VIVOTEK

A Delta Group Company

White Paper

Product Cybersecurity

2022 Ver. 1.0

Index

Introduction **3**

Security Strengthened 3

Security Strengthened Product 3

IACS Standard Compliance **4**

IEC 62443 Requirements Compliance 4

Cybersecurity Features **7**

Secure Boot 7

TrustZone 7

Secure Debug and Console 8

Secure VADP 8

Secure Upgrade File 8

Secure Firmware 8

Dual Firmware Design 9

Summary **9**

Appendix **10**

Appendix 1: Cybersecurity 10

Appendix 2: IEC-62443 10

Introduction

The constantly changing world and global events have caused shifts in people's daily routines. Remote working models are becoming more common, vastly increasing online activity. Inevitably, businesses must rely more on computers, sensors, and IoT connected devices, drawing the attention of cyber criminals looking to profit.

Maintaining good cyber hygiene is crucial in this era, especially to businesses, governments, and manufacturers. Furthermore, manufacturing commercial off-the-shelf (COTS) products is focusing more on the economies of scale and ensuring quality, and VIVOTEK is well aware that cyber hygiene for products and corporate information security is difficult to achieve during mass production.

Businesses that want to protect their network, devices and services from cyber-attacks require a collaborative effort to manage threats on a system level. This means the responsibility to prevent attacks also falls upon vendors across the entire supply chain, who need to provide enhanced solutions to help customers counter cybersecurity threats.

Security Strengthened

It is not practical to implement the highest security requirements in all environments. Instead, separating assets into different security levels based on their common requirements is more efficient.

Establishing zones and groups based on security requirements and levels (eg. the Purdue Model) makes it possible to achieve deeper and more systematic protection, thereby enabling defense in depth (DiD).

Companies' I.T. systems usually need to handle important and confidential data. This means it is generally recommended to avoid connecting them to new, unfamiliar, and complex technologies, as this introduces unknown risks.

In contrast to I.T. systems, surveillance systems in industrial automation and control system (IACS) networks are usually placed to achieve specific purposes. This makes it unnecessary to have sophisticated, multi-layered security protections for them.

Security Strengthened Product

Therefore, as a leading supplier of surveillance cameras, VIVOTEK provides product lines with strengthened security settings to help customers efficiently safeguard their security.

This ensures that the users of VIVOTEK cameras can also enjoy more rigorous cybersecurity for their entire corporate network.

IACS Standard Compliance

Currently, there is no security standard specific to video surveillance. Therefore, it is recommended to follow guidelines from other industrial or IoT security standards.
IEC-62443 is a comprehensive set of international standards for IACS that focuses on risk assessment and addresses security at all phases of design and development.

At the component level, IEC-62443 addresses the necessary improvements for IoT devices to strengthen cybersecurity.

Specifically, IEC-62443 4-2 divides components into levels 1 to 4 based on their security level capabilities (SLCs).

Each product will have a series of component requirements (CRs) and requirement enhancements (REs) applied to them based on their SLC level, thereby ensuring that each component fulfills the required specs for their SLC.

VIVOTEK cyber security features are compliant with the following requirements (CRs) by IEC 62443-4-2.

IEC 62443 Requirements Compliance

ID	62443-4-2 Foundational Requirement	62443-4-2 Requirement Description	VIVOTEK Security Features
1	CR 1.1 - Human user identification and authentication	To identify and authenticate all human users on all interfaces capable of human user access that support segregation of duties and least privilege in accordance with applicable security policies and procedures..	Account management
2	CR 1.4 - Identifier management	To integrate into a system that supports the management of identifiers and/or To support the management of identifiers directly according to IEC 62443-3-3 SR 1.4.	Compliant
3	CR 1.7 - Strength of password-based authentication	To enforce configurable password strength according to internationally recognized and proven password guidelines.	Password policy
4	CR 1.10 - Authenticator feedback	To obscure feedback of authenticator information during the authentication process	Compliant
5	CR 1.11 - Unsuccessful login attempts	To deny the consecutive invalid access during a configurable time period	Ban user
6	CR 1.12 - System use notification	To display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	System use notification before login

Supports IEC-62443 Technical Requirements

ID	62443-4-2 Foundational Requirement	62443-4-2 Requirement Description	VIVOTEK Security Features
6	CR 1.12 - System use notification	To display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	System use notification before login
7	CR 2.1 - Authorization enforcement	To provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities	Compliant
8	EDR 2.4 - Mobile code	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device: a) Control execution of mobile code; b) Control which users (human, software process, or device) are allowed to upload mobile code to the device; c) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Compliant
9	CR 2.5 - Session lock	a) To protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and b) For the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.	Session time out
10	CR 2.8 - Auditable events	To generate audit records relevant to security for the following categories:	Compliant
11	CR 2.9 - Audit storage capacity	a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and	Compliant

