61/6124/INF

For IEC use only

2020-09-04

INTERNATIONAL ELECTROTECHNICAL COMMISSION

TECHNICAL COMMITTEE NO. 61: SAFETY OF HOUSEHOLD AND SIMILAR ELECTRICAL APPLIANCES

Guidance document concerning the safety of appliances communicating remotely through public networks

---

This guidance document concerning the safety of appliances communicating remotely through public networks was developed by TC 61/MT 23. It is intended to provide supporting information for the users of 60335-1 6th Edition, to understand the requirements concerning appliances to be connected to a public network and their application, and in the specifics regarding clause 22.62 and new Annex U.

This document was originally circulated as 61/5761/DC and was later updated as 61/5761A/DC. The comments received to 61/5761A/DC where discussed by IEC TC 61 during its meeting in Bled in June 2019 and finalized by TC 61/MT 23. The results as given in 61/5808A/INF as well as the formal update to IEC 60335-1 Ed.6.0 with respect to the referenced clause number and Annexes are included in this updated version of the guide.

Introduction:

Due to the increase of home entertainment and automation networks, smart phone and tablet adoption, and the expansion of software applications in the digital era, the demand for connected household appliances is increasing. Consumer user stories and the consumer's demand for ease of use are driving the integration of connectivity into existing industries. The ability of an appliance to connect to a public network affords many opportunities to increase the value of the appliance to the consumer over its useable lifetime. At the same time, it introduces risks that need to be addressed to ensure the benefit of being connected does not compromise product safety.

This document provides guidance on the application of IEC 60335-1 (*Household and similar electrical appliances – Safety – Part 1: General requirements*) requirements which address the ability of an appliance to be connected to a public network, to interact with other entities over a public network and to authorize the downloading and installation of its software through the public network. The IEC 60335-1 standard limits the new requirements to such appliances and applications that could impair compliance with the safety principles of the 60335-1 and its related series of Parts 2 standards.

In developing this document, MT23 took into consideration the guidance provided in IEC Guide 110, Edition 2.0: *Home Controls Systems - Guidelines Relating to Safety* and IEC Guide 120, Edition 1.0: *Security Aspects - Guidelines for their inclusion in publications.* In addition to these publications, consideration is also given to main points raised during the discussions held at the TC61 meetings in Toronto (June 2017), Wellington (May 2018) and Bled (June 2019).

The exchange of data or the download and installation of software, which is provided from the manufacturer or its trusted third parties via remote communication through a public network, should be protected. The typical safety assessment of hardware random fault analysis and software systematic failures should be extended to include intentional threats such as hacking

and the manipulation of data, which are typically covered under the ‘Information Security’ series of standards.

Relationship between traditional Product Safety and Information Security standards

The requirements of Annex U have been developed to address the safety related risks associated with IoT (Internet of Things) technologies, while maintaining an all-encompassing standard for the evaluation of safety of household appliances. Figure 1 below illustrates the intersection of the technical committees JTC1 and TC61.

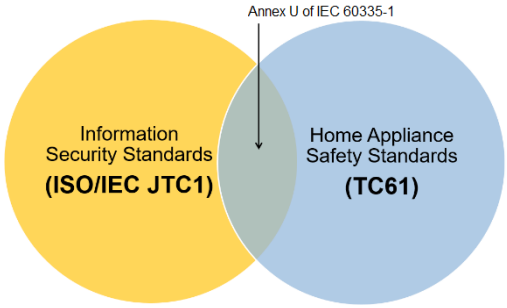


Figure 1 – Relationship between Information Security Standards and Home Appliance Safety Standards

The work and publications of sub-committees JTC1/SC27 (security techniques) and JTC1/SC41 (Internet of things and related technologies) are of particular importance and should be monitored to ensure the requirements in Annex U remain state of the art. As the information security standards bubble illustrates, there are additional requirements pertaining to information security that do not affect the safety of household appliances, which warrants the creation of Annex U as opposed to requiring additional compliance with all of the ISO/IEC JTC1 suite of standards.

