International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4806

(11/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Security capabilities supporting safety of the Internet of things

Recommendation ITU-T Y.4806

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	**Y.4800–Y.4899**
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4806

Security capabilities supporting safety of the Internet of things

Summary

Recommendation ITU-T Y.4806 provides a classification of the security issues for the Internet of things (IoT) and examines how the security threats may affect safety, in order to determine which security capabilities specified in Recommendation ITU-T Y.4401/Y.2068 support safe execution of the Internet of things.

The appendices of this Recommendation consider how the joint analysis of threats and security capabilities mentioned herein may be used to establish security requirements for the different applications of the Internet of things.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4806	2017-11-13	20	11.1002/1000/13391

Keywords

Internet of things, safety, security, security capability, security requirement, threat.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4806

Security capabilities supporting safety of the Internet of things

1 Scope

This Recommendation identifies security threats that may affect safety and security capabilities based on [ITU-T Y.4401].

Firstly, this Recommendation determines security threats with a possible impact on safety. Secondly, it identifies which security capabilities can be applied to mitigate these threats.

The Internet of things poses specific security challenges, which may not be covered by existing security objectives (such as confidentiality, integrity, availability) completely. Further elaboration of specific security countermeasures relies on an interpretation of security capabilities according to the identified threats.

This Recommendation is mostly applicable to safety-critical Internet of things (IoT) systems, such as industrial automation, automotive systems, transportation, smart cities, wearable and standalone medical devices, however it has no specific restrictions and may be used for any domain area of IoT.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things.*

[ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 adversary [b-NISTIR 7298Rev2]: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

3.1.2 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.3 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.1.4 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 IoT actor [ITU-T Y.4100]: An entity that is external to the IoT and that interacts with the IoT.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 impact vector: A path comprised of the communication links by which an adversary, exploiting weaknesses of IoT services, platforms, or devices may have an effect on the virtual or physical thing.

3.2.2 virtual environment: An infrastructure comprised of virtual things and actors, which are capable of communicating with things in the Internet of things using the appropriate services and data.

3.2.3 physical environment: An infrastructure comprised of physical things and actors, which are capable of interacting with things in the Internet of things via their sensing and actuating mechanisms.

NOTE 1 – It depends on the context when the thing is considered as a part if the Internet of things and when it is a part of its virtual or physical environment. When the thing is in focus, all other things may comprise the environment.

NOTE 2 – Separation to the virtual and physical environment is made on a use-case basis. Some things may be conceived as a part of the virtual or physical environment according to the nature of its interaction with the thing in focus. For example, heating, ventilating and air conditioning (HVAC) systems are usually considered as a part of the physical environment because an effect of their work is physical. At the same time, there are known cases when a HVAC system remotely maintained by a contractor was used to penetrate the internal network. In this scenario, the HVAC system is considered as a part of virtual environment because its virtual interfaces are in focus.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIC Availability, Integrity, Confidentiality

CIA Confidentiality, Integrity, Availability

HVAC Heating, Ventilating and Air Conditioning

IT Information Technology

IoT Internet of Things

PPE Personal Protective Equipment

SIS Safety Instrumented System

XSS Cross-Site Scripting

5 Conventions

None.

6 Classification of security issues in the Internet of things by their impact vector

Traditionally, security threats are considered as issues that arise in the virtual environment and target the data handling process. This leads to the interpretation of information technology (IT) security as the confidentiality, integrity, availability (CIA) set of aspects. Improper IT system behavior (e.g., software bugs, backdoors, Trojan programs) is also considered as a source of problems that affect these aspects and therefore cause only data handling concerns.

Attempts to classify security threats to the IoT in the same way they are classified for pure IT systems lead to difficulties in describing the potential physical impact caused by a cyberattack. One example of this approach is to rearrange the CIA triad to availability, integrity, confidentiality (AIC) by first ensuring the availability aspect in the physical systems and attaching less importance to confidentiality [b-NIST CPS]. The availability aspect is important, but alone, it cannot define all the physical characteristics that matter.

The Internet of things interconnects at least two types of environments: the virtual environment and the physical environment. Therefore, issues may arise from both types of environments and affect physical (P) aspects, virtual (V) aspects and the thing (T) itself. Figure 1 shows possible impact vectors in the Internet of things.

