# USNC CURRENT

Vol. 19, No. 1 - Winter 2024

# CYBERSECURITY

United States National Committee of the IEC

Published by the U.S. National Committee of the IEC, a committee of the American National Standards Institute

# CYBERSECURITY

## FEATURED STORIES



## IN THIS ISSUE

# THE HOME ELECTRONIC SYSTEM (HES) FAMILY OF STANDARDS

*Dr. Kenneth Wacks – Deputy Technical Advisor; ISO/IEC JTC1/SC25/WG1 TAG Convener, ISO/IEC JTC1/SC25/WG1*


The international standards working group ISO/IEC JTC 1/SC 25/WG 1, responsible for the Home Electronic System (HES), develops IoT-related (Internet of Things) standards for communication networks and interfaces. These standards enable the interconnection of electrical and electronic equipment and products for homes and small buildings. The primary markets for WG 1 standards are creators, manufacturers, and installers of these products and related services.

The HES comprises a family of standards that enable home and building occupants to:

- live more comfortably at home,
- be more protected and feel safe at home,
- work productively in smart buildings, and
- live and work more economically with minimal environmental impact by reducing energy consumption and/or producing and storing or selling excess energy.

Applications of products and services based on HES standards include entertainment, lighting, comfort control, life safety, health, and energy management. Energy management has become important with the evolution of distributed energy resources (DER: solar panels, wind turbines, and storage batteries) for installation at homes and buildings, possibly interconnected with smart grids to access public power. Energy efficiency, reliability, resiliency, and reduction of greenhouse gases to mitigate climate change are topics of global interest. SC 25/WG 1 develops standards supporting energy management for appliances and electric vehicle chargers within homes and small buildings.

## THE HES GATEWAY

A communications interface between a wide area network (WAN), such the Internet, and a local area network (LAN), used in homes and buildings, is called a gateway. A LAN in a house is often called a HAN: Home Area Network. This term is used in the ISO/IEC 15045 HES gateway series and in this article. The ISO/IEC 15045 series of international standards specifying the HES gateway extends the conventional

communications gateway with some unique features. All the HES gateway standards were proposed and managed by the U.S.

## HES GATEWAY FEATURES

The HES gateway links a WAN outside the home or building with a HAN to provide traditional gateway communication services, plus much more. The HES gateway provides these additional services:

- Support for multiple HANs
- Support for cybersecurity protection
- Support for applications
- Support for interconnected gateways
- Support for interoperability among competing products

As home automation evolved from a hobby to an industry, there were attempts nationally and internationally to create standards for a uniform communications infrastructure to interconnect devices such as sensors, actuators, controllers, and user interfaces. These standards were completed and were technically sound; however, they were not adopted. Instead the market fragmented into specialized networks, such as KNX, LonTalk, Wi-Fi, Zigbee, Z-Wave, etc. With this reality, HES focuses on enabling interoperability among disparate HANs and devices using these HANs.

## THE HES GATEWAY STRUCTURE

Figure 1 shows the functional components of a generic HES gateway.[1] The various interface cards are specialized for each WAN and HAN to translate messages

1 ISO/IEC 15045-1, *Information Technology – Home Electronic System (HES) Gateway – Part 1 A Residential gateway model for HES*
ISO/IEC 15045-2, *Information Technology – Home Electronic System (HES) Gateway – Part 2: Modularity and protocol*
ISO/IEC 15045 Parts 1 and 2 are published; the other parts cited are in development.

