SECURITY DIRECTIVE (SD) PIPELINE-2021-02C

Saudi Arabia – National Cybersecurity Authority

+1 866-849-6629 | info@xonasystems.com

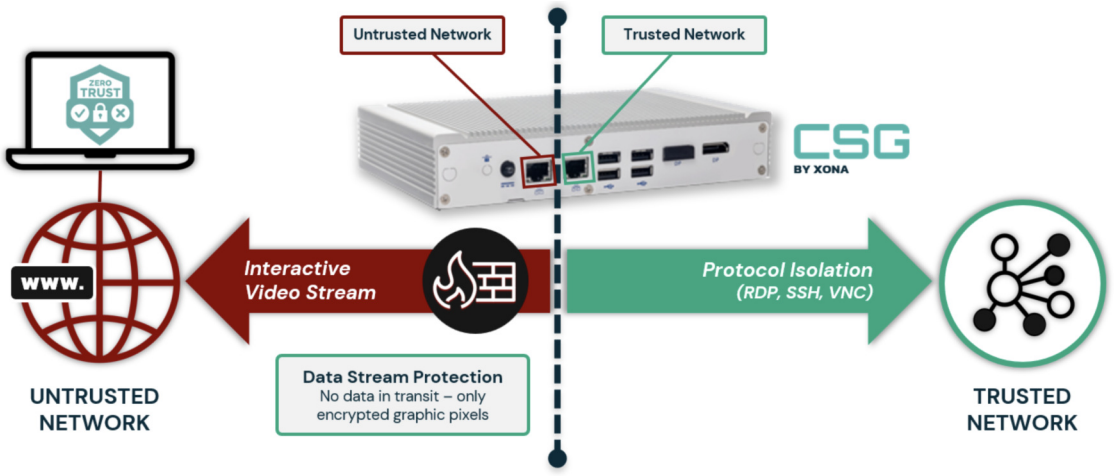
The National Cybersecurity Authority (NCA) was created to fulfill the strategic and regulatory cybersecurity needs of the Kingdom of Saudi Arabia. The NCA's Operational Technology (OT) Cybersecurity Controls (OTCC-1:2022) were developed to increase the protection of OT/ICS (Industrial Control System) environments. That includes all devices, systems, or networks used to operate and/or automate industrial processes.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

1	Cybersecurity Governance	2	Cybersecurity Defense	3	Cybersecurity Defense	4	Third-Party Cybersecurity

The controls defined in OTCC-1:2022 are for ICSs that reside in facilities that are deemed critical and owned and/or operated by organizations (e.g., ministries, authorities, establishments, and others) of the Saudi Arabia government, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures (CNIs) on behalf of the Saudi Arabia government.

XONA delivers a purpose-built, Zero-Trust based solution, that will provide your OT operators with frictionless[1] and secure user access to your OT/ICS assets. It will enable them to monitor, manage, and control those assets remotely and/or onsite.



[1] i.e., No client applications or web browser plug-ins required on operator devices – only requirement is a modern browser.

The XONA Critical Systems Gateway (CSG) is delivered as a self-contained appliance that can be used by your employees, contractors, and vendors to securely access OT/ICS assets without introducing any additional cyber- or physical risk into your OT environment. As such, it is a key piece of what Gartner refers to as a "Cyber-Physical Systems Protection Platform". [2]

The matrix below identifies each of the security controls in OTCC-1:2022 that a XONA CSG can either directly enforce or be used to help assist.

OTCC-1:2022

Controls	Control Objectives
1	**Cybersecurity Governance**
1-2	Cybersecurity Roles & Responsibilities: To ensure that roles and responsibilities are defined for all parties participating in implementing the operational technology cybersecurity controls (OTCC) within the organization.
1-2-1-2	Cybersecurity roles and responsibilities related to OT/ICS assets must be assigned to the cybersecurity function in the organization.
1	**Cybersecurity Governance**
2-2	**Identity and Access Management:** To ensure secure and restricted logical access to OT/ICS assets to prevent unauthorized access and allow only authorized access for users, which are necessary to accomplish assigned tasks.
2-2-1-2	Service accounts must be managed securely for OT/ICS services, applications, systems, and devices that are separated and disconnected from interactive users account logins.
2-2-1-3	Default credentials for all OT/ICS assets must be changed, disabled, or removed.
2-2-1-4	Sessions must be managed securely, including session authenticity, session lockout, and session timeout termination.
2-2-1-5	Automatic disabling/removing of service accounts, programs, or accounts related to OT/ICS assets must be prevented, except for monitoring systems.
2-2-1-6	Dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment must be employed.
2-2-1-7	Remote access to the OT/ICS networks must be restricted and exceptionally enabled when necessary and justified. A cybersecurity risk assessment must be conducted prior to granting remote access and its associated risks are monitored and managed. The granted access must be through trusted multi-factor authenticated and encrypted channel for a defined period of time and with limited access privilege. The remote access session must be monitored and recorded while its time duration and granted user's privilege must be in accordance with the cybersecurity risk assessment.

