pressure, lets contamination into pipes and stops sewage pumping, turning a power attack into a public health event.	**Water service is designed to stay safe through a power outage as long as a deliberate one could last.** **1** Size standby power and fuel storage for priority pumping and treatment against a multi-day outage. **2** Plan for loss of pressure: isolation zones, boil-water procedures and safe restart with flushing and testing. **3** Ask the electricity operator to treat key water sites as priority loads in restoration plans.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 7, 10, 1
BKS-IX-K	**Telecoms die when batteries do †** Mobile masts and exchanges run on batteries that last a few hours. In a long outage, SCADA telemetry, alarm diallers, field crews' phones and emergency calls fail together, just when operators most need them.	**Communications needed to run and restore essential services last longer than the outages they must survive.** **1** Identify which control, alarm and crew communications ride on public networks, and their backup duration. **2** Provide independent communications for control and crews, such as private radio or satellite, with their own power. **3** Agree priority restoration and portable generation for the telecom sites your control traffic depends on.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826, T1695 CIE 7, 10
BKS-IX-Q	**Gas and power fail together †** Gas-fired plants make electricity, while gas compressors, boilers and heating controls need electricity. An attack on either in winter can take down both, leaving homes without heat or power.	**Gas and power operators plan for their joint failure, not each in isolation.** **1** Map which gas facilities need grid power and which power plants need gas, and back them for each other. **2** Run joint exercises between gas and electricity operators that start from both systems failing. **3** Prepare winter priority plans for heat to vulnerable people that do not need both networks.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 7, 1
BKS-IX-J	**Generators need fuel that needs power †** Standby generators at hospitals, water works and telecom sites need refuelling, and fuel delivery needs depots, pumps, payment and communications that depend on power. In a long outage the backups run dry in a circle of dependencies. *Case: Colonial Pipeline, 2021.*	**Backup power arrangements are tested against the failure of the systems that resupply them.** **1** Hold enough fuel on site for the longest outage you plan for, and rotate it. **2** Contract priority refuelling that works without card payment or phone ordering. **3** Trace each backup's resupply chain and remove dependencies on the same grid it is backing up.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7, 10

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-IX-10	**Treatment chemicals run out †** Water treatment needs a steady supply of chemicals for disinfection and coagulation, delivered from a few manufacturers by road. Disrupting producers or logistics leaves plants unable to treat water safely within days.	**Chemical supply for water treatment is protected and buffered like the treatment works itself.** 1 Keep enough chemical stock on site for a realistic supply disruption. 2 Qualify more than one supplier and delivery route for each critical chemical. 3 Plan how treatment continues, and how the public is warned, if one chemical becomes unavailable.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7, 9
BKS-IX-9	**Many sectors, one cloud** Operators in different sectors rely, often unknowingly, on the same cloud region, DNS provider, identity service or certificate authority. One outage or compromise there stops many essential services at once, beyond any one operator's view.	**Each operator knows its third-party digital dependencies and can run critical functions without any single one.** 1 List the cloud regions, DNS, identity and certificate services each critical function needs, including vendors' dependencies. 2 Keep critical control functions working locally when a cloud service is unreachable. 3 Share dependency maps with the sector body so common points of failure across operators become visible.	STRIDE D CAPEC – CWE CWE-1357 ATT&CK ICS T0826 CIE 7, 8
BKS-IX-8	**Payment fails, food and fuel stop** Buying food, fuel and medicines depends on card networks, banks and mobile payments. When payment fails, essential goods stop moving even though supply and stores are intact, and little cash is held anywhere.	**Essential retail can keep selling when electronic payment is unavailable.** 1 Plan an offline payment mode with limits and deferred settlement. 2 Agree how cash and vouchers can be used in an extended outage. 3 Test the fallback at a few stores each year, including staff who have never handled cash.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7, 10
BKS-IX-7	**The cascade crosses borders** Interconnectors, pipelines, undersea cables and shared operators tie countries together. An attack on one country's infrastructure, or on a link between them, spreads to neighbours who neither saw it coming nor control the response. *Case: Balticconnector, 2023.*	**Cross-border dependencies are mapped and exercised with the operators on both sides.** 1 Map links to neighbouring systems and what happens on each side if they trip or are cut. 2 Exercise joint incidents with neighbouring operators and agree how to share information quickly. 3 Design the ability to island your system safely if a neighbour's fails.	STRIDE D CAPEC CAPEC-607 CWE – ATT&CK ICS T0826 CIE 7, 10
BKS-IX-6	**Mutual aid assumes neighbours are fine** Utilities and retailers rely on help from neighbours, contractors and vendors during incidents. A coordinated attack hits everyone at once, so the crews, spare parts and experts that plans count on are busy with their own outages.	**Response plans hold up when every organisation you would ask for help is also affected.** 1 Test your plan assuming no mutual aid and no vendor support for the first several days. 2 Hold key spares and recovery skills in house rather than relying on the same pool as everyone else. 3 Agree with the sector body in advance how scarce help will be prioritised.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 10, 7, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-IX-5	**Restoration waits on everyone else** Restoring power needs telecoms and fuel, restoring telecoms needs power, and restoring water needs both. Plans written per sector each assume the others come back first, so a broad outage stalls in deadlock.	**Restoration plans are sequenced across sectors, starting from all of them being down.** 1 Write restoration sequences that start with no grid, no public telecoms and no card payment. 2 Agree cross-sector priorities and the communication channels used during restoration. 3 Rehearse the sequence jointly with the other sectors it depends on.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7, 10
BKS-IX-4	**Staff cannot get to work** Running essential services needs people on site. If fuel, public transport, schools or phones fail, operators, engineers and drivers cannot get to work or be called in, and the systems that remain cannot be run.	**Staffing plans cover the disruptions an attack would cause to staff's own lives.** 1 Identify roles that must be on site and plan transport, fuel and accommodation for them in an emergency. 2 Keep call-out lists and procedures that work without mobile phones. 3 Cross-train staff so fewer people are irreplaceable.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 12, 10
BKS-IX-3	**Cooling depends on water** Data centres, power plants, hospitals and industrial processes need water for cooling. A water outage forces them to shut down, carrying an attack on a water utility into computing, power and health.	**Cooling for critical facilities has a source that does not depend on the public water supply alone.** 1 Identify which critical systems need mains water for cooling and how long they last without it. 2 Provide on-site storage or alternative cooling for the most critical loads. 3 Tell the water utility which customers are critical so restoration plans include them.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7
BKS-IX-2	**Shared sites, shared fate** Telecom masts sit on water towers, cables share ducts and bridges, and control rooms for several services share a building. One cyber or physical event at a shared site takes out several services that each believed they were independent.	**Services that must be independent are shown to be independent on the ground, not only on paper.** 1 Map physical routes and sites for your critical links and compare them with your backups. 2 Route backup links and control centres through separate sites and paths. 3 Ask co-located parties for their incident contacts and plans.	STRIDE D CAPEC CAPEC-607 CWE – ATT&CK ICS – CIE 7, 4