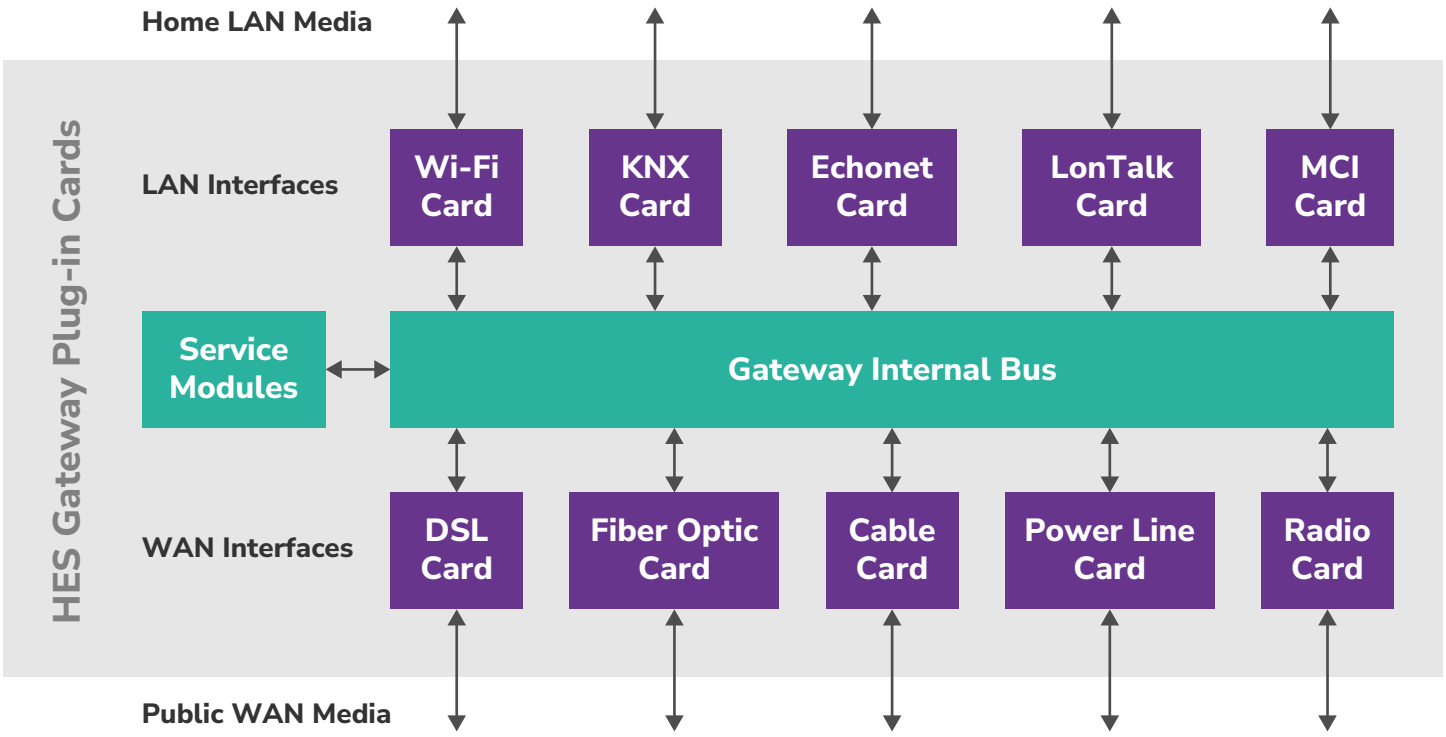


*Figure 1: HES Gateway structure*

using an HES gateway feature called the Interworking Function. The core functionality of the HES gateway is embodied in service modules. A service module contains instructions for processing service data to implement protocol translation, cybersecurity protections, applications, and any other responsibilities assigned to the HES gateway.

Standards are developed to provide specifications for models, architectures, interfaces, and communication protocols while offering flexibility for manufacturers to create significant product differences. Manufacturers can differentiate their HES gateway offerings from competitors by choosing, for example:

» Which HES gateway functions to include from among the options in the standards

» Whether to package the HES gateway with other consumer electronics

» The user interface for the consumer or installer to configure the HES gateway

These standards encourage a diverse market for HES gateway products. ISO/IEC 15045-4-1[2] and subsequent parts[3] specify classes of HES gateway configurations that range in capabilities and complexity.

The primary function of the gateway is a communications interface. Some commercial home automation systems are being developed around a platform that acts as a communications hub and a host for controlling applications. The HES gateway includes the option for embedding Service Modules that support applications, so the HES gateway can be configured as a platform both for communications and for applications. Applications such as energy management could be hosted by the HES gateway, as specified in ISO/IEC 15045-5-1[4] and ISO/IEC 15045-5-2.[5]

## HES GATEWAY CYBERSECURITY

The ISO/IEC 15045-3 series specifies features for an HES gateway to provide cybersecurity services for homes and buildings. These services are intended to protect user data, privacy, and safety. Data protection is a growing challenge as devices are designed with access to Internet services. Such access makes these devices targets for data theft, reprogramming to create mayhem, and launching platforms for malware bots (Internet robots) that attack other devices.

## THE HES DEVICE REGISTRY

With the proliferation of non-wired networks such as radio, infrared (typically used in remote control units), and power-line carrier, it is easy to insert rogue devices into a home network. Therefore, the HES gateway can include a registry of legitimate devices. The gateway validates cybersecurity certificates presented by attached devices to determine if the device belongs on this network. A certificate is a digital message to verify that a device was provided by a known company and operates according to agreed rules. It is analogous to a driver's license issued by the government attesting that the holder has demonstrated driving competency.