Supports IEC-62443 Technical Requirements

ID	62443-4-2 Foundational Requirement	62443-4-2 Requirement Description	VIVOTEK Security Features
12	CR 2.10 - Response to audit processing failures	b) Provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.	Compliant
13	CR 2.11 - Timestamps	a) provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and	Compliant
14	CR 2.12 - Non-repudiation	b) Provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Compliant
15	CR 3.1 - Communication integrity	To create timestamps (including date and time) for use in audit records.	Compliant
22	CR 6.1 - Audit log accessibility	To access audit logs on a read-only basis for authorized humans and/or tools	Audit log
23	CR 7.2 - Resource management	To limit the use of resources by security functions to protect against resource exhaustion.	Compliant
24	CR 7.4 - Control system recovery and reconstitution	To be recovered and reconstituted to a known secure state after a disruption or failure.	Secure boot and Secure FW
25	CR 7.6 - Network and security configuration settings	To be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	Compliant
26	CR 7.7 - Least functionality	To specifically restrict the use of unnecessary functions, ports, protocols and/or services.	Compliant

* Only specific models with specific firmware versions are compliant with IEC 62443 standard. For detailed information, please contact your regional sales.

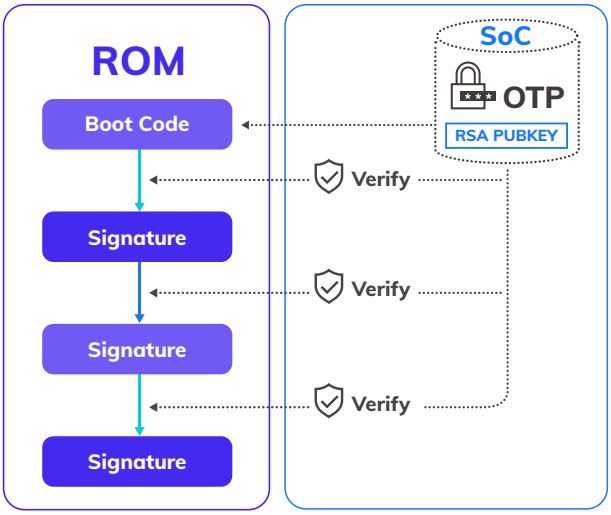
Cybersecurity Features

Secure Boot

The device goes through a series of steps in the boot process to ensure the installation proceeds as expected for the device to run correctly and securely.

Secure boot applies signed firmware to make sure the device only loads VIVOTEK's authorized firmware.

For security, devices with secure boot enabled do not permit JTAF and USB boot.



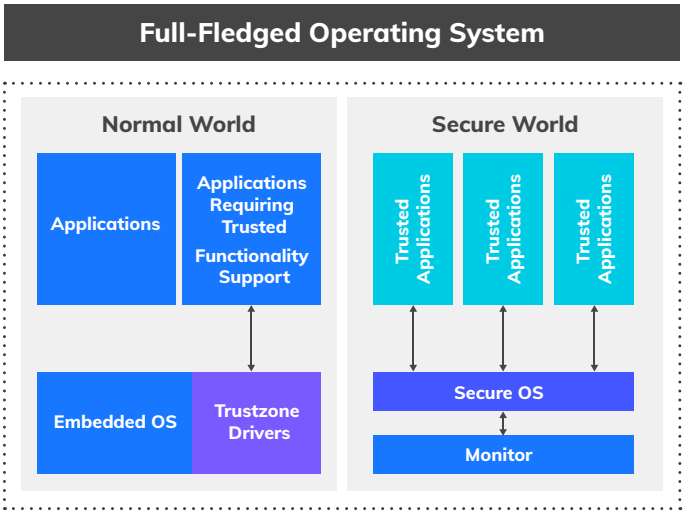
TrustZone

Devices with secure boot enabled will have the TrustZone feature.

TrustZone involves a Normal World and a Secure World connected via a Secure Monitor.

Rich applications only run inside the Normal World, while Secure World is in separated memory space, which means it won't be affected by any attack in Normal World.

The design of TrustZone further strengthens security and functionality on the OS level.



Secure Debug and Console

Secure Debug and Console are made to ensure that only authorized support engineers with the consent of users could enable the remote access console for troubleshooting purposes. Secure Debug & Console are made to ensure that only authorized support engineers, with user consent, could enable the remote access console for troubleshooting purposes.

When Secure Boot is enabled, the system console will be disabled automatically to prevent security breaches. With key-based authentication, only manufacturers that possess the corresponding authenticated keys, along with the device owner's explicit permission, will be eligible to enable the Secure Debug Mode.

The system console and SSH/SFTP will not be enabled unless it is under Secure Debug Mode.

Secure VADP

The VIVOTEK Application Development Platform (VADP) is an open platform that enables end users, resellers, and system integrators to enhance the features of VIVOTEK network products by adding third-party stand-alone applications or plug-in modules for specific security, business, and storage requirements.

Enhanced Secure VADP with digital signature and encryption capabilities further strengthen security.

Secure Upgrade File

Like all IoT product vendors, VIVOTEK provides customers with system upgrades via firmware updates. However, hackers often target publicly released firmware for system defects and loopholes.

