Basler Electric®

www.basler.com
+1 618.654.2341 (USA)
info@basler.com

Cybersecurity Deployment Guidelines

Introduction

This document provides information on Basler Electric cybersecurity features and details a defense-in-depth strategy for system implementation of the following products:

- DECS-150
- DECS-250
- DECS-250N
- DECS-250E
- DECS-450
- DECS-450R

Overview of Security Features

Table 1 lists cybersecurity features included in Basler products in order to harden the security posture of systems.

Table 1. Device Security Features

Feature	DECS-150	DECS-250	DECS-250N	DECS-250E	DECS-450	DECS-450R
User authentication and obfuscation of password entry	✓	✓	✓	✓	✓	✓
Device identification and authentication	✓	✓	✓	✓	✓	✓
No wireless access	✓	✓	✓	✓	✓	✓
Port access controls	✓	✓	✓	✓	✓	✓
Session timeouts	✓	✓	✓	✓	✓	✓
Concurrent session control	✓	✓	✓	✓	✓	✓
Login attempt failures	✓	✓	✓	✓	✓	✓
Security log	✓	✓	✓	✓	✓	✓
Event log	✓	✓	✓	✓	✓	✓
System-in-use message	✓	✓	✓	✓	✓	✓
Digitally-signed software (BESTCOMS*Plus*®)	✓	✓	✓	✓	✓	✓
Digitally-signed firmware	✓					
Secure boot	✓					
BESTCOMS*Plus*® proprietary protocol	✓	✓	✓	✓	✓	✓
Real-time clock (timestamps)	✓	✓	✓	✓	✓	✓
Settings input range checking	✓	✓	✓	✓	✓	✓
Watchdog fail-safe operation and deterministic outputs	✓	✓	✓	✓	✓	✓
Real-time operating system (RTOS) to prioritize essential functions	✓	✓	✓	✓	✓	✓

Note

The Basler Electric products and software covered in this publication provide a variety of cybersecurity features, but system owners and administrators must make choices regarding settings configuration and physical and network access to create and maintain robustly secure control systems. Review the following sections for an overview on Basler Electric's cybersecurity recommendations. Refer to your device's instruction manual for more detailed instructions on individual settings.

Physical Access

Products use either urethane encapsulation or metal enclosures for environmental and physical hardening.

For additional physical security, products should be installed in enclosures which limit access to terminals, connectors, and rear communication ports (while adhering to standard industry practices). Also, all unused communication ports should be disconnected to help prevent unauthorized access.

Security of Portable Devices

Product configuration requires the use of a Windows® PC or laptop. When using these devices, configuration access should be limited to authorized personnel and equipment. Additionally, equipment used to communicate with the product should be managed and updated using current cybersecurity practices, including installation of anti-virus and anti-malware software and periodic patching.

User Authentication

Products support multiple user accounts (total number varies by product) with six different types of selectable security access. When selecting access levels for individual users, system administrators should consider least-privilege principles.

Product features allow for password expiration periods, but they cannot enforce password strength. Credential expiration and password strength standards are recommended; enforcement of these standards must be managed by system administration.

File Management

Basler Electric products utilize settings, logic, and security files for configuration. These files are created, consolidated, and saved using BESTCOMS*Plus*. The files do not utilize encryption methods, so they should be managed in a secure manner consistent with the system owner's policies.

During commissioning, review firmware and software versions installed to ensure they are the latest version, and continue to remain current with all firmware and software versions. Initial BESTCOMS*Plus* installers can be downloaded from basler.com. Refer to the *Firmware and Software Upgrade Process* section for more information.

Session Management

Session management controls can be used to limit login attempts, create session timeouts, and initiate system-in-use messaging. These are especially important for Ethernet-based access. Coordination of these features can delay brute-force hacking attacks. In addition to these, use of a network security monitor to detect network anomalies is recommended.

Port Access Controls

Port access controls are available to restrict unauthorized user levels from accessing ports. Configuration can be set to completely disable a port if needed. Users must not lock out access on all ports or risk losing access to the device.

Caution

Selecting NONE secure access levels for BESTCOMS*Plus* via USB and BESTCOMS*Plus* via Ethernet can lock out access to communication ports and render the product unconfigurable.

Access Controls

To prevent unused or inactive ports from being used for malicious activities, a session timeout setting is available. This setting should be set based on a reasonable session time needed for the system. A long timeout setting can leave the session exposed to session hijacking. Performing a communication disconnect with BESTCOMS*Plus* will end an open session.

To slow brute-force password hacking attempts, login failure attempts are supported. Once the Login Attempts are reached, consecutive login attempts are ignored for the Login Lockout Time. This feature only slows a malicious login attempt. It is recommended to have a network monitoring system to annunciate such network intrusions.