Security Goals of Information Security:

The requirements of Annex U ensure the integrity and authenticity of remote communications between appliances and server software applications, is designed to prevent eavesdropping, tampering, or message forgery, it happens only through trusted/verified sources and the messages are received as sent. Refer to Figure 2 which illustrates the security goals of the fundamental Information Security Model.

a. **Availability**: property of being accessible and usable upon demand by an authorized entity

b. **Integrity:** property of accuracy and completeness

c. **Authenticity:** property that an entity is what it claims to be

d. **Non-Repudiation**: ability to prove the occurrence of a claimed event or action and its originating entities

e. **Confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Figure 2 – Security goals of the fundamental Information Security Model. Only b. and c. are relevant for Product Safety

The requirements of Annex U, however, do not specifically address confidentiality of data or consumer privacy, commonly referred to as 'Data Protection'; or the tracing and logging of events. 'Data Protection' is a very critical aspect concerning consumer protection and legal compliance but does not directly affect product safety. Reference should be made to national laws governing 'Data Protection', which are out of the scope of IEC 60335-1 and its series of standards. Furthermore, as required in subclause U.3.6, the requirements of Annex U also do not address the topic of availability, as it is assumed the public network will not always be available, and therefore the safe operation of the appliance cannot rely solely upon the availability of remote communications.

Considering future trends in cloud computing, the appliance should remain safe and in compliance with all requirements of the standard in case of a lost connection, latency or lower/insufficient bandwidth in the public network. Although ensuring product safety only relies upon fulfilling the security goals of integrity and authenticity, manufacturers may need to implement additional measures to ensure the reliability and performance of their digital services, as required by other non-safety related technical standards or regulations.

Requirements Development based upon the Threat Model

In developing the requirements for remote communication, IEC Guide 120 was used to evaluate which threats are applicable to household appliances and which potential attacks should be considered. The blue dotted line in Figure 3 illustrates the basis for the Annex U requirements. For further explanation for 'Planted in System', see footnote[1].

———————

[1] 'Planted in system' attacks are those in which the mechanism is loaded onto the device and from there it attacks other devices. Not all of these attacks lead to the threat of reduced integrity, which is the main security goal.
The premise is that all communications with household appliances that could affect the safety of the appliance should come from a trusted communication partner and the data packages should be protected in such a way that their integrity is guaranteed all the way to the electronic which executes the software. If the source of the software is a

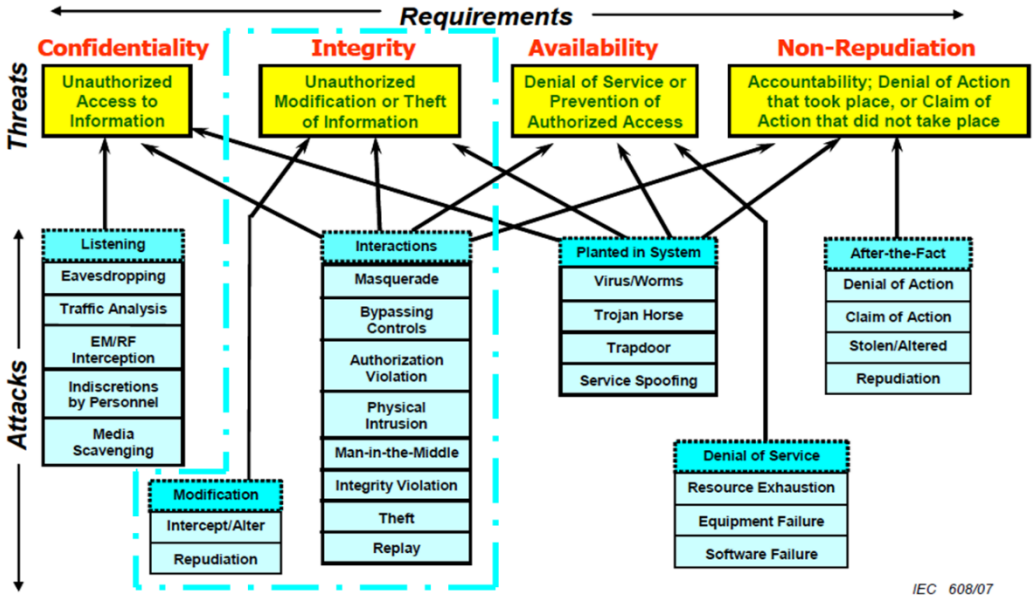


Figure 3 – Security aspects – Guidelines for their inclusion in publications (Figure 4 of IEC Guide 120)

