SIDEL Security Bulletin
General Cybersecurity Guidelines

1 GENERAL CYBERSECURITY GUIDELINES

1.1 Security by design approach

- Adopt a risk-based approach to cybersecurity and prioritise actions based on business requirements.
- Adopt a “breach assumption” mentality and improve resiliency by following these principles:
  - In-depth defence
  - System and network hardening and attack surface reduction: removing any functionalities that could induce risk
  - Least privilege
  - Situational awareness and continuous monitoring: identifying system and operational dependencies (network map, asset inventory, …)

1.2 Awareness

- Periodically train all employees to follow cybersecurity best practices (e-learning modules, ethical phishing campaigns, awareness campaigns, …).
- Periodically train all employees having access to production networks and equipment to follow Operational Technology (OT) specific cybersecurity best practices. Topics covered by this training could be but are not limited to:
  - Why protecting the security of industrial control systems has become a significant concern
  - The different types of threats and common attacks to industrial automation networks
  - The potential consequences of successful cyber attacks
  - Recommended security measures to protect plant assets and employees against cyber threats
  - Understanding the necessity of implementing a risk management process
  - Standards and best practices to secure control systems and plant operations
  - Avoiding social engineering and leakage of sensitive information
  - Managing passwords and user accounts
  - Secure access to critical automated production systems
  - Detecting and reporting suspicious activities

1.3 Physical access

- Limit access to production environments to authorised personnel only.
- Install physical controls so that no unauthorised personnel can access your industrial control and safety systems, components, peripheral equipment and networks.
- Keep all electrical cabinets and racks locked and keep track of keys.
- Protect all accessible communication ports (USB, Ethernet) with physical locks

1.4 Network architecture

- Remote connectivity to OT networks and devices provides a known path that can be exploited by cyber actors. External exposure should be reduced as much as possible.
- Use publicly available tools, such as Shodan, to discover internet-accessible OT devices. Take corrective actions to eliminate or mitigate internet-accessible connections immediately.
- Follow best practices relating to network hardening:
  - Fully patch all internet-accessible systems.
  - Segment networks to protect PLCs and workstations from direct exposure to the internet. Implement secure network architectures utilising demilitarised zones (DMZs), firewalls and jump servers.
  - Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
  - Implement network traffic control at component level (host firewall)

- Ensure all communications to remote devices use a virtual private network (VPN) with strong encryption further secured with multifactor authentication.
- Check and validate the legitimate business need for such access.
- Filter network traffic to only allow IP addresses that are known to need access.
- Capture and review access logs from these systems.
- Use managed switches and disable all unused ports.
- Choose to use secured communication protocol (TLS based encryption)

1.5 Resiliency

- Scan all external devices (technicians' laptops, USB keys, external hard drives, …) before using them in terminals or in any node connected to production networks.
- Backup "gold copy" resources, such as firmware, software, ladder logic, service contracts, product licenses, product keys and configuration information. Verify that all "gold copy" resources are stored off-network and store at least one copy in a locked tamperproof environment (e.g. locked safe).
- Test and validate data backups and processes in the event of data loss due to malicious cyber activity.
- Restore OT devices and services in a timely manner. Assign roles and responsibilities for OT network and device restoration.
- Periodically scan all components for malware infection (with the recommendation to proceed with scans during maintenance windows to avoid any disruption). In case of infection, proceed immediately with a full restore.
    - Using a realtime protection security solution (antivirus and/or EDR) is recommended.
    - Implement a central SIEM solution to collect all relevant system and security logs from production networks to streamline incident response and forensics analysis. A minimum set or required events to collect on components running Windows can be communicated by Sidel
    - Using a realtime monitoring security solution for is recommended (EDR)

2 CHANGELOG

- **V1.0:** October 2, 2020 - Initial publication
- **V1.1**: February 2, 2022 – Update with recommendations including security event logging, use of a SIEM and use of an antivirus/EDR solutions