

White Paper

Cybersecurity Enhancement of Wisenet 9 Products

July 2025

Contents

- 1. Introduction**
- 2. Compliance with ETSI EN 303 645 Standard**
 - 2.1. Overview of ETSI EN 303 645
 - 2.2. Key aspects of ETSI EN 303 645
 - 2.3. Certified Secure Products
- 3. Compliance with IEC 62443-4-1 Standard**
 - 3.1. Overview of IEC 62443-4-1
 - 3.2. Summary of IEC 62443-4-1
 - 3.3. Certified Secure Development Process
- 4. Implementing Secure Element for Secure Storage**
 - 4.1. FIPS 140-3 Certification
 - 4.2. Security Level of FIPS 140-3
 - 4.3. Use Cases and Scenarios of the Secure Element
- 5. Enhancing Software Supply Chain Security**
 - 5.1. Introduction of SBOM
 - 5.2. Features of Hanwha Vision's SBOM
 - 5.3. Utilizing Hanwha Vision's SBOM
- 6. Conclusion**
- 7. Reference #A**

1. Introduction

Hanwha Vision's Wisenet SoC (System on a Chip) has continuously evolved by incorporating new technologies to strengthen product security. Cameras equipped with the latest Wisenet 9 SoC demonstrate an enhanced focus on product security, development process security, data security, and supply chain security, further boosting customer confidence in Hanwha Vision's video surveillance solutions.



Enhancing product security demands a proactive commitment to robust security standards and security processes. Among many global standards, Hanwha Vision has strategically chosen **ETSI EN 303 645**, a widely respected industry security standard for Internet of Things (IoT) devices. This enables independent third-party validation of our security certifications. This document outlines the importance of product security and details Hanwha Vision's approach to meeting the core requirements of ETSI EN 303 645.

Hanwha Vision wanted to obtain official verification of the security of our development process as well, which has been upgraded over a long period of time. So, we pursued **ISA/IEC 62443-4-1 certification** which provides guidance on how to design, develop, test, and maintain security features, even though we already have ISO/IEC 27001 certification related to information security.

Protecting sensitive data starts with systematically identifying the assets and data that require safeguarding, followed by developing technical solutions to secure them. To add a crucial layer of protection, we employ Secure Storage with a Root of Trust (RoT), enabled by a **Secure Element certified to the FIPS 140-3 standard**. This document further explores the use cases and scenarios for Hanwha Vision's Secure Element and strategies to minimize the impact of security incidents.



In today's development and distribution, the security and transparency of the software supply chain have become increasingly vital. **A Software Bill of Materials (SBOM)**, which clearly documents and manages software components, plays a key role in addressing security vulnerabilities, maintaining operational efficiency, ensuring compliance with open-source licenses, and preventing software supply chain attacks. This document highlights the key benefits of an SBOM and shows how it significantly enhances software security and management efficiency.

2. Compliance with ETSI EN 303 645 Standard

Hanwha Vision has implemented the requirements of the EN 303 645 standard in its Wisenet 9 products. This international security standard, developed by the European Telecommunications Standards Institute (ETSI), is designed to enhance the cybersecurity of IoT devices. By ensuring that Hanwha Vision's products powered by Wisenet 9 comply with this standard, our customers can trust the platform's cybersecurity.

2.1. Overview of ETSI EN 303 645

This ETSI EN 303 645 standard, initially established in the European Union (EU), has been widely adopted as a security requirement for IoT devices in European and Asian countries, including Germany (BSI/IT Security Label), the UK (PSTI Act), and Singapore (Cybersecurity Labeling Scheme Tier 1 and 2). It is also currently under consideration for adoption in other regions, such as Japan (JC-STAR1) and within the EU Cyber Resilience Act.

To assist stakeholders in understanding, testing, and implementing its security requirements, the ETSI EN 303 645 standard provides the following three documents:

- Security Baseline Requirements: ETSI EN 303 645 V2.1.1 (2020-06)
- Conformance Assessment Methodology: ETSI TS 103 701 V1.1.1 (2021-08)
- Guidance on Implementation: ETSI TR 103 621 V1.1.1 (2022-03)

Hanwha Vision has prior experience with the UL 2900-2-3 standard, a U.S.-based software cybersecurity certification for network-connectable products, applied to Wisenet 7 products. The UL 2900-2-3 standard is adopted by the American National Standards Institute (ANSI) and the National Standard of Canada (NSC).