VIVOTEK firmware is secure signed and encrypted to prevent hackers from getting into the details of the code, finding vulnerabilities in the system, or modifying firmware without authorization.

Secure Firmware

Bootloader: The system makes certain that all data needed is intact through Boot-Rom and secure signed certificates and keys.

Kernel, rootfs: All data are secure signed and encrypted with keys to ensure no data leaks during manufacturing.

Flash partition: The user storage area is encrypted with unique IDs to prevent data leaks if the Flash memory is stolen.

Replay Protection Memory Block (RPMB): A method for systems to store data in a specific memory area in an authenticated and replay protected manner, allowing only successfully authenticated accesses to read and write data.

Dual Firmware Design

Boot / Kernel / Rootfs images are stored with one additional copy to ensure that incidents during the update process won't affect system integrity.

Cameras won't need to use safe mode if there is any data loss, which lowers the risk of intrusions.

Summary

Surveillance systems have always played crucial roles in a variety of business scenarios, such as building automation and industrial automation.

VIVOTEK offers enhanced security to guarantee that its products fulfill customers' security requirements in this constantly changing world.

Information security risks can be effectively mitigated at a reasonable cost.

Appendix

Appendix 1: Cybersecurity

Suggestions for the establishment of security baselines

• Separating the surveillance network from other application networks is recommended.

• Setting up surveillance network access control lists (ACLs) is highly recommended.

• Maintain a list of devices in the surveillance network and check them regularly.

• Use firewalls to protect surveillance systems and the network whenever possible.

• Use intrusion detection systems or similar technologies to monitor the network status and network behaviours to track abnormal activity.

• Regularly check for security updates and cybersecurity information from VIVOTEK and update your surveillance system regularly.

• Regularly replace EOL / EOS systems with updated systems in networks.

• Design recovery policies and SOPs for when undesirable events happen, and hold drills for the SOPs according to the risk environment.

Appendix 2: IEC-62443

As mentioned, a key part of IEC-62443 is security levels (SLs).

SLs are used to assess the cybersecurity risks in each system. This helps customers understand how to best address cybersecurity risks.

Security Level	Description	Threat Actor	Examples of Actors
SL1	Protection against casual or coincidental violation	Insider and/ or External	• Careless or disgruntled employees or contractors • Intruders with low skills and motivation
SL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation		
SL3	Protection against intentional violation using sophisticated means with moderate resources, system-specific skills, and average motivation	External “professionals”	• Cybercriminals • Industrial espionage • State-sponsored malicious actors
SL4	b) Provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.		

Appendix 2: IEC-62443

In IEC-62443, basic security requirements for the assets and zones of IACS are defined in seven standpoints called Foundation Requirements (FR)

Foundation Requirements (FR)

- **Identification and Authentication Control (IAC)**
- **User Control (UC)**
- **Data Integrity (DI)**
- **Data Confidentiality (DC)**
- **Restricted Data Flow (RDF)**
- **Timely Response to Events (TRE)**
- **Resource Availability (RA)**

All requirements for assets and zones are set by assigning a level for each of these seven items.
To measure a security level, System Requirements (SR) are specifically defined for each Foundation Requirement (FR). Furthermore, for each System Requirement (SR), Requirement Enforcements (RE) are specified to satisfy each Security Level (SL).

Foundational Requirement	Associated Process
FR1 – Identification, Authentication, and Access Control	User authentication and authentication
FR2 – Use Control	Enforcement of roles and responsibilities
FR3 – System Integrity	Change management
FR4 – Data Confidentiality	Use of encryption
FR5 – Restrict Data Flow	Network segmentation
FR6 – Timely Response to Event	Audit logs
FR7 – Resource Availability	System backup and recovery

VIVOTEK

A Delta Group Company

www.vivotek.com

VIVOTEK Inc.
6F, No.192, Liancheng Rd., Zhonghe Dist.,
New Taipei City 235, Taiwan
| T +886-2-82455282 | E sales@vivotek.com

VIVOTEK USA
2050 Ringwood Avenue, San Jose, CA 95131
| T 408-773-8686 | E salesusa@vivotek.com

VIVOTEK EMEA
Zandsteen 15, 2132 MZ Hoofddorp,
The Netherlands
| T +31(0)20-800-3817 | E saleseurope@vivotek.com

VIVOTEK Japan
〒105-0012東京都港区芝大門2-1-14,
デルタ芝大門ビル
| T +81-3-5733-1280 | E salesjp@vivotek.com

VIVOTEK India
602, Best Sky Tower, Plot No. F-5, Netaji Subhash Place,
Pitampura, New Delhi-110034
| T +91-11-45137465 | E salesindia@vivotek.com

VIVOTEK LATAM
Ejército Nacional No. 418 Piso 7, Oficina 711. Col. Polanco V Sección,
Alcaldía Miguel Hidalgo, Ciudad de México
| T + 52 55 1101 1793 | E saleslatam@vivotek.com