Requirements for Appliances Capable of Remote Functionality

The general requirement for appliances [IEC 60335-1, Clause 4] is that they "shall be constructed so that in normal use, they function safely so as to cause no danger to persons or surroundings, even in the event of carelessness that may occur in normal use." The requirements in subclauses 22.40, 22.49, 22.50, 22.51 and 24.1.7 address the capability of an appliance to be connected to a telecommunication network and to be capable of remote operation. To address the threats associated with remote communication via a public network, subclause 22.62 and Annex U have been developed.

Subclause 22.62 is essential for determining whether or not the requirements in Annex U are to be applied.

22.62 ***Remote communication*** *through* ***public networks*** *shall not impair compliance with this standard.*

The requirement is only applicable to:

a) ***Remote communication*** *that includes the download of software or the transmission of data that includes:*

- measures according to normative Annex R necessary for compliance with 22.46, or

- means necessary for compliance with the clauses 8 to 32 of this standard.

_____

trusted source, the idea is that these risks are covered since a manufacturer would not release a virus for their own products. Furthermore, since the virus or Trojan would not be introduced in the first place, there is no need to consider these risks with respect to detection of a planted virus/worm/Trojan, etc.

This requirement addresses the fact that consideration should be made not only for abnormal operation implementing functional safety (including single fault conditions), but rather compliance with the entire standard should not be impaired by remote communication through a public network. Annex U addresses the threats and associated risks of remote communication through a public network so that in the case of a SW update, for example, the level of compliance of the 'new' SW would be the same as what had been installed in the appliance when manufactured and placed on the market.

The first bullet point addresses compliance with the standard and the fault condition of a programmable protective electronic circuit (PEC) as defined in clause 19 and corresponding compliance with Annex R.

The second bullet point addresses the functional/application/process SW which may impair compliance with the standard under normal conditions.

Considering in greater detail, the requirement of 22.62, a), first bullet point, Annex U would apply if software used in programmable protective electronic circuits (i.e. functional safety software) can be downloaded and installed. Furthermore, if the software algorithms are fixed, but the limits or parameter sets used by these algorithms are configurable by a set of functional safety constants, then the annex also applies. An example of a functional safety constant would be the temperature set point of an electronic thermal motor protector protecting against motor overload. If the value were to be compromised via remote communication, the safety of the appliance could be affected. Figure 4 demonstrates two scenarios where Annex U would apply.