The UL 2900-2-3 standard is more focused on testing for the presence of vulnerabilities, software weaknesses, and malware, as well as the presence of security risk controls in the architecture and design. The standard also required penetration testing to be performed on the products.

The ETSI EN 303 645 is more focused on tests for protecting customers' personal data. The standard also requires manufacturers to provide customers who use their products/services with choices regarding personal data. This includes providing the option to consent to data collection, allowing users to withdraw consent at any time, and explaining the purpose of data collection and its intended use, as shown in Reference #A.

In spite of these differences, both standards require a vulnerability disclosure policy, ongoing vulnerability monitoring, identification, and remediation activities, secure authentication and authorization, secure communication, secure boot, secure update, and protection mechanisms for external interfaces and services.



2.2. Key aspects of ETSI EN 303 645

- **No Universal Default Passwords:** Security cameras should not have pre-set passwords that are the same for all devices, which makes them easier to hack.
- **Secure Communications:** Cameras should use secure communication protocols for transmitting video and data, thereby preventing unauthorized interception and unauthorized data manipulation.
- **Vulnerability Management:** Manufacturers should have a process in place to address and report vulnerabilities discovered in their cameras.
- **Data Privacy:** Cameras should have features to protect personal and sensitive data from unauthorized access, misuse, or leakage. Also, it should provide instructions and confirmation that the data has been deleted clearly.
- **Regular Software Updates:** Manufacturers should provide regular software updates to ensure that the devices remain protected against emerging vulnerabilities throughout their lifecycle.
- **Secure Storage:** Manufacturers should provide means for securely storing crucial information, such as cryptographic keys, user passwords, and unique device ID.

2.3. Certified Secure Products

Hanwha Vision Wisenet 9 products are built on our deep expertise, developed through meeting diverse security requirements, customer demands, and industry standards. We remain committed to monitoring market trends, anticipating customer needs, and upholding industry-lead security standards to deliver superior products.

3. Compliance with IEC 62443-4-1 Standard

Hanwha Vision complies with the IEC 62443-4-1 standard requirements throughout the security development process of its products, including Wisenet 9 products, and will be able to inform customers of its compliance activities through obtaining this certification.

3.1. Overview of IEC 62443-4-1

IEC 62443-4-1 is an international standard that specifies security development lifecycle (SDL) requirements for Industrial Automation and Control Systems (IACS). Increasingly, customers in surveillance camera sectors, such as those for European ships, distribution, and railways, also demand compliance with this standard, leading to a rising need for certification.

This standard systematically reflects security in the product development process, including hardware, software, and firmware, and requires development organizations to implement security processes and design products with security inherently built-in.

3.2. Summary of IEC 62443-4-1

The IEC 62443-4-1 standard's requirements are organized into eight major process areas, containing a total of 47 requirements. The summary of each process area and major requirements is as follows:

[Table 1] Summary of IEC 62443-4-1 requirements

Process area	Major requirements
Security management (13 requirements)	Establish security policies & procedures, Define security roles & responsibilities
	Operate security education & awareness programs
	Manage security requirements and risks
Security requirements specification (5 requirements)	Identify security requirements, then document, review, approve, and track them
Security design (4 requirements)	Apply security design principles & design security architecture
	Perform security design review, verification, tracking, and risk analysis
Security implementation (2 requirements)	Apply secure coding standards and conduct code review
	Use static analysis tools

Security verification & validation testing (5 requirements)	Test for security requirements, threat mitigation, vulnerability, and penetration
Managing security-related issues (6 requirements)	Report, review, evaluate, resolve, and publicize security issues Periodic review of security flaw management practices
Manage security updates (5 requirements)	Provide security updates and documentation
Security guidelines (7 requirements)	Provide product protection and security enhancement (disposal/operation) guide

By complying with this standard, Hanwha Vision has demonstrated that it has an environment and process for improving development reliability and creating secure products. Hanwha Vision ensures its products meet high cybersecurity standards by incorporating robust security processes that include identifying requirements, designing and implementing security features, reviewing and managing security issues, and distributing firmware and documentation to resolve issues.

3.3. Certified Secure Development Process

By complying with the IEC 62443-4-1 standard, Hanwha Vision is officially certified as having a product development organization with an SDL process that meets this international standard. This certification ensures the reliability of Hanwha Vision's products developed through these processes. Hanwha Vision will continue to strengthen its development process to strengthen security management throughout the product lifecycle, fulfilling its commitment to trust and responsibility, and providing superior services in the global market.