MP · MONEY AND PAYMENTS

THE ESTATE · BKS-MP-A TO BKS-MP-2 · https://ostering.com/taxonomies/critical-infrastructure/money-and-payments/

How money moves: the routing data, messages, ledgers, settlement and fallbacks that let people pay for food, fuel and medicines and get paid.

BKS-MP-A Routing reference data poisoned at source
BKS-MP-K Ledgers nobody can reconcile
BKS-MP-Q One settlement system for a country
BKS-MP-J No stand-in when authorisation fails
BKS-MP-10 Bulk payment files changed in transit
BKS-MP-9 Directory updates loaded blindly
BKS-MP-8 Key accounts quietly remapped
BKS-MP-7 Messages altered at the SWIFT interface
BKS-MP-6 Payee checks turned against payers
BKS-MP-5 Sanctions lists corrupted
BKS-MP-4 Format translation changes the payment
BKS-MP-3 No cash to fall back on
BKS-MP-2 One route to the outside world

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-MP-A	**Routing reference data poisoned at source** Banks route payments with shared reference data: the IBAN-to-BIC mapping, the BIC directory and national clearing tables, published by a few sources. Corrupt the source or its distribution, and every bank that loads the update misroutes or rejects payments at once, and nobody can quickly prove which payments went where.	**Shared routing data must be authenticated, checked for plausibility and reversible before any bank acts on it.** **1** Verify the publisher's signature on every directory file, and refuse files that fail or arrive outside the expected schedule. **2** Compare each update with the previous version and hold large changes, or changes to critical institutions, for review. **3** Keep the last known-good version ready to restore within minutes, and record which version routed each payment.	STRIDE T, D CAPEC CAPEC-194 CWE CWE-353, CWE-347 ATT&CK ICS – CIE 1, 9, 10
BKS-MP-K	**Ledgers nobody can reconcile** An adversary alters or destroys account balances and transaction records inside a bank or payment system. When positions no longer reconcile, the institution cannot say who owns what, payments stop, and the doubt spreads to every institution that settles with it. *Case: Bank Sepah, Iran, 2025.*	**Records of value must be provably intact, and rebuildable from a copy the attacker could not reach.** **1** Chain or sign ledger records so an altered entry breaks verification, and check the chain continuously. **2** Reconcile against counterparties and the settlement system often during the day, not only at day end. **3** Keep immutable, offline copies of end-of-day positions, held by a separate party, as the basis for rebuilding.	STRIDE T, R, D CAPEC – CWE CWE-353, CWE-1293 ATT&CK ICS – CIE 1, 10, 2
BKS-MP-Q	**One settlement system for a country** A country's interbank payments settle through one real-time gross settlement system, one clearing house or a few central counterparties, and many firms share the same providers. If one of them is disabled, payments, salaries and trades stop for everyone, while contingency plans assume service returns the same day. *Case: ICBC Financial Services, 2023; ION Trading, 2023.*	**Every payment system a country cannot do without must keep settling, at reduced scope, when its main platform is lost.** **1** Run a tested contingency platform on separate technology and staff, able to settle priority payments for days. **2** Define in advance which payments go first: wages, benefits, fuel, food and utility settlement. **3** Rehearse a full switchover with participants at least yearly, including manual and file-based settlement.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 10, 7, 1
BKS-MP-J	**No stand-in when authorisation fails** Card payments at tills, pumps and pharmacies need a live answer from the acquirer, processor or card scheme. When that path is down, terminals refuse every card, and shops that hold little cash cannot sell food, fuel or medicines, even with the goods on the shelf. *Case: Kaseya VSA and Coop Sweden, 2021.*	**Essential purchases must still be possible when online authorisation is lost.** **1** Enable offline or stand-in authorisation with limits for essential merchants, and test it regularly. **2** Give terminals a second route to a different processor where the scheme allows. **3** Keep cash handling, float and procedures ready at essential outlets, with staff who know them.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 10, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-MP-10	**Bulk payment files changed in transit** Salaries, pensions and benefits leave as bulk files from payroll bureaus and government agencies to banks. A file altered between approval and submission pays the wrong people or nobody, on the day households depend on it, and the error is found only when complaints arrive.	**A bulk payment file must be provably the one that was approved, and checked before release.** 1 Sign bulk files at the point of approval and verify the signature at the bank before processing. 2 Check each file against the previous run for unusual changes in totals, counts and payees. 3 Agree a fallback with the bank to repeat the last good run when a file cannot be trusted.	STRIDE T CAPEC CAPEC-153 CWE CWE-353, CWE-924 ATT&CK ICS – CIE 2, 10
BKS-MP-9	**Directory updates loaded blindly** Banks load reference data updates into payment engines automatically, from a vendor feed or a shared folder, with no check on who changed what. Whoever reaches the feed, the folder or the loading job can change routing for the whole bank without touching the payment systems themselves.	**Changes to reference data are changes to production and need the same control.** 1 Load reference data only from an authenticated source, through a controlled job with its own credentials. 2 Show the differences from the last version to a named approver before the update goes live. 3 Log every reference data change with source, approver and time, and alert on loads outside the schedule.	STRIDE T, E CAPEC CAPEC-75 CWE CWE-15, CWE-732 ATT&CK ICS – CIE 3, 9
BKS-MP-8	**Key accounts quietly remapped** A small change to one entry in routing or payee data redirects payments for a single target: a government agency, a utility's settlement account or a payroll bureau. Nothing fails, so nothing alarms, and money flows to the wrong place until a counterparty asks where it is.	**The accounts that essential services depend on must be watched more closely than the rest.** 1 Keep a protected list of critical accounts and routing entries, and alert on any change to them. 2 Confirm changes to critical payee details out of band with the account holder. 3 Reconcile expected incoming payments for critical institutions daily and investigate gaps at once.	STRIDE T, S CAPEC – CWE CWE-1293 ATT&CK ICS – CIE 8, 6
BKS-MP-7	**Messages altered at the SWIFT interface** Between core banking and the SWIFT interface sit middleware, file transfers and operator workstations. An adversary there can create, change, delete or hide payment messages and their confirmations, as in the Bangladesh Bank theft, and can use the same position to disrupt rather than steal. *Case: Bangladesh Bank, 2016; Mexico SPEI connections, 2018.*	**A payment message must be checkable end to end against the system that created it, wherever it passes.** 1 Reconcile messages sent through SWIFT against core banking records independently and in near real time. 2 Protect the messaging zone as SWIFT's Customer Security Controls Framework requires, with separate credentials and monitoring. 3 Send confirmations and statements to a channel the messaging operators cannot alter.	STRIDE T, R, S CAPEC CAPEC-94 CWE CWE-924, CWE-353 ATT&CK ICS – CIE 3, 6