[2] https://www.gartner.com/en/documents/4017995

Controls	Control Objectives
2-2-1-8	Secure and complex password standards must be implemented.
2-2-1-9	Secure mechanisms to store OT/ICS assets' passwords must be used.
2-2-1-11	Access shall be immediately revoked when no longer needed.
2-3	System and Processing Facilities Protection: To ensure the protection of OT/ICS systems and processing facilities against cyber risks.
2-2-1-11	Advanced protection mechanisms and techniques must be utilized and securely managed to block and protect from malware, Advanced Persistent Threats (APT), malicious files, and activities.
2-3-1-3	Periodic security patches and upgrades must be implemented in alignment with vendor implementation guidance or recommendations with respect to cybersecurity and an organization's formal change management mechanisms.
2-3-1-4	Principles of least privilege and least functionality must be applied.
2-3-1-7	OT/ICS assets must be managed through dedicated, segmented, and hardened Engineering Workstation (EWS) and Human-Machine Interface (HMI) for management purposes and maintenance.
2-3-1-9	Usage of external storage media in the production environment must be restricted unless secure mechanisms for data transfer are developed and properly implemented.
2-3-1-10	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.
2-3-1-12	New communications sessions and commands execution must be detected and analyzed.
2-3-1-13	Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.
2-4	**Networks Security Management:** To ensure the protection of the organization's OT/ICS networks from cyber risks.
2-4-1-1	OT/ICS environment must be segmented logically or physically from other environments or networks.
2-4-1-7	Direct exposure of common remote authentication and access management services on external-facing hosts must be prevented.
2-4-1-9	Direct communications between corporate zone and OT/ICS zones must be prevented, and direct all the required connections through dedicated, secured, and hardened jump host/solution in the DMZ zone.
2-4-1-10	Remote access point in the DMZ zone must not be connected to the OT/ICS networks unless needed, while ensuring that the session is multi-factor authenticated, recorded, and established for a defined period of time.
2-4-1-12	Dedicated gateways must be used to segment OT/ICS networks from corporate zone.
2-4-1-13	Dedicated DMZ zone must be used to reside any system that needs services provided by corporate zone.
2-4-1-14	Strict limitation on enabling/usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.

Controls	Control Objectives
2-5	**Mobile Devices Security:** To ensure the protection of mobile devices (including laptops, handheld configuration devices, network test devices, etc.) from cyber risks and to ensure the secure handling of sensitive data and the organization's information
2-5-1-5	Encryptions mechanisms must be used for mobile devices authorized to access the OT/ICS assets.
2-6	**Data and Information Protection:** To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyber-attacks to prevent or minimize the negative impacts on the organization's operations.
2-6-1-4	Transfer or usage of OT systems' data in any environment other than production environment must be limited, except after applying strict controls for protecting that data.
2-11	**Cybersecurity Event Logs and Monitoring Management:** To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyber-attacks to prevent or minimize the negative impacts on the organization's operations.
2-11-1-1	Cybersecurity event logs and audit trails must be activated for all OT/ICS assets.
2-11-1-2	Failure attempts in accessing the organization's monitoring systems must be detected and logged.
2-11-1-5	Upload or download activities of OT/ICS assets including Safety Instrumented Systems (SIS) must be detected.
2-11-1-6	All remote access sessions must be monitored
4	**Third-Party Cybersecurity**
4-1	**Third-Party Cybersecurity:** To ensure the protection of organizational assets against the cybersecurity risks related to third-parties, including manufactures of OT/ICS-related hardware and software, vendors of OT/ICS products and suppliers of OT/ICS-related services as per organizational policies and procedures, and related laws and regulations.
4-1-1-3	Third-party contractors and vendors must use formal and documented Secure Development Life Cycle (SDLC) practices for systems and components designed or deployed in OT/ICS environment.
4-1-1-4	Periodic cybersecurity assessment and audits of third-party providers must be conducted to ensure the mitigation of any identified cyber threats.

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

+1 866-849-6629 | info@xonasystems.com