4. Implementing Secure Element for Secure Storage

Secure Storage is an essential technology designed to safely store sensitive data and protect it from unauthorized access or data leakage.

Hanwha Vision initially developed the Hanwha Trusted Platform Module (HTPM), starting with the Wisenet 7 SoC, and a TPM module independent of the SoC to implement Secure Storage in its high-end products. Building on this extensive experience, Hanwha Vision has now implemented its first hardware Secure Element, certified to the latest version of the FIPS 140-3, Level 3 standard, in the Wisenet 9 products. This Secure Element allows Hanwha Vision IP cameras to provide a secure vault for the storage of sensitive data.

4.1. FIPS 140-3 Certification

FIPS 140-3 is an international standard that provides reliability in the global market for evaluating the security of cryptographic modules such as Secure Storage. Compared to FIPS 140-2, FIPS 140-3 introduces significant enhancements and strengthens security requirements across various areas, as described below.

- **Integration of ISO/IEC 19790 and ISO/IEC 24759:** FIPS 140-3 is based on the ISO/IEC 19790 (Security Requirements for Cryptographic Modules) and ISO/IEC 24759 (Test Requirements for Cryptographic Modules) standards. This enhances compliance with international standards.
- **Module Type Classification:** Evaluation criteria have been refined through the precise classification of cryptographic modules into hardware, software, firmware, and hybrid module types.
- **Software / Firmware Security:** The standard now includes explicit definitions for Software and Firmware integrity verification methods. Level 2 recognizes both digital signature-based and message authentication code-based integrity, while Level 3 only recognizes digital signature-based integrity.
- **Self-Tests:** The encryption module must perform pre-operational self-tests before operation and perform conditional self-tests when providing specific functions.
- **Life-Cycle Assurance:** Comprehensive security requirements have been introduced to cover the entire lifecycle of the encryption module, spanning from design, development, deployment, to decommissioning.

4.2. Security Level of FIPS 140-3

FIPS 140-3 categorizes cryptographic modules into four progressive levels (Level 1 to Level 4), each characterized by increasing rigor in its security requirement. The Secure Element, which Hanwha Vision uses, is designed to achieve Level 3. This level offers enhanced security compared to Level 2 in critical areas such as:

- Roles / Services / Authentication
- Software / Firmware Security
- Physical Security
- Non-Invasive Security
- Security Parameter Management
- Life-Cycle Assurance

[Table 2] FIPS 140-3 Summary¹

Requirement Area		Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification		Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces		Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication		Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security		Approved integrity technique, or EDC based integrity test. Defined SPMI, HPFI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test	
Operational Environment		Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security		Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security		Module is designed to mitigate against non-invasive attacks specified in Annex "F".			
		Documentation and effectiveness of mitigation techniques specified in Annex "F"		Mitigation testing	Mitigation testing
Security Parameter Management		Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
		Automated SSP transport or SSP agreement using approved methods			
		Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests		Pre-operational: software/firmware integrity, bypass, and critical functions test			
		Conditional: cryptographic algorithm, pair-wise consistency, SWFW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance	Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
	Design	Module designed to allow testing of all provided security related services			
	FSM	Finite State Model			
	Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation associated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
	Testing	Functional testing		Low-level testing	
	Delivery & Operation	Initialization procedures	Delivery procedures		Operator authentication using vendor provided authentication information
	Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks		Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

¹ This table was prepared with reference to <https://lightshipsec.com/fips-140-3-is-here/>



Briefly, the security requirements by level are summarized as follows:

- **Level 1:** This is the lowest security level, requiring basic encryption and key management capabilities, suitable for software-only modules.
- **Level 2:** This level introduces physical security measures to guard against unauthorized access and detect physical tampering (e.g., locks, tamper-evident stickers), with role-based authentication.
- **Level 3 (Applied to Secure Element which is used in Hanwha Vision):** This demands a higher level of physical security. It requires anti-tampering resistance to detect physical intrusion attempts, identity-based authentication, and protection against environmental attacks, including temperature and voltage fluctuations.
- **Level 4:** As the highest security level, it focuses on preventing highly sophisticated attacks, with tamper-active features, multi-factor authentication, and the ability to erase sensitive data upon detecting environmental attacks or fault injections.

4.3. Use Cases and Scenarios of the Secure Element

End-users typically don't need to understand the detailed use cases of the Secure Element built into their devices. However, it is the manufacturer's responsibility to account for these considerations to ensure strong cybersecurity throughout the product. Security features must be designed to protect users without adding complexity or inconvenience.