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-MP-6	**Payee checks turned against payers** Name checks such as Verification of Payee and Confirmation of Payee answer from data held by the payee's bank or a shared service. Corrupt that data and the check approves fraudulent payees or flags genuine ones, so money goes astray or ordinary payments stall while people phone to confirm.	**A payee check must fail safe and show when its own answers cannot be trusted.** 1 Protect the account-name data behind the check as critical data, with change control and monitoring. 2 Watch match and mismatch rates across the service and alert on sudden shifts. 3 Define how payers proceed when the service is unavailable or unreliable, without abandoning the check.	STRIDE T, S CAPEC – CWE CWE-807 ATT&CK ICS – CIE 2, 6
BKS-MP-5	**Sanctions lists corrupted** Payment screening relies on sanctions and watch lists loaded from authorities and vendors. A poisoned list blocks legitimate payments for whole sectors or lets sanctioned parties through, and banks cannot tell which until regulators or customers point it out.	**Screening lists are critical inputs and must be authenticated and checked like code.** 1 Load lists only from authenticated sources and compare each update with the official publication. 2 Alert when an update adds or removes far more entries than usual. 3 Keep the previous list ready to restore, and record which list version screened each payment.	STRIDE T CAPEC CAPEC-194 CWE CWE-353 ATT&CK ICS – CIE 9, 2
BKS-MP-4	**Format translation changes the payment** Many banks translate between the older SWIFT MT formats and ISO 20022 messages. Each translation layer is a place where fields are truncated, mapped wrongly or altered, and one change there affects every payment that passes through it.	**Every translation of a payment message must be checkable against the original.** 1 Keep the original message alongside the translated one and compare key fields automatically. 2 Test translators against hostile and malformed messages, not only valid samples. 3 Control changes to mapping rules as strictly as changes to payment code.	STRIDE T CAPEC CAPEC-277 CWE CWE-1287 ATT&CK ICS – CIE 4, 2
BKS-MP-3	**No cash to fall back on** When cards and transfers fail, cash is the fallback, but ATMs, cash centres and cash-in-transit routes run on the same networks, power and fuel. Where cash use has fallen, few shops accept it and households hold little, so a payments outage becomes an outage of everything.	**A minimum cash system must be kept able to work when digital payments do not.** 1 Keep cash distribution able to run on its own power, communications and fuel for days. 2 Agree with authorities which outlets must accept cash in a payments outage, and test it. 3 Plan ATM and branch operation on reduced connectivity, with limits rather than shutdown.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 10, 7

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-MP-2	**One route to the outside world** Cross-border payments for a country or region pass through a few correspondent banks and messaging connections. Disrupting them cuts importers off from suppliers of food, fuel and medicines just when they are needed, and alternative routes take weeks to arrange.	**Payment routes for essential imports must have a tested alternative before it is needed.** 1 Map which correspondents and connections carry payments for essential imports. 2 Hold active, tested relationships with at least one alternative correspondent and route. 3 Agree with authorities how priority import payments move if normal routes fail.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 7, 10

TRUMPS · STRUCTURAL HAZARDS

BOTH DECKS · BKS-TR-1 TO BKS-TR-10 · https://ostering.com/taxonomies/critical-infrastructure/structural-hazards/

Ten structural hazards of essential services as a whole. Both decks carry them, ranked 1 (highest) to 10.