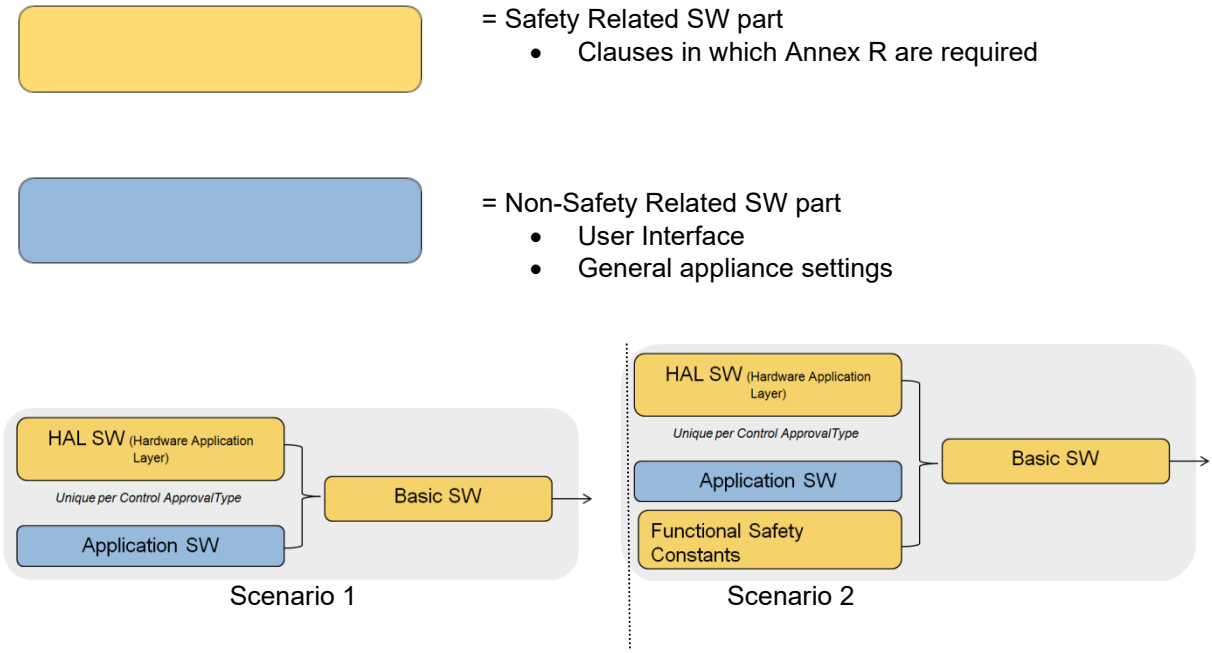


Figure 4 – Scenarios where appliance basic SW contains functional safety SW and/or functional safety constants

Considering the requirement of 22.62, a), second bullet point, Annex U would apply if software controlling normal operation, when corrupted, could impair compliance with clauses 8 to 32 of the standard. In 61/2586E/INF *Guidance on functional safety,* it is stated *'In IEC 60335-1, software controlling normal operation (Clause 11) is considered to be functional software that does not require validation.'* This statement is valid for most cases of the standard, except for the case of remote communication via public networks. Corruption of process steps, timers, constants, etc. used in the functional software could, for instance, impair compliance with the temperature rise limits of Table 3 in clause 11 for motor windings, surface temperatures, or components. An example of a process step, which could lead to a non-compliant condition, is the length of the spinning process in washing machines. If the time was manipulated such that

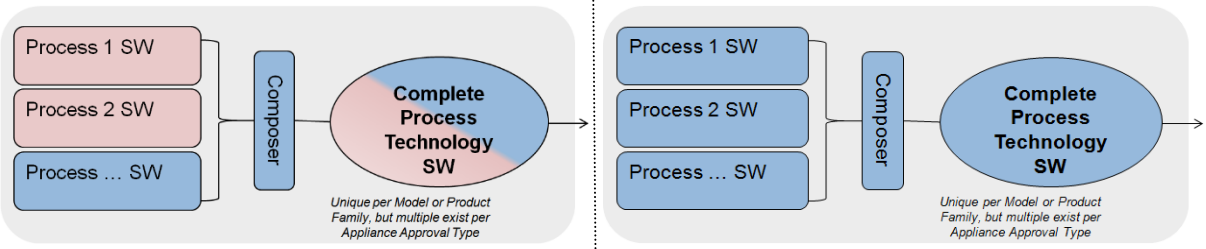
the temperature rise limits of Table 3 are no longer fulfilled, but the maximum temperature is not high enough to trigger an over temperature limiting device necessary for subclause(s) 19.7, 19.8 and 19.9, then the standard is no longer fulfilled.