As a responsible manufacturer, Hanwha Vision has proactively identified sensitive data—such as cryptographic keys and user-defined passwords—that require protection. The table below outlines these data categories in more detail.

One of the best practices for protecting sensitive data is encrypting it while it is stored in the device (data at rest). However, the encryption keys themselves must also be securely protected. To address this, the most effective solution is to store and manage sensitive data using a Secure Element embedded in the device.

[Table 3] Type of Sensitive Data

Category	Sensitive Data
User-defined passwords	Login for Device access
	SMTP/FTP/NAS'S server access
User-defined cryptographic keys	Private keys/Certificates for 802.1x access
	Private keys/Certificates for HTTPS/TLS
	CA Certificates for Authenticity of 802.1x Authentication server
Manufacturer-defined cryptographic keys	Private keys/Certificates for HTTPS/TLS, device authentication
	Public keys for Verifying Secure Boot/Signed Firmware
	CA Certificates for Authenticity of Open Platform App
	CA Certificates for Authenticity of Mutual authentication
	Secret keys for Backup/Restore

Hanwha Vision's Secure Element encrypts sensitive data on a per-device basis using a unique symmetric key generated during manufacturing. While this key is protected by a FIPS 140-3 Level 3 certified Secure Element—making any exposure extremely unlikely—even in the rare event of a leak, it would only affect that specific device. This isolation greatly limits the impact of any potential security incident and minimizes overall risk.

5. Enhancing Software Supply Chain Security

Hanwha Vision has initiated the distribution of a Software Bill of Materials (SBOM) for its new software platform, beginning with the Wisenet 9 product line.

5.1. Introduction of SBOM

An SBOM (Software Bill of Materials) is a detailed list of all software components, clearly identifying every open-source and third-party library that makes up a software product. These components can be introduced into the development repository from multiple sources, which may unintentionally bring known open-source vulnerabilities into the product.

For this reason, managing open-source vulnerabilities has become a crucial part of software supply chain security, with the SBOM playing a key role in enabling effective control. Managing and maintaining an SBOM improves the transparency and security of the software supply chain, providing benefits such as:

- **Improving Software Transparency and Reliability:** Modern software relies heavily on open-source and third-party libraries. An SBOM clearly lists all components included in the software, enabling quick identification of those with security vulnerabilities (CVEs) or malicious code. This enhances the reliability of the software supply chain, builds trust, and offers greater transparency to customers and users.
Example: When a security issue such as the Log4j vulnerability (Log4Shell, 2021) occurs, an SBOM can be used to quickly identify and respond to any software that includes the affected library.
- **Meeting Regulatory Compliance and Industry Standard:** Many countries now require the use of an SBOM for regulatory compliance.
Example: Under U.S. Executive Order 14028 (2021), software vendors contracting with the federal government must provide an SBOM. Using an SBOM to verify compliance with standards can also prevent legal issues related to software license violations.
Example: An SBOM is a crucial factor in the industry standard ISO/IEC 5230 [Standard for License Compliance of Open Source Software based on the Linux Foundation OpenChain Specification].
- **Vulnerability Management and Security Incident Response:** By including version information of software components, an SBOM enables customers to quickly identify security vulnerabilities by comparing them against the Common Vulnerability Index (CVE). In the event of a security incident, the SBOM helps customers promptly identify and respond to affected software.
- **Efficient Software Maintenance:** An SBOM helps both customers and manufacturers systematically manage information about software components,

making it easier to carry out maintenance tasks like updating outdated components or removing deprecated ones.

- **Open-Source License Compliance:** An SBOM ensures license compliance by clearly documenting the open-source libraries and their associated licenses included in the products. This helps manufacturers meet the requirements of licenses such as GPL, Apache, and MIT.
- **Preventing Software Supply Chain Attacks:** With the recent rise in software supply chain attacks (e.g., the SolarWinds, Log4j, and Kaseya incidents), an SBOM plays a critical role in identifying and preventing vulnerabilities throughout the supply chain. It helps track the origin of software components and remove untrusted components.

5.2. Features of Hanwha Vision's SBOM

Hanwha Vision has published its SBOM to help customers easily access and manage essential information. This includes the name and version of open-source software components, their origin, functional descriptions, licenses, copyright holders, Common Platform Enumeration (CPE), Package URL (purl), and vulnerability patch details.