BKS-TR-1 One console, a thousand sites †
BKS-TR-2 Vendor monoculture
BKS-TR-3 The adversary has time
BKS-TR-4 Every feature is dual-use †
BKS-TR-5 Safety cases assume accidents †
BKS-TR-6 Everything runs on power and comms †
BKS-TR-7 IT and OT share a fate
BKS-TR-8 The plant outlives its software
BKS-TR-9 Nobody can run it by hand †
BKS-TR-10 Planned for crime, not war

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TR-1	**One console, a thousand sites †** Central platforms let one operator or vendor change settings across every site at once. That is their purpose, and it means a single compromised account or session can do to a thousand stores, pump stations or chargers what used to take a thousand intrusions. *Case: Supermarket refrigeration attacks, 2026; Kaseya VSA and Coop Sweden, 2021.*	**The reach of any account, session or command is limited, and fleet-wide actions need more than one person.** **1** Limit how many sites a command or account can affect, and require a second approval above that limit. **2** Let each site reject commands outside its safe envelope, whatever their source. **3** Alert in real time on bulk changes and on changes at unusual hours.	STRIDE T, E CAPEC CAPEC-122 CWE CWE-1220 ATT&CK ICS T0836, T0859 CIE 1, 4, 2
BKS-TR-2	**Vendor monoculture** Whole sectors buy the same controllers, firmware and management software from a handful of vendors. One flaw, one stolen vendor key or one compromised update reaches every operator at once, and they all need the same scarce vendor to recover. *Case: Danish energy sector, 2023; Viasat KA-SAT modems, 2022.*	**Critical functions do not all fail from one product, one vendor or one key.** **1** Know which vendors and product versions your critical functions depend on, and which other operators share them. **2** Where consequence is high, use diverse products or an independent safety layer from another supplier. **3** Agree in contracts how the vendor will support many customers in a simultaneous incident.	STRIDE D CAPEC CAPEC-186 CWE CWE-1357, CWE-1395 ATT&CK ICS T0862 CIE 9, 8, 7
BKS-TR-3	**The adversary has time** A state adversary can wait years inside networks, learning the process and choosing the moment. Defences built to stop quick criminal attacks, and detection tuned for noisy intrusions, miss quiet access that does nothing until it is ordered to. *Case: Volt Typhoon pre-positioning, 2024 advisory.*	**The design assumes access may already exist and limits what dormant access can do when activated.** **1** Hunt for persistent access in edge devices, accounts and engineering systems, not only for malware. **2** Require fresh authorisation for dangerous actions so stolen standing access is not enough. **3** Keep logs long enough to look back over years, stored where an intruder cannot delete them.	STRIDE S, E CAPEC – CWE CWE-778 ATT&CK ICS T0859, T0883 CIE 6, 5
BKS-TR-4	**Every feature is dual-use †** Defrost cycles, flushing, test modes, firmware update modes, remote shutdown and bulk configuration exist for good reasons. Each one is also a ready-made attack: the adversary needs no exploit, only the authority to use the feature at the wrong time. *Case: Supermarket refrigeration attacks, 2026; Ukraine grid attack, 2015.*	**Features that can cause harm are bounded by physics and design, not only by who is allowed to press the button.** **1** List the built-in functions that could cause damage if used maliciously, and their worst case. **2** Bound those functions with interlocks, duration limits and local conditions that cannot be overridden remotely. **3** Remove or disable functions the operation does not need.	STRIDE T, E CAPEC CAPEC-554 CWE CWE-749, CWE-912 ATT&CK ICS T0831, T0858, T0800 CIE 4, 2, 1

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TR-5	**Safety cases assume accidents †** Safety engineering assumes faults are random and independent. An adversary is neither: they defeat the alarm, the trip and the backup together, and choose the moment when people are exposed. *Case: TRITON safety system attack, 2017.*	**Safety cases consider deliberate, coordinated action against the safety functions themselves.** **1** Review hazard analyses asking what happens if an intelligent adversary triggers several failures at once. **2** Keep the last line of protection mechanical or hard-wired where the consequence is loss of life. **3** Separate safety systems from control systems so one compromise cannot reach both.	STRIDE T, D CAPEC – CWE CWE-636 ATT&CK ICS T0880, T0837 CIE 1, 2, 5
BKS-TR-6	**Everything runs on power and comms †** Every essential service needs electricity and communications, and most have only hours of backup for either. An attack on power or telecoms is an attack on water, food, fuel and health care too. *Case: Viasat KA-SAT modems, 2022.*	**Each critical function's dependence on power and communications is known, backed up and tested for long outages.** **1** Record how long each critical function lasts without grid power and without public telecoms. **2** Back the most critical functions with independent power and communications. **3** Test backups for the duration a deliberate outage could last, not only for minutes.	STRIDE D CAPEC – CWE – ATT&CK ICS T0826 CIE 7, 10
BKS-TR-7	**IT and OT share a fate** Plants that never connected their controls to the internet still depend on billing, scheduling, directories and email. When corporate IT falls, operators often shut the physical process down too, because they cannot see, bill or trust it. *Case: Colonial Pipeline, 2021; NotPetya, 2017; JBS meat plants, 2021.*	**Physical operations can run safely for a planned time with corporate IT unavailable.** **1** List which IT services operations need, and plan how to run without each one. **2** Keep separate directories and accounts for operational systems. **3** Exercise running operations for days with corporate IT disconnected.	STRIDE D CAPEC – CWE – ATT&CK ICS T0828, T0826 CIE 3, 10, 7
BKS-TR-8	**The plant outlives its software** Controllers, drives and substations are built to run for twenty to forty years, far longer than their software is supported. Known flaws stay in service for decades because patching means downtime, recertification or replacement. *Case: Ukraine grid attack, 2015.*	**Systems are designed to stay defensible after their vendor stops supporting them.** **1** Plan lifecycle and replacement funding for control equipment from the start. **2** Put compensating controls around unsupported devices: isolation, allow-listing and monitoring. **3** Prefer products whose firmware can be updated without replacing hardware.	STRIDE T, E CAPEC CAPEC-682 CWE CWE-1329, CWE-1277, CWE-1104 ATT&CK ICS T0819, T0866 CIE 8, 5
BKS-TR-9	**Nobody can run it by hand †** Automation has replaced the people, procedures and equipment needed to run the process manually. When control systems are lost or cannot be trusted, there is no one left who knows how, and no gauges or valves to do it with. *Case: Norsk Hydro, 2019; Ukraine grid attack, 2015.*	**Critical functions can be run manually for long enough to recover, by people who have practised it.** **1** Keep local instruments and manual controls for critical functions, and maintain them. **2** Write manual operating procedures and practise them on a schedule. **3** Keep experienced staff involved in training, and record what they know.	STRIDE D CAPEC – CWE – ATT&CK ICS T0827, T0829 CIE 10, 12