System-in-Use Messaging

Settings changes implemented while the system is running can cause adverse effects. As such, some products (refer to Table 1) provide system-in-use messaging. When enabled, this feature notifies BESTCOMS*Plus* users at login if the system is currently running.

Trusted Networks

The Basler Electric products covered in this publication are embedded devices with limited network traffic handling capabilities. As such, devices should only be used on trusted networks with known network traffic rates, especially if the system is utilizing the network load share feature. It is recommended to manage and monitor the network to guarantee optimal performance.

Use of trusted networks can also help to avoid exposure to denial-of-service and brute-force attacks. Basler Electric products are designed to maintain critical functionality in the event of a denial-of-service attack. Communications to a device may fail or momentarily be disabled, but key functions like regulation will continue. If the network load sharing feature is used, this function may be impacted by a denial-of-service attack or high network traffic. As such, only trusted networks with known and managed traffic rates should be used to ensure proper operation. Note that the additional use of cyber security network monitors is recommended to detect and prevent brute-force attacks.

Modbus® TCP can be implemented for connection to SCADA systems. This implementation allows for a single user's login to have write access. However, Modbus is an open ubiquitous protocol and is easily targeted by hackers, so Modbus should be implemented on trusted networks only.

Table 2. List of Ports

Function	Port
BESTCOMS*Plus*®	Protocol TCP 2102; Discovery UDP 7021
Modbus®	TCP 502
Network Load Sharing	UDP 2760 & 2761

Cybersecurity Maintenance and Service Returns

Log Review

Sequence-of-events and security data logs (for some products; see Table 1) are generated for use in commissioning, maintenance, and security monitoring. These logs can be output and saved in a human-readable format using BESTCOMS*Plus*.

The product generates timestamped logs pertinent to system events and security activities. The product retains a circular buffer of each log. It is recommended to periodically download, review and archive the logs to assist in determining events on the system. Both logs are human readable after being downloaded. To avoid tampered records, it is recommended to download the records on a trusted network and store them in a secure location.

Refer to the product's instruction manual for more details about the sequence of events log and the security log (if available).

Verification and Restoration of Settings

The authenticity of system settings is critical. Malicious or misconfigured settings can cause adverse operations. As such, product settings should be created and verified by qualified personnel, as well as periodically re-verified to ensure the settings are correct. To perform verification, BESTCOMS*Plus* provides a settings comparison tool. Once settings are verified through commissioning, the settings file should be retained for later settings verification and quick restoration in the event of an incident. Refer to the device's instruction manual for more information.

Return for Service

In the event a product needs to be returned to Basler Electric for evaluation, private information should be removed from the device. File settings, logic, and security settings can be overwritten by uploading the default BESTCOMS*Plus* file settings, logic, and security settings to the unit. If necessary, Basler may request the settings and logic files themselves. In this case, security settings and private information should be removed from the file prior to transmitting it to Basler.

Firmware and Software Upgrade Process

Basler Electric periodically releases feature additions, improvements, and bug fixes for firmware and software.

Notification of available firmware updates is available through an email subscriber list. To be added to the email subscriber list, make an account at basler.com, and use the Software Notifications link under My Account to sign up for updates on applicable products. Requests for firmware updates can be made through technical support. To perform the firmware update, refer to the product's instruction manual for details.

BESTCOMS*Plus* contains an update notification feature built into the software. Upon launching of BESTCOMS*Plus*, the software attempts to access the Basler Electric server. If successful, BESTCOMS*Plus* will notify the users of any available updates. Updated installers can be launched from that screen.

Field firmware upgrades are supported through BESTCOMS*Plus*. During the firmware installation process, the digitally-signed firmware (see Table 1) is authenticated. If the authentication fails, BESTCOMS*Plus* will provide indication of the failed firmware load, and the original firmware version will be retained. In addition, products with secure boot capabilities (see Table 1) authenticate firmware during the boot process. The BESTCOMS*Plus* installer and executables are digitally-signed with an industry-recognized certificate authority.

Incident Response

In the event of a cybersecurity incident involving a product and/or BESTCOMS*Plus*, please contact Basler Electric technical support. To receive the most efficient and effective support, please provide the following:

- A description of the event
- Log files and/or other evidence of the event
- The configuration and logic file
- The serial number of the product
- The installed firmware and BESTCOMS*Plus* versions
- The system Modbus configuration

Decommissioning

At the end of life of the product, Basler Electric recommends removal of private information from devices. To remove private information from a device, upload the BESTCOMS*Plus* default file to replace the settings, logic, and security data.