= Potentially Safety Related software program part (subroutine)

- Clauses 8 to 32 (except §19.11 & §22.46, IEC 60335)

= Non-Safety Related SW parts

- User Interface
- General appliance settings



Scenario 1 - Further analysis of impact necessary - Annex U may apply

Scenario 2 - No effect upon safety - Annex U does not apply

Figure 5 – Scenarios illustrating the potential dependency upon functional software

*b) **Remote communication** that includes the download of software or the transmission of data, that only affects that part of the software that is not covered by the above case a), but where compliance with the standard may be impaired due to improper separation or partitioning from the software or data in the above case a).*

Considering the requirement of 22.62, b), the application of Annex U may also be dependent upon the SW architecture employed in the product. For many household appliances, the software programmed during production is an image file, which contains merged modules of code such that only one file is programmed to the appliance. If this is the same approach that would be used for remote software updating, then it may not be possible to avoid overwriting safety related software or data, even if these software modules or data have not been modified as part of the software update. Figure 6 illustrates a SW architecture that requires investigation to Annex U.

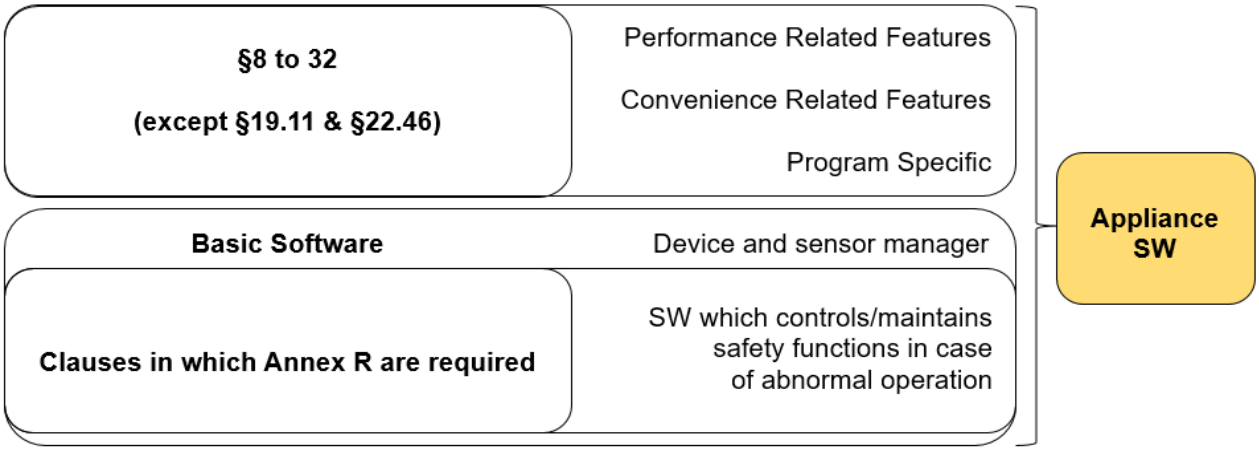


Figure 6 – Example of a merged SW file, such that SW updates would always require re-programming safety related software or data

Appliances not requiring investigation to Annex U are defined as:

- *appliances where all measures to comply with the standard are independent of software;*

  An example of such would include irons featuring an electro-mechanical bi-metal thermostat for controlling the temperature if it can be proven that surface temperatures of handles and knobs as well as adjacent surfaces are still fulfilled and not dependent upon a programmable timer.

- *appliances using remote communication through public networks for the send-only transmission of data;*

  The send-only transmission of data refers to appliances which communicate as beacons, always transmitting a defined set of data at defined intervals. An example of this would be a remote weather station which sends temperature and humidity values every minute.

- *appliances which only provide event driven messages or push remote monitoring.*

  Although this dashed item is very similar to the previous dashed item, it differs in the aspect of ‘transmission on demand’. Event driven messages are messages which are sent based upon the fulfilment of a predetermined task or a change in appliance state, such as automatic notifications that the dishwashing cycle has been completed, or the oven is preheated. Push remote monitoring refers to an active request for information from the appliance, such as program remaining time, fill level of rinse aid in dishwashers, or actual cavity temperature of ovens.