ID	THREAT	MITIGATION PRINCIPLE AND DESIGN MEASURES	MAPPINGS
BKS-TR-10	**Planned for crime, not war** Incident plans, insurance and contracts assume criminals after money: pay or restore, and claim on the policy. A state adversary is after effect, won't negotiate, may strike many operators at once, and insurers may refuse payment as an act of war. *Case: NotPetya, 2017.*	**Plans are tested against an adversary who wants disruption and is not after money.** 1 Add scenarios where no ransom is possible and several sectors are hit at once. 2 Check whether insurance and contracts exclude state or war-like attacks, and plan for that gap. 3 Agree in advance with authorities who decides, and how, when attribution is uncertain.	STRIDE D CAPEC – CWE – ATT&CK ICS – CIE 12, 10

Public cases and sources

Each case was checked against the sources listed, and attribution is given only where an official body made it or a group claimed it.

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
Supermarket refrigeration attacks, 2026	Overnight on 11 to 12 October 2026 attackers forced the remote-managed refrigeration controllers of hundreds of French supermarkets into defrost, heating cabinets to as much as 50C; stock was destroyed and some equipment caught fire. CERT-FR told operators to disconnect the controllers or tightly filter access to them. A second wave on 2 November hit supermarkets and food businesses in Sweden, Belgium, Ireland, Luxembourg, Estonia and Italy, and five Danish companies, where the attacks were stopped quickly. Danfoss confirmed its products were involved, and France's cyber agency judged the campaign probably still under way. *The Hacker News: attackers heat French supermarket fridges* *BleepingComputer: cyberattack shuts down refrigerators at French supermarkets* *DR: what we know about the attacks on European supermarkets* *Today.it: attacks on refrigeration in Italy, ACN alert*	Unattributed at time of writing; Paris prosecutor's investigation open	BKS-RM-A, BKS-RM-K, BKS-SC-A, BKS-PE-10, BKS-ST-Q, BKS-ST-J, BKS-ST-9, BKS-RD-5, BKS-AD-J, BKS-FD-8, BKS-FM-A, BKS-FM-K, BKS-FM-Q, BKS-FM-9, BKS-FM-5, BKS-FM-4, BKS-FM-2, BKS-RA-A, BKS-TT-2, BKS-TR-1, BKS-TR-4
Leipzig/Halle airport drone, 2026	On the night of 4 to 5 August 2026 a drone carrying explosives was found at Leipzig/Halle airport near a Ukrainian cargo aircraft and was made safe by police; on 1 September the German government said it held Russia responsible and closed a Russian consulate. *Euronews: Russia behind drone incident at Leipzig airport, Berlin says* *OPB: Germany blames Russia for attempted drone attack at Leipzig airport*	Attributed by the German government (September 2026) to Russia	BKS-AS-K
Drones over Doel and Belgian airports, 2025	On the evening of 9 November 2025 drones were seen over Belgium's Doel nuclear power plant, without affecting its operation, the same evening that drones halted traffic at Liège airport; Brussels airport and several military bases had similar incursions that month. *European Pravda: unknown drones spotted over Belgian nuclear power plant* *DroneLife: drone incursions at Belgium nuclear plant*	Unattributed; Belgian intelligence services were reported to believe a foreign state, most likely Russia, was behind the series	BKS-AS-8, BKS-AS-7
Munich airport drones, 2025	On 2 and 3 October 2025 drone sightings closed Munich airport twice in less than 24 hours, diverting and cancelling flights; drones had also been reported over the nearby Erding air base. *Ukrainska Pravda: Munich airport suspends operations for second time in one day* *Business Standard: Munich Airport suspends flights again after fresh drone sightings*	Unattributed	BKS-AS-J, BKS-AS-7
Copenhagen and Oslo airport drones, 2025	On the evening of 22 September 2025 several large drones circled Copenhagen airport for hours and air traffic was suspended, with dozens of flights diverted and thousands of passengers stranded; Oslo airport also closed after sightings that night, and Danish airports saw further incursions in the following days. Denmark's prime minister called it the most serious attack on Danish critical infrastructure to date. *Euronews: flights halted after drone sightings at Copenhagen airport* *Reuters via The Star: Denmark links drones at Copenhagen airport to hybrid attacks*	Unattributed; Danish leaders said they could not rule out Russia, and Russia denied involvement	BKS-AS-J, BKS-AS-2

