# Securing critical infrastructure:

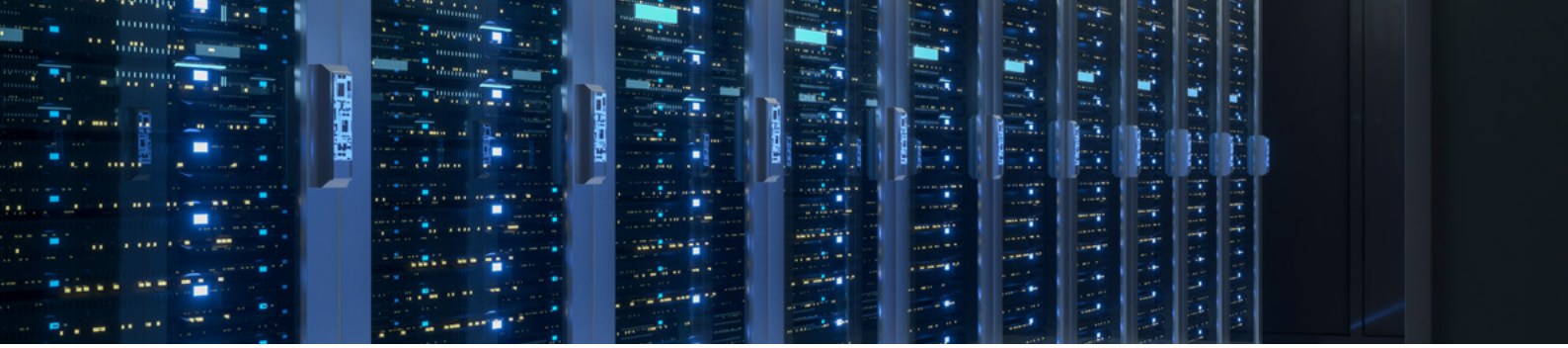
## Building upon Secure by Design to Secure by Operations

Secure by Operations Posture Paper

The acceleration of digital transformation through the adoption of cloud services, IoT architecture, AI, and automation has increased connectivity, expanded the attack surface, and created greater interdependencies among stakeholders with an interest and responsibility in securing critical infrastructure. These stakeholders include technology providers, system integrators, asset owners and operators, and government authorities. This paper aims to illustrate the responsibilities of stakeholders across the value chain by incorporating the concepts of Secure by Design at the product development stage, following secure deployment guidelines and configurations when integrating the technology into end-user operating environments, and utilizing Secure by Operations for the ongoing maintenance and oversight of deployed technologies throughout their lifecycles. It delineates roles at each of these stages to provide clear guidance, ensuring every stakeholder understands their part in maintaining the cybersecurity posture while fostering a collaborative and unified approach.

### Secure by Design

Secure by Design is a principle that emphasizes the importance of integrating security measures throughout the entire product development lifecycle. For technology providers, this means focusing on product security from the initial development stages to commissioning and ongoing vulnerability management. By embedding cybersecurity into every phase of the product lifecycle, technology providers aim for their offers to be resilient against potential threats.



This approach is implemented through a Secure Development Lifecycle (SDL), which should be an integral part of the product development framework. SDL requirements should adhere to international standards, such as the ISA/IEC 62443-4-1/ISO 27001 series, to streamline requirements and ensure the highest security practices. Assurance for this process can be achieved through rigorous security and penetration testing, responsible disclosure and vulnerability management, and by measuring the maturity of these activities over time. Additionally, when relevant, external certification of these processes can serve as an external validation of SDL practices.

Technology providers should prioritize the following actions:

- Implement and demonstrate Secure by Design practices with evidence-based approaches.
- Provide awareness initiatives, training, and certification internally and to system integrators and end-users, when possible.
- Offer secure implementation documentation and guidelines.
- Deliver services to identify gaps and enhance cybersecurity maturity.
- Share threat intelligence information.
- Manage supply chain cybersecurity risks while offering incident response support.

## The handoff from Secure by Design to Secure by Operations

Technology providers' solutions are targeted by threat actors, making it crucial that they are appropriately configured and adequately maintained in end-user environments. System integrators are generally responsible for secure implementations that combine diverse hardware, software, and communication protocols into a unified operating environment, playing a central role in critical infrastructure security. They must configure the technology securely, adhering to manufacturer secure deployment guidelines (inclusive of hardening guidelines, secure configurations, documentation, etc.), while prioritizing immediate user protection. This includes making end users acutely aware that deviating from safe defaults increases the likelihood of compromise unless additional compensating controls are implemented.

