White Paper: EST4 Cybersecurity

CYBERSECURITY IN COMMERCIAL FIRE ALARM: SHAPPING THE FUTURE, SETTING THE STANDARD

The following gives a broad overview of Cybersecurity and highlights the key cybersecurity features found in the EST4 Commercial Life Safety System.

Edwards EST4 Control Panel

OVERVIEW

Cybersecurity is defined by Merriam-Webster as the "measures taken to protect a computer or computer system (on the internet) against unauthorized access or attack." How does this apply to fire alarm systems that traditionally haven't connected to the internet like computers? While this may have been true in the past, in today's connected world, believing the life safety system is protected by an air gap - a space between the life safety system and external threats - may not be the case if the system provides even simple operations, such as sending event based email notifications. Connectivity is necessary and expected in an increasing number of installations, driving the need for protection against unauthorized access.

The EST4 system provides levels of protection and the flexibility to deploy in a manner that can mitigate cybersecurity threats. The internal EST4 life safety network takes advantage of industry standards in creating a secure peer-to-peer IPv6 mesh (or other topology design) network that deploys easily. The system's flexibility allows the installer to work with the building owner, local IT and cyber professionals to match the system to IT or cybersecurity needs. EST4 allows customized applications, matching the site's cybersecurity assessment needs to the panel function, all while keeping the life safety demands in the forefront.

Whether a site has a detailed Security Incident and Event Management (SIEM) structure or is more ad hoc in its approach, understanding how EST4 addresses cybersecurity attack surfaces (areas that may be exploited) helps both the installer and local IT align. Blending the active protection, compensating controls, and audit trail capabilities available to the cybersecurity and life safety needs of the project helps ensure a successful and secure installation.

CYBERSECURITY - ARE AIR GAPS ENOUGH?

An air gap, which is a space between the life safety system and external threats, can be enough to protect against threats in some instances. EST4 has multiple levels of physical security that can be deployed to meet requirements that call for an air gap. In fact, an air gap can be a compensating control for some cybersecurity requirements. Adding local physical access restrictions to a panel monitored via hardware, like tamper switches, can be deployed into EST4 cabinets. These access monitoring methods provide an audit trail of cabinet access. This, in conjunction with EST4 archives tied to building security protocols, provides additional levels of protection. However, an air gap means the life safety system should not connect to or communicate with any external IT infrastructure. In today's connected world, this is not always practical or acceptable, because it's the connections to external networks that provide the power for the simplest of operations, like sending an email based on a system event. The external connection needed from EST4 to the email server, allowing the email and its operational efficiencies, may not be available in an isolated (air gap) system. Plus, there are other external connections to be considered, such as to a central monitoring station (CMS) or third-party equipment.

EST4 panels address higher level cybersecurity needs through an internal network, hardware, and connectivity to the programming tool and outside networks.

The internal life safety network takes advantage of industry standards, bringing a self-configuring peer-to-peer IPv6 network that does not need a centralized server. The peer-to-peer network nodes authenticate with each other using a salted hashed unique identifier, allowing interoperation with nodes of the same project only. "Man-in-the-middle" attacks on the network are less likely and would be disclosed to the fire operations center, captured in history and auditable.

To further reduce risk and minimize the attack surface of EST4 hardware, all programming ports on microcontrollers are disabled during manufacturing, and physical connection points are removed on all microcontrollers and Printed Circuit Board (PCB) assemblies, making connection via product hardware difficult. All services and applications run non-root based, including user accounts. Console access to the operating system or firmware of the fire system is not provided.

When external connections are needed, EST4 protects the life safety network by offering a fully fire-listed firewall that is part of the fire panel, not a third-party add-on device. The EST4 firewall (4-FWAL) separates the life safety network from outside networks and is designed as a proxy firewall – no network data packets are passed from one side of the firewall to the other. All network traffic is handled within the firewall itself, transformed and repackaged before being provided on the other side of the firewall.

Protocols and ports are restricted to only those needed by EST4 operation; the firewall will block all other traffic.

4-FWAL CYBERSECURITY AT A GLANCE

- Email/SMS, ECPxml, web browser services are via 256 bit AES via SSL/TLS (FIPS-197)
- Email/SMS root certificates are from Mozilla Public License
- Central Station connections (IP dialer): 128 bit AES Tyco Protocol, encryption/authentication key provided by central station on an account by account basis
- Email/SMS and IP to a CMS are outgoing communication services only initiated by the EST4
- Browser and ECPxml communications are incoming communications using a passphrase for authentication within a TLS

session. ECP is hashed by port and requires a passphrase of up to 40 Unicode characters and a Hashed salted license key. The web browser session is authenticated by the firewall system, requiring a passphrase of up to 40 Unicode characters

- Web browser provides access only to system reporting functions, no update methods are provided
- 4-FWAL incoming service requests can be turned off at startup, by time of day or via programming, with only outgoing requests allowed. This firewall policy keeps system critical events always being able to be sent to services like central monitoring stations
- Session timeout is enforced
- Brute force access through the web browser shuts down after five unsuccessful authentication tries. These access attempts are stored to history as monitor events

While the EST4 firewall works in tandem with the site IT infrastructure, the site should always include its own commercial firewall to protect the building network or intranet.

ACCESS AND AUTHENTICATION

Access to EST4 is based on industry-standard best practices. A physical barrier, such as a locked door, provides the first layer of defense for unauthorized access to the system, and tamper switches can be installed to monitor panel access. To gain access to higher level system operations, a seven digit code is needed, where the first three digits identify the user and the last four digits represent the user's PIN. All panel access is role-based; a user can only perform actions explicitly allowed by the system configuration and permissions policy set for the access level entered. For example, a user with a high level of access can enable and disable devices, but a lower level user cannot. EST4 does not lock the user interface (UI) if the maximum number of login attempts is exceeded, keeping the primary objective of the life safety system active, available and unobstructed. To further enhance access security, a timeout is also put in place to force a user logout after a period of inactivity, limiting exposure due to panels being logged into without surveillance. All password attempts, successful or not, are logged to local history for audit trail access.

The system configuration software (4-CU), its project and connection to EST4, meets FIPS 197 infrastructure requirements. Additionally, two-factor authentication is needed for configuration access to the panel, including a project passphrase that is up to 40 Unicode characters combined with a licensed PC, and a 6-digit session access code is randomly generated by the panel. No passphrases, access codes, or PINs are stored in any database as plain text. All 4-CU access to the panel is logged to history, including the user information. The 4-CU software enforces lockout after five failed attempts to access a project.

As cybersecurity needs expand, EST4 provides solutions that can help meet the demands of a connected life safety system.

EST4 - supporting cybersecurity while keeping life safety at the forefront.

To learn more, please visit us at edwardsfiresafety.com/EST4.