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
Collins Aerospace MUSE, 2025	From 19 September 2025 ransomware on Collins Aerospace's MUSE check-in and bag-drop platform disrupted Heathrow, Brussels, Berlin and other European airports, forcing manual check-in and cancellations. *Security Affairs: cyberattack on Collins Aerospace disrupted major European airports* *BleepingComputer: UK arrests suspect for RTX ransomware attack causing airport disruptions*	Criminal ransomware, confirmed by RTX; the UK National Crime Agency arrested a suspect; no state attribution	BKS-TN-7
United Natural Foods, 2025	In June 2025 a cyberattack forced United Natural Foods, the main distributor to Whole Foods and many independent grocers, to take systems offline, leaving some stores with empty shelves. *Security Affairs: UNFI cyberattack caused bare shelves*	Unattributed	BKS-LS-K
Bank Sepah, Iran, 2025	On 17 June 2025, during the Israel-Iran war, a cyberattack disrupted Iran's state-owned Bank Sepah, closing branches and stopping cards and some fuel payments; the group claiming it said it had destroyed the bank's data, and reports said damage to backups prolonged the outage. *BankInfoSecurity: pro-Israel hacking group claims to disrupt Iran's Bank Sepah* *Iran International: banking disruptions persist after cyberattacks*	Claimed by Predatory Sparrow	BKS-MP-K
Marks & Spencer and Co-op, 2025	In April 2025 attackers who had talked IT help desk staff into resetting passwords disrupted Marks & Spencer, which paused online orders for 46 days and had gaps on its food shelves; Co-op UK was hit at the same time. *Ground News: attackers duped IT help desks* *Reuters via StreetInsider: after 46-day pause M&S resumes online orders*	No official attribution; reported as linked to Scattered Spider	BKS-SC-J, BKS-RA-8, BKS-LS-K
Bremanger dam, Norway, 2025	In April 2025 an attacker reached the control system of a dam at Bremanger, Norway, and set the outflow valve to open; it ran for about four hours before staff noticed and reversed it. *BleepingComputer: pro-Russian hackers blamed for dam sabotage in Norway*	Attributed by Norway's security service (PST) to pro-Russian hackers	BKS-ST-J, BKS-ST-5, BKS-FD-8, BKS-RA-A
Transport for London, 2024	In September 2024 attackers broke into Transport for London's network; services such as Oyster refunds and photocard applications were disrupted for weeks and data in the refund system was exposed. *The Record: guilty pleas in TfL cyberattack*	Criminal; two members of the Scattered Spider group pleaded guilty in 2026	BKS-TN-2
French high-speed rail arson, 2024	On the night of 25 to 26 July 2024, hours before the Paris Olympics opened, fires were set in trackside conduits carrying fibre-optic cables for signalling and points on the Atlantic, northern and eastern high-speed lines; about half of services were cancelled and some 800,000 passengers affected, and cables had to be repaired one by one. *The Local: sabotage on French rail network before Olympics, what we know*	Unattributed; the Paris prosecutor opened an inquiry into an attack on fundamental national interests	BKS-TN-10
GNSS interference, Baltic region	Widespread GNSS jamming and spoofing has affected the Baltic region since 2022; in April 2024 Finnair suspended flights to Tartu, Estonia, for a month because aircraft could not rely on GPS approaches there. *ERR News: Finnair suspends flights to Tartu*	Estonian officials blamed Russia	BKS-AS-Q, BKS-TT-J
Volt Typhoon pre-positioning, 2024 advisory	A February 2024 joint advisory found PRC state-sponsored actors inside the IT networks of US communications, energy, transport and water organisations, holding access, in some cases for at least five years, to disrupt operational technology in a crisis or conflict. *CISA advisory AA24-038A*	Attributed by CISA, NSA and FBI to PRC state-sponsored actors	BKS-PP-A, BKS-PP-K, BKS-PP-J, BKS-PP-8, BKS-PP-5, BKS-PP-3, BKS-CC-Q, BKS-CC-3, BKS-RA-K, BKS-TR-3

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
Texas water systems, 2024	In January 2024 a group calling itself the Cyber Army of Russia Reborn claimed interference with water systems in small Texas towns; a tank in Muleshoe overflowed before staff took the system offline. *CyberScoop: Sandworm linked to Texas water facility* *Treasury sanctions leader and primary member of the Cyber Army of Russia Reborn (19 July 2024)*	Mandiant assessed links to Sandworm (APT44); the US Treasury sanctioned two of the group's members in July 2024	BKS-ST-5, BKS-AD-8
FrostyGoop, Lviv, 2024	In January 2024 malware sent Modbus commands to heating controllers of a district heating company in Lviv, Ukraine; more than 600 apartment buildings were without heating for nearly two days in sub-zero temperatures. *Dragos intelligence brief: FrostyGoop* *Axios: a malware strain threatening critical services*	Unattributed (Dragos did not attribute it)	BKS-ST-K, BKS-FD-Q
DP World Australia, 2023	In November 2023 a cyber incident led DP World Australia to cut its terminals off from the internet, halting freight at its four container terminals for about three days. *The National: DP World Australia resumes operations* *gCaptain: DP World Australia back online*	Unattributed	BKS-LS-7
Unitronics PLCs at water utilities, 2023	From November 2023 attackers defaced internet-exposed Unitronics PLCs at the Municipal Water Authority of Aliquippa and other US sites, getting in with the default password; the Aliquippa booster station was run by hand. *Industrial Cyber: US, Israeli agencies warn of IRGC activity using OT devices* *The Register: Iran-linked attacks on US water*	Attributed by CISA, FBI and partners to CyberAv3ngers, affiliated with Iran's IRGC	BKS-RM-A, BKS-ST-5, BKS-AD-8, BKS-AD-2, BKS-FD-9, BKS-RA-A
ICBC Financial Services, 2023	In November 2023 ransomware disrupted ICBC Financial Services, the US arm of the world's largest bank, which could not settle US Treasury trades for other market participants; settlement details were carried across Manhattan on a USB stick. *Computer Weekly: ransomware attack on major Chinese lender disrupts financial markets* *Security Affairs: ICBC suffered a ransomware attack*	Criminal ransomware (LockBit, as reported); no state attribution	BKS-MP-Q
Balticconnector, 2023	In October 2023 the Balticconnector gas pipeline between Finland and Estonia and nearby telecom cables were damaged; Finnish investigators found it was caused by the dragged anchor of a Hong Kong-flagged ship, and the gas link was out of service for months. *Al Jazeera: Finland says Chinese vessel's anchor caused Balticconnector damage*	Finnish authorities linked the damage to the ship Newnew Polar Bear; intent not established	BKS-IX-7
Polish rail radio stops, 2023	In August 2023 about 20 trains in Poland were brought to an emergency stop by Radio-Stop signals broadcast on the rail radio network, which does not authenticate them. *Euronews: is Russian sabotage behind train incidents in Poland* *Hackaday: Polish railways fall victim to cheap radio attack*	Unattributed; two people were arrested in Poland	BKS-TT-Q
Port of Nagoya, 2023	In July 2023 ransomware stopped the terminal system at the Port of Nagoya, Japan's busiest port by cargo volume, halting container loading and unloading for about two days. *Dark Reading: ransomware halts operations at Port of Nagoya* *Maritime Executive: ransomware stops container operations at Nagoya*	Claimed by the LockBit ransomware group	BKS-LS-7
Danish energy sector, 2023	In May 2023 attackers compromised 22 Danish energy companies in coordinated waves through flaws in the firewalls that protected them, the largest such attack Denmark had seen. *SecurityWeek: 22 energy firms hacked in Denmark* *SecurityWeek: Russian hackers likely not involved*	Unattributed; SektorCERT saw indicators linked to Sandworm in at least one attack, which other researchers later questioned	BKS-RM-Q, BKS-PP-K, BKS-ST-Q, BKS-RA-K, BKS-TR-2