For appliances providing only event driven or push remote monitoring, and for which Annex U has been deemed to be not applicable, it will be the manufacturer’s responsibility to demonstrate that the SW architecture of the product does not allow contamination of the safety areas of the controller. For example, page 9 details the requirements which already pertain to partitioning safety related, functional safety SW from other application software. This concept may need to be extended to include logical and/or physical separation of functional/application/process SW from the software enabling communication. It is not the intention of these requirements that only a hardware separation can be used for the communication modules to fulfil the event driven or push remote monitoring functionality.

Public Network

IEC 60335-1 defines "**public network**" [3.11.3] as "network carrying digital data or analogue signals or both where access to the data and signals is not restricted by the physical space within the household or similar use environment of the appliance". While the internet is clearly a public network, most forms of telecommunication are either directly or indirectly part of a public network. In fact, it is the default assumption that if an appliance can communicate with an external entity, that communication potentially faces the same threats as communications on any public network. It does not matter that communication is between a Wi-Fi modem and an appliance in a household or from a smart phone Bluetooth connection. Both the modem and the phone are, in-turn, connected to public networks and therefore are potential gateways to accessing the appliance. A typical topography is shown in figure 7.

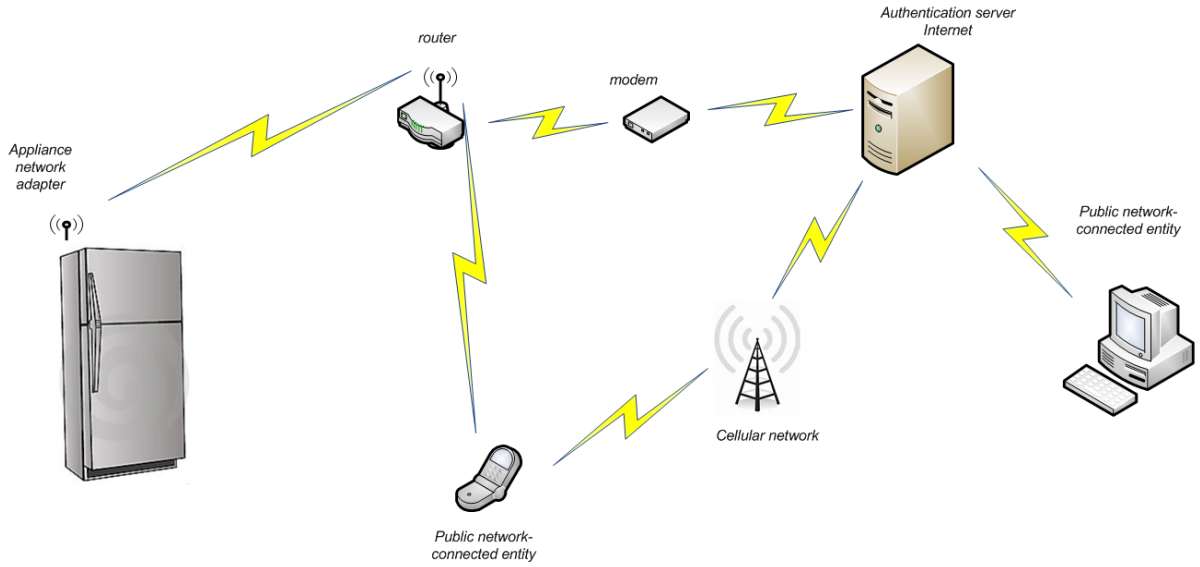


Figure 7 – Typical Topography of an appliance connected to public network(s)

However, the standard recognizes that certain communication technologies pose less risk for unauthorized access or manipulation of transmitted data. These have limited range of communication (e.g. near field communication), communicate only via line of sight (e.g. conventional hand-held IR remote controls) or are hardwired such that there is no physical connection to a public network. The configuration of the network is such that a hacker must be physically present to compromise the system. However, if a cell phone is communicating with an appliance via NFC (Near Field Communication) but downloads the new safety relevant software package via Wi-Fi, the overall configuration is still considered a public network.

