CE+T POWER
Leading Conversion Technology for Power Resilience

# Inview Cybersecurity

Bolster cybersecurity and reduce cyber threats in your industrial environment.

## Inview Cybersecurity

In the context of **critical backup** and **energy transition**, the significance of **cybersecurity** cannot be overstated. Any compromise in the security of industrial equipment could lead to disruptions in power supply, which could have far-reaching consequences for businesses, communities, and even national security. Moreover, with the evolving landscape of energy technologies and the integration of renewable sources, the complexity and vulnerability of these systems to cyber threats only increase.

In this scenario, **CE+T Inview Power controllers (Slot, S, XC and X)** stand out as ideal solutions for **bolstering cybersecurity in industrial environments**. With the release of Inview v5.5 and subsequent versions, significant cybersecurity enhancements have been implemented to address various security concerns. When the Inview controller is equipped with the Operation license, additional security functionalities become accessible.

- **HTTPS (Hypertext Transfer Protocol Secure)** is used to secure communication between a client (such as a web browser) and a server (such as a website). It protects against eavesdropping, data tampering and impersonation by malicious actors. Using a custom/official certificate requires the **Operation license**. Without it, a self-signed certificate is included, but it may generate warnings in the web browser.
- **RADIUS (Remote Authentication Dial-In User Service)** ensures that only authorized users are granted access to network resources, enhancing overall network security. This requires an **Operation license**.
- **Low-level platform security hardening** prevents unauthorized access to the boot loader and operating system.
- **Device tampering prevention features**, including the possibility to configure the controller to prevent downgrades and factory resets that could compromise device security.
- **Upgraded operating system**, incorporating numerous security improvements across different components.
- **Streamlined software distribution** and settings reduce the attack surface by removing unused components from the operating system.
- **Enhanced software upgrade package verification** using private/public key signing ensures the authenticity and integrity of software updates.
- **Web service security enhancements**, including improved user input filtering and protection against various types of attacks such as brute force password attacks.
- **Implementation of policies to prevent unauthorized app side-loading** ensure that only approved software is installed on the device.
- **Improved user management** with differentiated profiles and privilege escalation prevention measures to control access and minimize the risk of unauthorized actions.
- **Strengthened storage and file management** operations with added safeguards against file upload and data storage vulnerabilities.
- **Optimization of network security rules** and internal firewall behavior to protect against external threats.
- **Implementation of robust password policies**, including alerts for unchanged default passwords and checks for password quality to enhance overall system security.

By incorporating these **cybersecurity enhancements**, the **Inview CE+T Power controllers** offer a comprehensive solution for **safeguarding critical industrial equipment** related to **backup systems and energy transition initiatives**. These measures not only protect against **potential cyber threats** but also **ensure the reliability**, **integrity**, **and resilience** of **industrial operations** in the face of **evolving security challenges**. In essence, the Inview CE+T Power controller serves as a reliable and secure choice for organizations seeking to **fortify their critical infrastructure against cyber risks** in the context of energy transition and critical backup systems.