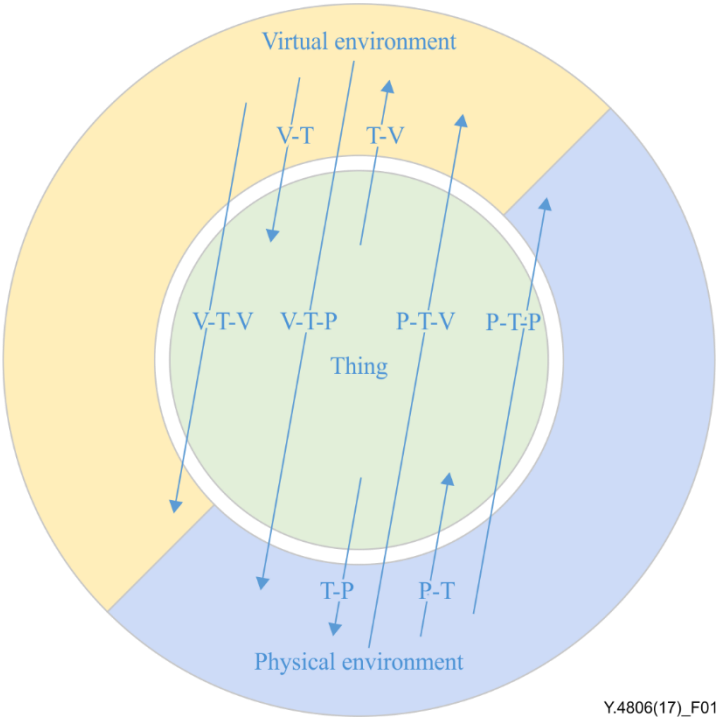

Figure 1 – Possible impact vectors in the Internet of things

The potential impact and prevention measures may vary significantly for these issues.

The classifications of security threats in the IoT domain are listed in Table 1, in accordance with the impact vectors shown in Figure 1.

The purpose of this classification is to determine which security threats are relevant to each impact vector according to the following criteria:

– They take place only for the physical things, that may be actuated by virtual means (i.e., things located in both environments), thus supporting the assumption about Internet of things as a key factor facilitating the issue.
– They may be enabled remotely, without getting physical or local access to the thing, thus providing the enhanced probability of such attacks in the connected world.
– Their impact may go beyond the confidentiality, integrity and availability of information, thus demonstrating the inability of many computer security methods to deal with them.

They may cause functional safety issues and thus provide a motivation to find ways to withstand them. This Recommendation will give further consideration to those threats that fit the criteria listed above.

Table 1 – Classification of computer security threats in the Internet of things according to their impact vector

Impact vector	May take place only for the things presented both in the virtual and physical environment	May be caused remotely without physical access to the thing	May go beyond the aspects from the CIA triad	May cause functional safety issues	Description	Examples
V-T	No	Yes	No	No	An attack targeting the thing from within its virtual environment	Denial of service attack Confidential information stealing
T-V	No	Yes	No	No	Exploiting software bugs or concealed features harming security of environment without any influence. May be treated as an informational safety issue.	Improperly implemented or infected with malware virtual thing capable of harming other
V-T-V	No	Yes	No	No	An attack targeting the virtual environment of the thing by exploiting its improperly implemented features	Cross-site scripting (XSS) Distributed denial of a service using botnet
V-T-P	Yes	Yes	Yes	Yes	An attack targeting the physical environment of the thing(s) and intended to cause physical damage or harm physical aspects of its functioning.	Attack on a smart vehicle intended to change its driving direction, speed, or cause any other physical effect Attack on industrial control system affecting the execution or efficiency of the technological

Table 1 – Classification of computer security threats in the Internet of things according to their impact vector