Remote Communication

There are many remote communication technologies available for use with appliances. Common examples of telecommunication standards used in appliances are IEEE 802.11 (Wi-Fi) and IEEE 802.15 (e.g. Zigbee and Bluetooth). Cellular technologies (e.g. CDMA, LTE) are also used with appliances. Regardless of the communication technology, they all have rules or standards (collectively known as protocols) that define the syntax, semantics and synchronization of communication and error recovery methods.

When the communication between entities includes the exchange of data or the download of software which could impair compliance with the other clauses of this standard, and this communication occurs over a public network, then the communication should be protected considering:

- unauthorized access - only trusted and authorized communication partners should be allowed to communicate with the appliance.

- Intentional corruption of data - cryptographically procedures, digital signatures, hash functions, etc.
- random transmission faults/errors - Use of standardized communication/transmission protocols with error handling or correction.

Partitioning

Subclause U.3.1 requires ‘software enabling communication with a public network shall be partitioned into modules separate from software which is necessary to comply with the other requirements of this standard’. Proper partitioning is an important aspect of SW and systems architecture and is used already in household appliances for the separation/isolation of functional safety software and application software providing normal operation. ‘Separation of concerns’, is a modular software engineering design principle, used for separation of the software code in independent sections/modules each of them addressing a specific concern. It helps to prevent unwanted interactions and cross-coupling interference between functionally independent software modules and allows for simplification and maintenance of the software code.

Although the most straight forward way to achieve separation of software modules would be through physical separation with two completely independent processors, such hardware separation is not required and the equivalent isolation can also be provided utilizing proper software architecture. Partitioning requirements already exist in IEC 60335-1, refer to subclause R.3.2.2.1.

Authenticity

Concerning the aspect of authenticity, and the fact that only trusted and authorized entities should have the ability to exchange data or provide software which could impair compliance with this standard, the identification of communication partners is very critical. IEC 60730 provides guidance on this topic in clause H.2.24.5 with the following examples of identification procedures:

- *bi-directional identification – Where a return communication channel is available, exchange of entity identifiers between senders and receivers of information can provide additional assurance that the communication is actually between the intended parties,*
- *dynamic identification procedures – Dynamic exchange of information between senders and receivers, including transformation and feedback of the receiver information to the sender. Can provide assurance that the communicating parties not only claim to possess the correct identity, but also behave in the manner expected. This type of dynamic identification procedure can be used to preface the transmission of information between communicating safety-related processes and/or it can be used during the information transmission itself.*

Software Modification via Software Download and Installation

Software download capability may be desirable for a number of reasons.

For example, it may be necessary to update the communication protocols or security measures of the communication module so they can continue to communicate with public network entities. These updates may be automatic and necessary to ensure continued ‘availability’ of the appliance via services and communications through a public network. As stated on page 3, ‘availability’ does not directly affect the safety of the appliances as such, and therefore was not included in the Annex U, however, it is still an important issue for the consumer and is a potential reason for needing software updates of the communication enabling components such as communication modules or routers. See figure 3, column ‘Availability’.

Additional examples include new cooking menu items or washing cycles that can be implemented after the appliance has been installed and used for some time due to changing consumer needs. Also, downloading software bug fixes for maintenance and servicing actions can enhance the normal appliance operation, reducing the need for service personnel to physically visit the appliance. Because appliance software is increasingly complex, and the transfer of software from one entity to another has the potential for corruption or unauthorized modifications, the appliance downloading software should employ safeguards to ensure compliance of the appliance with this standard is not impaired during or after the new software has been installed.

Where software modification is implemented, the updated software should be investigated before being approved for download to the appliances. The investigation should be the same as traditional factory installed software used for new appliances and designs, repeating the evaluation and relevant tests in cases where the modification potentially influences compliance with the requirements of this standard. This approach to software development and testing, referred to as the V-Model, is one approach that may be used, and is described and illustrated in Figure 8. This is also the same approach taken in 22.46 for software in programmable protective electronic circuits. Furthermore, guidance is also provided in subclause R.3.4 of Annex R of IEC 60335-1. Prior to deploying a new software or firmware version, the manufacturer should ensure the technical documentation has be maintained to demonstrate that the changes will not impact the safety or conformity of the appliance.