After the device certificate is validated, the gateway can then establish a secure link with the device and an

2 ISO/IEC 15045-4-1, I*nformation Technology – Home Electronic System (HES) Gateway – Part 4-1: HES gateway structural class and module requirements*

3 ISO/IEC 15045-4-2, *Information Technology – Home Electronic System (HES) Gateway – Part 4-2: Simple HES gateway*
ISO/IEC 15045-4-3, *Information Technology – Home Electronic System (HES) Gateway – Part 4-3: Complex integral HES gateway*
ISO/IEC 15045-4-4, *Information Technology – Home Electronic System (HES) Gateway – Part 4-4: Complex modular HES gateway*
ISO/IEC 15045-4-5, *Information Technology – Home Electronic System (HES) Gateway – Part 4-5: Interconnected HES gateways*

4 ISO/IEC 15045-5-1, *Information Technology – Home Electronic System (HES) – HES gateway, Application services, Part 5-1: Overview, foundation, and requirements*

5 ISO/IEC 15045-5-2, *Information Technology – Home Electronic System (HES) – HES gateway, Application services, Part 5-2: Energy management and measuring application (EMMA)*

application controller by distributing encryption keys. Since the device certificate registry is maintained in the HES gateway, a loss of external communications would not impact cybersecurity, as would a cloud-based security service.

## HES MESSAGE SERVER SCREENING

The HES gateway has the option of examining message headers to determine if local devices are communicating with the intended cloud-based servers. To accomplish this, the HES gateway maintains a list of servers with which each local application could be communicating for accessing remote services. Users would be warned of attempts to reach unauthorized servers.

## HES PRIVACY AND SAFETY PROTECTION

The HES gateway supports an optional feature that screens data traffic for compliance with policies intended to protect consumer privacy. Also, appliance control messages impacting safety might be screened and blocked by the same mechanism.

Figure 2 illustrates the elements in the gateway for protection of Premises and Personally Identifiable Information (PPII, explained in the next section) and safety. The "CS, PPII & Safety Controller" block in Figure 2 contains the rules about which data flows are allowed and which are blocked. The "CS, PPII & Safety Processor" block enforces these rules by filtering the data to allow or block transmission.

For example, using a smart phone app when away from home to start a burner on a cooktop could be dangerous unless someone is at home to check that the appropriate pot with food is in place and nothing flammable is nearby. The HES gateway safety service modules could be programmed to screen remote control commands sent to such appliances. The functions of screening and filtering data extend the mission of the gateway to provide "data sentry" services for cybersecurity protections of customer data, privacy, and safety.

Privacy policies have focused on protecting PII such as name, address, government-issued identification