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
ION Trading, 2023	In early 2023 ransomware hit ION, whose software many firms use for derivatives trade processing and clearing, disrupting trading and reporting in the City of London. *Computer Weekly: ransomware attack on major Chinese lender disrupts financial markets* *ESRB: systemic cyber risk (2024 presentation)*	Criminal ransomware (LockBit); no state attribution	BKS-MP-Q
DSB trains and Supeo, 2022	On 29 October 2022 an attack on Supeo, a supplier whose app gives Danish State Railways' crews speed restrictions and safety notices, took its servers down; DSB stopped its trains because they could not be run safely without it. *Bitdefender: Denmark's train network frozen due to cyberattack on subcontractor* *Security Affairs: a cyberattack blocked the trains in Denmark*	Unattributed; DSB said the supplier reported criminal hackers	BKS-TN-6
Yandex Taxi gridlock, Moscow, 2022	On 1 September 2022 attackers sent bulk orders through the Yandex Taxi app so that dozens of cabs converged on one address in Moscow, jamming Kutuzovsky Prospekt for close to an hour. *The Register: Moscow taxi jam*	Unattributed	BKS-TN-4
Khuzestan steel plant, 2022	In June 2022 a group claimed a cyberattack that caused a fire at an Iranian steel plant and published video of molten metal spilling; the company halted production. *CCDCOE Cyber Law Toolkit: Predatory Sparrow operation against Iranian steel maker*	Claimed by Predatory Sparrow	BKS-AD-K
Industroyer2 attempt, 2022	In April 2022 attackers planted Industroyer2 and disk wipers to switch off high-voltage substations of a Ukrainian energy company; CERT-UA and ESET stopped it before it ran. *ESET WeLiveSecurity: Industroyer2* *TechCrunch: Ukraine disrupts attempt to take down energy provider*	Attributed by CERT-UA to Sandworm	BKS-RD-10, BKS-FD-K
Viasat KA-SAT modems, 2022	As Russia invaded Ukraine on 24 February 2022, the AcidRain wiper bricked tens of thousands of KA-SAT satellite modems across Europe; about 5,800 Enercon wind turbines in Germany lost remote monitoring and control, and many modems had to be replaced. *DatacenterDynamics: satellite outage impacts more than 5,000 wind turbines* *energate: Enercon, thousands of wind turbines need new hardware*	Attributed by the EU, UK and US governments (May 2022) to Russia	BKS-ST-Q, BKS-RD-J, BKS-FM-10, BKS-TT-A, BKS-TT-K, BKS-TR-2, BKS-TR-6
Iran fuel stations, 2021 and 2023	In October 2021 attackers disabled the fuel card system at about 4,300 Iranian fuel stations; in December 2023 a similar attack disrupted around 70 per cent of them. *Al Jazeera: Iran says cyberattack disrupts petrol stations* *Security Affairs: Predatory Sparrow disrupted 70% of Iran's fuel stations*	Claimed by Predatory Sparrow; Iran blamed Israel	BKS-AD-2, BKS-LS-10
Kaseya VSA and Coop Sweden, 2021	In July 2021 ransomware was pushed through Kaseya VSA, a remote management tool used by managed service providers; Coop Sweden's tills stopped working and it closed about 800 stores for several days. *The Record: Coop closes 800 stores after Kaseya ransomware attack* *Truesec: Coop restored within 6 days*	Attributed by the FBI to the REvil ransomware group	BKS-SC-A, BKS-SC-Q, BKS-RD-5, BKS-FM-K, BKS-LS-9, BKS-MP-J, BKS-TR-1
Iran railway, 2021	On 9 July 2021 display boards at stations across Iran showed false messages of long delays and cancellations because of a cyberattack, urging passengers to call a number that belonged to the Supreme Leader's office. *Dawn: hackers disrupt Iran's rail service with fake delay messages* *Wikipedia: Predatory Sparrow*	Claimed by Predatory Sparrow	BKS-TN-3