Figure 1.1: XNV-A9084R's published SBOM in Hanwha Vision website

Hanwha Vision's commitment goes beyond simply providing an SBOM. We are also dedicated to proactively addressing known open-source vulnerabilities through regular firmware updates, in line with each product's Long-Term Firmware Support Policy.

- The SBOM is available for products running a firmware version 24.00.00 or later.
- Hanwha Vision's SBOM uses Cyclone DX format, a standard led by the Open Web Application Security Project (OWASP, <https://owasp.org/>), and is provided as a .JSON files.
- The SBOM Utility or viewer can be used to easily view and search the contents.

5.3. Utilizing Hanwha Vision's SBOM



Here's how customers can effectively use Hanwha Vision's SBOM to strengthen security and streamline software component management:

- 1. Vulnerability Impact Assessment:** If customers want to check whether their product is affected by a known CVE (Common Vulnerabilities and Exposures) in a specific open-source software, they can refer to the product-specific SBOM provided by the vendor. This allows them to quickly identify which open-source software and versions are impacted - often without needing to contact the vendor directly.
- 2. Patch Verification:** If an affected version is identified, customers should consult the SBOM for available vulnerability patch (pedigree) information. In some cases, security patches for CVEs may be backported to older versions, meaning the specific version in use may not actually be vulnerable.
- 3. Manufacturer Consultation for Undetermined Impact:** If a vulnerability patch is not listed in the SBOM, it may mean that the vulnerable code was not included by the compiler during the build time or that the vulnerability is not exposed externally. In such cases, customers should contact the manufacturer to confirm whether their product is actually affected.
- 4. Software Update Request:** If an actual impact is confirmed, customers can ask the manufacturer to update or patch the affected open-source software. For discontinued models, support will depend on the applicability and duration of the Long-Term Firmware Support Policy.

[For more information, please refer to the **Long-Term Firmware Support Policy** document].



6. Conclusion

Product security goes beyond just preventing product vulnerabilities; it also encompasses managing supply chain security for software components, securing development environments and personnel, and protecting the data stored and processed within the product.

Understanding how security vulnerabilities arise highlights why a comprehensive range of protective measures is essential. Vulnerabilities can be introduced at any stage—from product planning and design to implementation, distribution, and even operation. While proactively eliminating these vulnerabilities is ideal to reduce costs, it is often difficult in practice. Therefore, it's crucial to have a development and vulnerability response process that enables rapid action when new vulnerabilities are discovered in the wild. Global security standards mandate such controls, and Hanwha Vision is committed to continuously integrating these requirements into its products and development processes to deliver superior solutions.

Hanwha Vision will continue its proactive security efforts, including conducting penetration tests to identify product vulnerabilities, running internal bug bounty programs for developers, and performing thorough security reviews. As a dedicated CVE Numbering Authority (CNA), we remain faithful to our role in identifying and disclosing vulnerabilities. With a trusted supply chain and an unwavering focus on cybersecurity, Hanwha Vision stands as a leader in world-class video surveillance manufacturing.

7. Reference #A

- [5.11-1] Providing a function to easily delete user information.
 - ※ User information: password, key, environment configuration information, personal information, etc.
- [5.11-2] Providing a function to easily remove personal information stored in related services
 - ※ Case only when the user's personal information (account information, video, etc.) is stored in a cloud service connected to the device
- [5.11-3] Providing concise and accurate user documentation on how to delete personal information.
 - ※ Case only when personal information is stored.
- [5.11-4] Providing clear confirmation and successful completion messages for all deletion functions that the personal information has been deleted.
 - ※ Case only when personal information is stored.
- [6-1] Providing transparent information on personal information processing.
 - ※ Personal information list, purpose/method/subject of use, etc.
 - ※ Case only when personal data is processed.
- [6-2] Obtaining customer's consent for personal information processing.
 - ※ Customer's consent must be obtained in a valid manner.
 - ※ Case only when personal information is processed based on the customer's consent.
- [6-3] Providing customers with the right to withdraw consent to personal information processing at any time.
 - ※ Case only when personal information is processed based on the customer's consent.
- [6-4] Personal information processing must be kept to the minimum necessary for the intended function.
 - ※ Case only when telemetry data is collected.
- [6-5] Providing customers with information on telemetry data.
 - ※ List of telemetry data, purpose/method/subject of use, etc.
 - ※ Case only when telemetry data is collected.

Hanwha Vision

13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
www.HanwhaVision.com

Copyright © 2025 Hanwha Vision. All rights reserved.