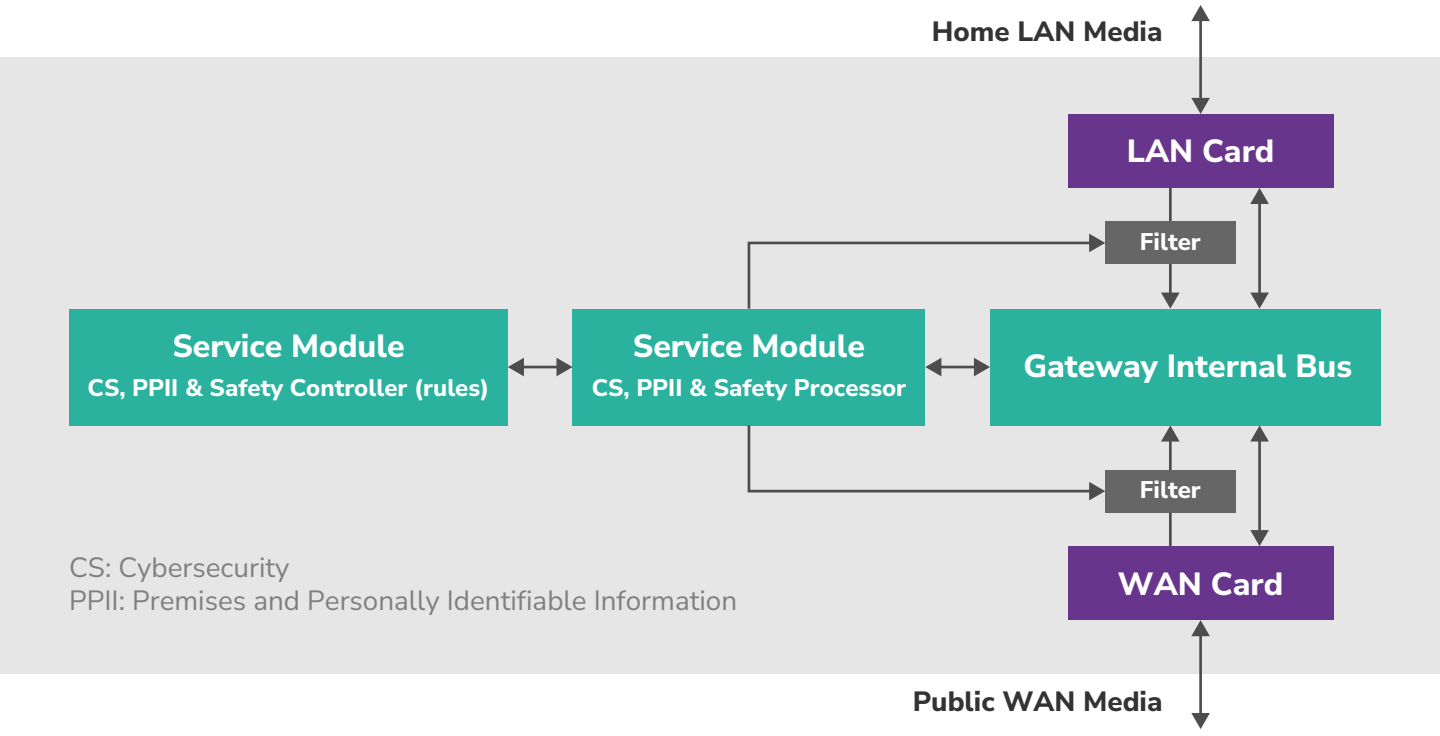


*Figure 2: Gateway Service Modules*

numbers, facial photos, etc. ISO/IEC 29100[6] specifies a privacy framework for enterprise-level information technology (IT). This framework defines common privacy terminology, the elements that control and process PII, considerations for safeguarding privacy, and references to privacy principles that apply to IT. The scope of ISO/IEC 29100 states that these PII standards apply "to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII."

The HES gateway ISOIEC 15045-3[7] series extends the enterprise privacy framework from persons to devices by introducing the term PPII to incorporate devices and persons. The data sentry screening functions are intended to:

- Prevent active inbound attacks and unsafe commands.
- Discover and classify outbound traffic.
- Mediate network traffic within homes and buildings.
- Manage mechanisms for privacy and security.
- Develop a dashboard for reporting gateway activities and status to a non-technical end user.

## HES GATEWAY DATA SCREENING

For the gateway technology to enforce privacy and safety provisions, all messages to and from devices must be checked by the gateway for compliance with the provisions of the privacy contract. The gateway scans and filters messages in real-time as the messages pass through the gateway.

For data not needed in real time, the gateway might function as a repository where these data are buffered. For example, a thermostat could register with the gateway and be allocated storage of a specified number of readings. The remote user with appropriate permission to access this repository would then retrieve these temperature readings from the gateway.

A gateway hardened against unintended data flows is effective if the gateway is the sole data pipe into the home. However, mobile (cellular) operators are planning communication protocols to transport IoT (Internet of Things) data. As mobile data transmission becomes cheaper, it is possible that manufacturers might install mobile phone data transceivers inside appliances and IoT devices to report on usage and performance without informing the customer. For HES compliance, messages to be sent via such a mobile interface are pre-screened by the HES gateway to enable customer cybersecurity protection.

## CYBERSECURITY PROTECTION MANDATES AND PREFERENCES

The HES gateway cybersecurity services can provide protection for customer's data, privacy, and safety. This is important for energy data and applications since energy consumption patterns can reveal who is home, when they are home, and what they are doing.

We may be at a confluence of social, political, and technical events that make standards and technology specifications for privacy timely. Consumers are becoming aware that personal data can be misused. In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) became law. It protects the personal data, such as names, addresses, photos, and voice recordings, of all EU residents, regardless of where the data are processed. Explicit consent is required before processing personal data for one or more specific purposes.

6 ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

7 ISO/IEC 15045-3-1, *Information Technology – Home Electronic System (HES) gateway – Part 3-1: Introduction to privacy, security, and safety*
ISO/IEC 15045-3-2, *Information Technology – Home Electronic System (HES) gateway – Part 3-2: Privacy framework*

Market studies have shown that privacy concerns are impacting the sale of connected home products. Parks Associates, a market research firm that tracks home systems, surveys 10,000 broadband households periodically for "Smart Home Device Inhibitors." Privacy concerns have consistently ranked third after device costs and benefits for 2020 through 2022. More than 30% of those surveyed agreed, “I have data privacy and security concerns about having smart devices in my home.” [These survey results were provided courtesy of Parks Associates by president and chief marketing officer Elizabeth Parks in 2023.]

Privacy is no longer just an abstract concept, but can be enabled with appropriate policies, technology, and products. Consumers need products with technology that can protect privacy. The HES gateway ISO/IEC 15045-3 series specifies technology that allows consumers and service providers to choose and enforce privacy options. It is now up to designers and manufacturers to incorporate privacy technology into products and service providers to offer privacy choices with opt-in provisions. Building in privacy protection during product design is less costly for manufacturers than fixing problems later and compensating customers for cybersecurity breaches.