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
JBS meat plants, 2021	In June 2021 ransomware halted JBS meat processing plants in the US, Canada and Australia for several days; the company paid a ransom of about 11 million dollars. *NPR: REvil behind JBS cyberattack, FBI says*	Attributed by the FBI to the REvil ransomware group	BKS-TR-7
Colonial Pipeline, 2021	In May 2021 ransomware on Colonial Pipeline's business IT led the company to shut down the pipeline, which carries about 45 per cent of the US East Coast's fuel, for five days; shortages and panic buying followed. *CBS News: Colonial Pipeline paid ransom* *The Chemical Engineer: Major US pipeline restarts*	Attributed by the FBI to the DarkSide ransomware group	BKS-AD-9, BKS-IX-J, BKS-TR-7
SolarWinds Orion, 2020	In 2020 a trojanised update to SolarWinds Orion network management software was downloaded by up to 18,000 customers, giving the attackers a way into selected government and company networks. *Security Affairs: SolarWinds confirms 18,000 customers may have been impacted* *Janes: UK and US confirm Russian responsibility*	Attributed by the US and UK governments (April 2021) to Russia's SVR	BKS-SC-K
Norsk Hydro, 2019	In March 2019 LockerGoga ransomware hit the aluminium maker Norsk Hydro; plants switched to manual operation while systems were rebuilt. *Fortune: Norsk Hydro cyber attack*	Criminal ransomware; no state attribution	BKS-CC-7, BKS-TR-9
Mexico SPEI connections, 2018	In April 2018 attackers compromised software that five Mexican financial institutions used to connect to the central bank's SPEI payment system and sent hundreds of false transfer orders worth about 300 million pesos; dozens of institutions moved to a contingency connection. *Finextra: hackers steal millions from Mexican banks* *Expansión: cronología del hackeo al SPEI*	Unattributed	BKS-MP-7
NotPetya, 2017	In June 2017 NotPetya, destructive malware disguised as ransomware, spread from a Ukrainian accounting software update. Maersk rebuilt its network and recovered its directory from a domain controller in Ghana that had been offline during a power cut; Mondelez's insurer cited a war exclusion, a dispute settled in 2022. *Redmond: the domain controller nightmare* *The Record: Mondelez and Zurich reach settlement*	Attributed by the UK and US governments (2018) to the Russian military	BKS-RD-10, BKS-RD-9, BKS-RD-2, BKS-AD-Q, BKS-CC-Q, BKS-LS-7, BKS-TR-7, BKS-TR-10
TRITON safety system attack, 2017	In 2017 malware reprogrammed Triconex safety instrumented systems at a Saudi petrochemical plant; it was found after the safety controllers tripped and shut the plant down. *MIT Technology Review: Triton* *E&E News: The inside story of the world's most dangerous malware*	Attributed by the US Treasury (2020 sanctions) to Russia's Central Scientific Research Institute of Chemistry and Mechanics	BKS-PE-A, BKS-FD-A, BKS-TR-5
Kyiv substation attack, 2016	In December 2016 Industroyer (CrashOverride) malware, which spoke grid protocols directly and carried a denial-of-service module against protection relays, cut power at a transmission substation near Kyiv for about an hour. *ESET WeLiveSecurity: Industroyer*	Attributed by the US Department of Justice (2020 indictment) to Russia's GRU Unit 74455 (Sandworm)	BKS-PE-K, BKS-FD-K, BKS-FD-Q
Bangladesh Bank, 2016	In February 2016 attackers inside Bangladesh Bank's network used its SWIFT-connected systems to send fraudulent transfer requests worth about 951 million dollars to the Federal Reserve Bank of New York; 81 million dollars reached accounts in the Philippines. *Finextra: US charges North Korean over Bangladesh Bank hack* *RFA: US charges three North Korean spies*	Attributed by the US Department of Justice (2018 complaint, 2021 indictment) to North Korean state-sponsored hackers (Lazarus Group)	BKS-MP-7

CASE	WHAT HAPPENED	ATTRIBUTION	CITED BY
Ukraine grid attack, 2015	On 23 December 2015 attackers used three Ukrainian distribution companies' own control systems to open breakers, cutting power to about 225,000 customers. They also overwrote firmware on serial-to-Ethernet converters, wiped systems with KillDisk, tampered with backup power and flooded call centres with calls. *CISA ICS alert IR-ALERT-H-16-056-01* *MITRE ATT&CK campaign C0028*	Attributed by the US Department of Justice (2020 indictment) to Russia's GRU Unit 74455 (Sandworm)	BKS-PE-8, BKS-ST-K, BKS-RD-J, BKS-RD-10, BKS-RD-6, BKS-FD-10, BKS-CC-K, BKS-CC-7, BKS-RA-Q, BKS-RA-J, BKS-TR-4, BKS-TR-8, BKS-TR-9
DDoS on US banks, 2011 to 2013	Between late 2011 and mid-2013 a campaign of denial-of-service attacks, coming in waves most weeks, hit 46 US financial institutions over 176 days, leaving hundreds of thousands of customers unable to reach their accounts online. *US Attorney General remarks on the indictment (24 March 2016)* *BankInfoSecurity: 7 Iranians indicted for DDoS attacks against US banks*	Attributed by the US Department of Justice (2016 indictment) to seven Iranians working for companies acting for the Iranian government, including the IRGC	BKS-ST-8
Stuxnet, 2010	Malware found in 2010 changed the speed of uranium enrichment centrifuges at Natanz, Iran, while operators saw normal readings, damaging equipment over months. *Schneier on Security: More Stuxnet news* *iTnews: Stuxnet the first to attack Iran nuclear plant*	No official attribution; widely reported as a US and Israeli operation	BKS-PP-Q, BKS-PP-9, BKS-SC-8, BKS-PE-J, BKS-PE-5, BKS-PE-4, BKS-FD-7, BKS-FD-6, BKS-CC-A, BKS-CC-J, BKS-CC-2, BKS-FM-8
Łódź tram points, 2008	In January 2008 a 14-year-old in Łódź, Poland, used a modified television remote control to switch tram points by infrared; four trams derailed and passengers were injured. *Dark Reading: teenage hacker takes over Polish tram system*	A local teenager, charged before a juvenile court; no state involvement	BKS-TN-A