Impact vector	May take place only for the things presented both in the virtual and physical environment	May be caused remotely without physical access to the thing	May go beyond the aspects from the CIA triad	May cause functional safety issues	Description	Examples
						process Attack on the wearable medical device in order to change the taken dose of medicines
P-T-V	Yes	No	No	No	Actions posing problems for information security aspects by purely physical means.	Destroying hardware, cable breakage Physical tampering of video surveillance systems by placing a picture in front of a camera
P-T-P	No	No	Yes	Yes	Physical hazards that are usually capable of harming the physical environment or people.	Sabotage, negligence Faulty treatment
T-P	No	No	Yes	Yes	Software bugs or functions that may affect important factors in the physical environment. May be treated as thing functional safety.	System functions implemented without or with insufficient consideration of safety requirements
P-T	No	No	Yes	Yes	Physical hazards that are usually capable of harming the system or its components.	Disregard of operating instructions Faulty treatment

The vectors that arise from the virtual environment are cyberattacks. Cyberattacks may be performed remotely without getting physical access. The vectors V-T and V-T-V are generally well studied within the traditional computer and network security area. These vectors are not addressed in detail in this Recommendation.

However, the vector V-T-P targeting the physical environment is not well studied yet.

All issues that have their roots in the thing behavior due to its improper implementation or due to being compromised may be interpreted as pure safety problems in the informational and functional

aspect (vectors T-V and T-P respectively). These vectors are addressed in detail in this Recommendation.

The vectors P-T-P and P-T that arise in the physical environment are actually among those that are usually capable of harming the thing and surrounding infrastructure. These hazards are usually mitigated by a set of physical, organizational and deterrent measures. These vectors are not addressed in detail in this Recommendation.

The vector P-T-V refers to the effects on information security by purely physical means. Although such attacks may be important, they are specific to the IoT domain or environment of the thing. This vector is not addressed in detail in this Recommendation.

All threats targeting virtual environment may be mapped onto the CIA triad to determine the security objectives and appropriate security measures that need to be implemented to withstand attacks. At the same time, factors which may jeopardize the physical process, or harm the environment, or even human health and life may be hard to interpret in terms of confidentiality, integrity or availability of information.

Based on these possible types of issues in the IoT, it is necessary to pay special attention to the V-T-P impact vector, to reveal the conditions under which the existing methods of ensuring proper thing behavior may be ineffective for this impact and to propose an appropriate approach to threat modeling that eliminates the relevant safety risks.

It is worth mentioning that the impact vector may be interpreted as V-T-P even if the result of attack is data alteration only, but where the physical objects are finally damaged because of wrong decisions or actions according to these data. An example could be an aircraft crash caused by wrong data about the altitude in poor visibility and rough weather conditions.

This Recommendation will focus on the analysis of threats and measures associated with the V-T-P impact vector.

While the methods that guarantee safe things behavior in some IoT domains are well known and have been applied for decades, these methods may not always give the same guarantees in the event of deliberate attempts to cause improper thing behavior. The IoT has a wide-ranging potential for the implementation of such attempts due to the provided communication capabilities.

7 Security threats affecting safety in the Internet of things

Security threats affecting safety generally use the V-T-P impact vector to affect the physical environment (in particular, to cause a safety violation) by exploiting thing features or vulnerabilities.

7.1 Sources of security threats affecting safety

The sources of security threats affecting safety lie in the virtual environment. These sources may pose risks for both unintentional mistakes and deliberate abuses of thing functionality.

The set of potential malicious actors formally includes any actor that may access the thing by any virtual means. An external attacker remotely accessing the system is usually considered as a striking example for demonstration purposes. In fact, any IoT actor both in the virtual and physical environment may be considered as a possible source of issues, or as an adversary.

Further restrictions on the list of possibly malicious actors are set according to the assumptions about their trustworthiness. The role of assumptions is explained in more detail in clause 7.3.

Thus, the sources of attacks from within a virtual environment in the IoT are indistinguishable from the sources of attacks on the security of pure IT systems. Those of sources that may affect the physical environment are of the particular interest for this Recommendation.

7.2 Scenarios of threatening functional safety

For different IoT domains, the ways in which the physical aspects of thing functioning are impacted will obviously vary. It is worth mentioning that if the physical process is directly controlled by commands issued by a virtual thing; these commands are usually checked to avoid direct harm. Hence, scenarios, whereby safety is affected by virtual means, have to be more sophisticated. For example, an adversary may use two independent channels to cause an undesirable effect (e.g., one for disabling the protection mechanisms and another for placing the thing into an invalid state).