## Secure by Operations

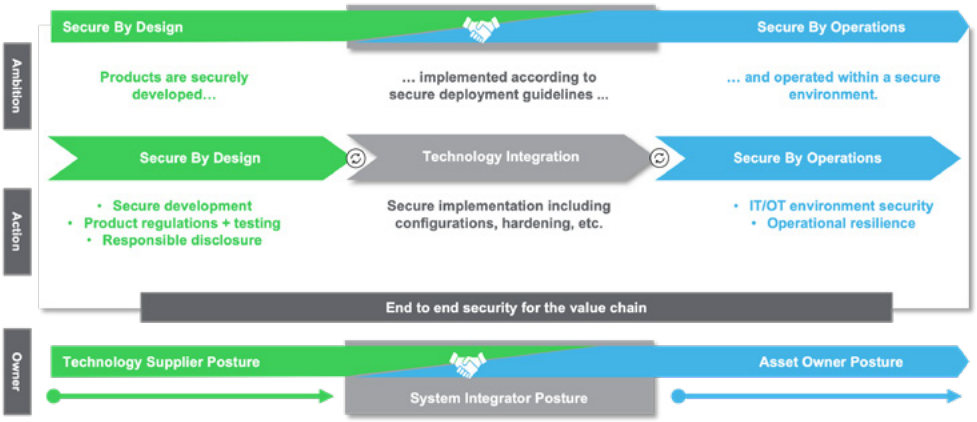
Secure by Operations focuses on the operational environment and guides asset owners and operators in maintaining a secure, multi-technology landscape after deployment. Despite mature product security practices as part of Secure by Design efforts, cyber incidents on critical infrastructures remain a significant concern. These incidents are often caused by system misconfigurations that lead to insecure operational environments. The impact of insecure environments can be severe, as a cyberattack on one stakeholder in the value chain can cause significant operational, financial, or reputational damage to others both upstream and downstream. Therefore, asset owners should perform tasks such as routine patching and monitoring as part of their operations.

**Asset owners/operators should prioritize the following actions:**

- Establish the appropriate organization and procedures for their risk tolerance that are appropriate to their environment to ensure cybersecurity controls throughout the system lifecycle.
- Ensure that integrators and operators are qualified and follow security instructions from manufacturers.
- Identify and manage relevant cybersecurity risks in the environment.
- Comply with cybersecurity regulations, policies, export control, and other rules.
- Provide training and certification on system secure guidelines for commissioning and operation.
- Continuously monitor and maintain a secure environment through network monitoring and OT threat detection capabilities.
- Implement access management, data classification, and network segmentation controls.

**Service providers/system integrators should prioritize the following actions:**

- Continuously monitor and maintain a secure environment through network monitoring and OT threat detection capabilities.




## The role of governments

Given the scale of these challenges, government regulators also have a role to play in raising awareness and incentivizing proper practices within their jurisdictions. Transparent reporting requirements in regulations such as the European Union Cyber Resilience Act (CRA) and stakeholder guidance such as the United States Department of Energy's Supply Chain Cyber Security Principles are examples of how government can leverage policy to clarify roles and responsibilities for the security of critical infrastructure.

Beyond policy, governments can use their unique authorities and convening power to bring diverse stakeholders to a common forum to share information and threat analysis across the value chain and educate stakeholders about their roles and responsibilities in securing critical infrastructure.

## Closing and call to action

In conclusion, this paper aims to spread awareness and focus on Secure by Operations principles, serving as an aspirational guide to defining roles and responsibilities in alignment with key industry standards. It is important to note that the roles and responsibilities outlined here are representative and not exhaustive. We encourage all stakeholders to actively engage in this collaborative effort, continuously improve their security practices, and adapt to the evolving threat landscape. By working together, we can ensure the resilience and security of our critical infrastructure for the future.

## Reference links


https://gca.isa.org

https://www3.weforum.org

https://gca.isa.org

https://www.se.com


se.com

Life Is On Schneider Electric


Schneider Electric Industries SAS
35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0)1 41 29 70 00