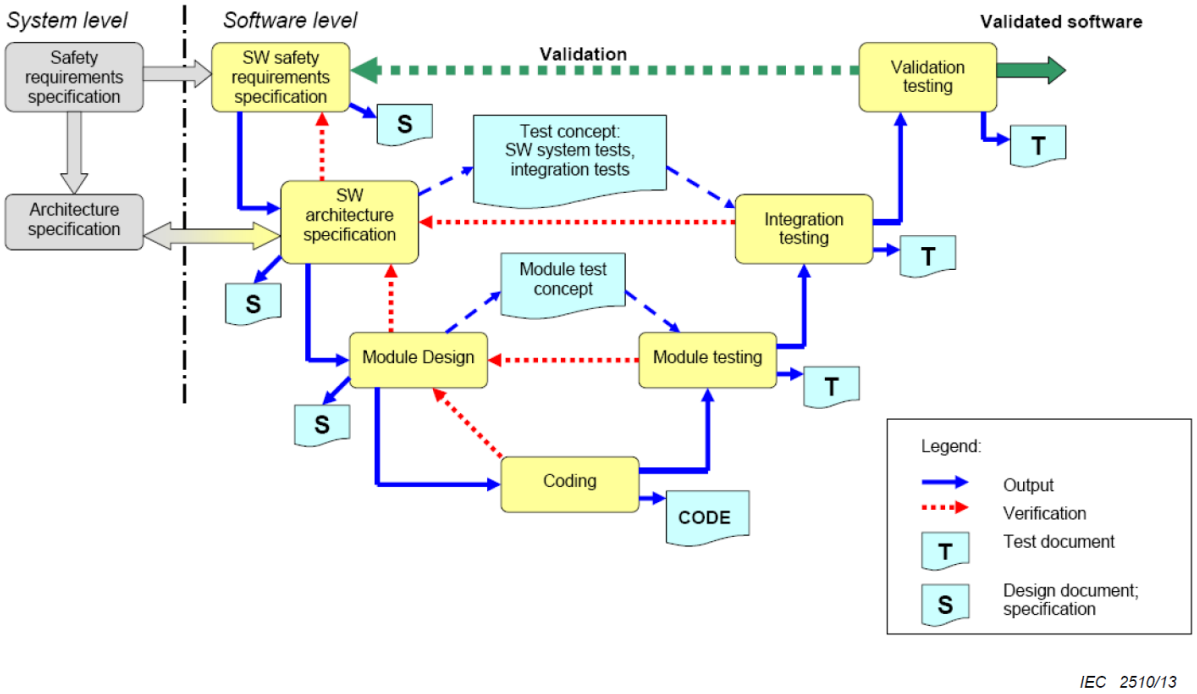


Figure 8 – V-Model for the SW life cycle

The general software update process via remote communication can be summarized by the following steps:

1. Establishing remote connection
2. Authentication
3. Authorization
4. Compatibility Check of Software Download Package
5. Download/Transmission
6. Verification of Received Software Download Package

7. Application of Received Software Download Package

8. Conclusion of Remote Software Update Process

9. Validation of Updated Software Package

A critical point to consider is the requirement in subclause U.3.8, which states:

Provisions shall be taken to ensure that software updates provided by the manufacturer and transmitted to the appliance via remote communication shall be verified prior to its installation:

The text '*verified prior to its installation*' is dependent upon the SW architecture employed in the product and the methods used for verification. The text is not meant to require redundant memory such that all SW is first downloaded, then verified for correctness and completeness, prior to flashing and replacing the current executable code. It is sufficient if the verification checks can detect incompatibilities or failures in the transmitted SW prior to its use or during an initialization phase of the microcontroller. In this case, the appliance could revert back to the previous SW version or remain in the safe state. As stated on page 3, availability is not determined to be a safety critical property for household appliances, and therefore, an appliance which ceases to function due to a failed SW update process is considered acceptable.