7.3 Requirement for the identification of security threats affecting safety

An effective threat modelling technique takes into account both possible system flaws and threats that may be of interest to the adversary. Threat identification and modelling is used to find out which vulnerabilities of the thing are most dangerous and how they can be exploited by the adversary to violate the security aspects and cause harm (in particular to safety).

The validity of the results of threat identification depends on the correctness of the assumptions set out. This is true both for information security and for functional safety. In particular, if safety mechanisms rely on assumedly reasonable actor behavior (even taking into account unintentional mistakes), a safety violation may be caused by an intentionally malicious actor. Security incidents also often happen according to an unforeseen system usage scenario. The adversary breaks the assumptions made during threat modelling and security mechanism implementation to bypass this mechanism.

Identification of security threats affecting safety requires:

– The revision of assumptions made by safety engineers from a security point of view.

– Consideration of possible weaknesses in the protection components.

– Using an approach allowing the unification of security threats and safety hazards within a structured (possibly formal) description.

7.4 Safety measures and how they mitigate threats

Though safety requirements posed by the things across IoT domains can vary drastically, generally safety provisions for diverse applications include monitoring and enforcement mechanisms. This simple classification also covers the extreme cases. If the safety mechanism is oriented more on placing the thing in a safe state, the monitoring just ensures that the condition to enforce protection is fulfilled. If the interference into the process is undesirable or unreasonable, the monitoring may be the only mechanism that follows up on the safety parameters.

In some cases, the V-T-P impact vector can be effectively eliminated by safety enforcement measures that were initially designed for the T-P vector; but in other cases, this will not be possible. The analysis of such other cases reveals the following reasons for this ineffectiveness:

– **Possibility of tampering or bypassing the safety restrictions**. Safety measures usually do not seek to cover the possibility of intentional violations. The violations they address are considered as accidents or sets of coincidences.

  Exploitation of the weaknesses of safety mechanisms helps to make the adversary's actions appear safe when they are not. For this purpose, the adversary injects the specifically formed data as the system input to mislead the validation algorithms.

– **Attacks on separately implemented safety mechanisms**. Implementation of safety mechanisms by an independent party and installation separately from the controlled system reduce this risk of common cause failures. At the same time, the adversary may compromise standalone safety monitoring and enforcement mechanisms if they are not properly protected.

7.5 Security measures

On the understanding that an attack constitutes a special input (to exploit a vulnerability) intended to place the system into an unusual (insecure) state under particular conditions, two general methods for keeping the system in a secure state may be described as follows:

– Input data validation. As a result of this validation, input data or data processed by the connected system may be corrected to fit the established rules, or the appropriate attempt of interaction with the system may be rejected.

– Security control of the system or its environment (secure state control). As a result of this control, the system, its components or data may be forced to return to a state that meets the necessary security requirements.

These methods are applicable universally to all types of systems and software. Some protection solutions may implement these methods jointly. For example, antimalware solutions may use signature detection as a method of input validation and implement restrictions, which is a kind of the system state control. Any technical protection method may be interpreted as a kind of input validation or secure state control.

In the IoT context, conventional protection solutions and methods may be ineffective due to the following reasons:

– **Absence of input data validation or possibility of bypassing it**. The adversary may use special techniques and exploit system features in an inappropriate way to affect the physical aspects of system functioning. This activity may be either not covered by an input surveillance mechanism or not detected with validation methods due to a lack of knowledge about the physical nature of the thing. With the exception of things based on a special-purposed platform, the protection software may not exist.

– **Conflict of security and safety, or of security and functionality**. Active measures taken to halt the security violation might end up having a harmful interference on running processes. Such interference may be unacceptable for some physical processes requiring continuous execution. Most safety engineers prefer to cut off the security measures to passive security validation.

– **Attacks on security mechanisms**. Security mechanisms, both separate and built-in, may also be a target of attack. Separate security controls are more likely to be attacked. At the same time, for many applications security is considered as a secondary factor that is allowed for disabling in any doubtful situation. The adversary may exploit this fact to compromise security.

7.6 List of IoT security threats

For the Internet of things, the use cases for maintaining safe and secure thing functioning can be summarized as shown in Figure 2. This figure extends the general use case model described in [ITU-T Y.4100].

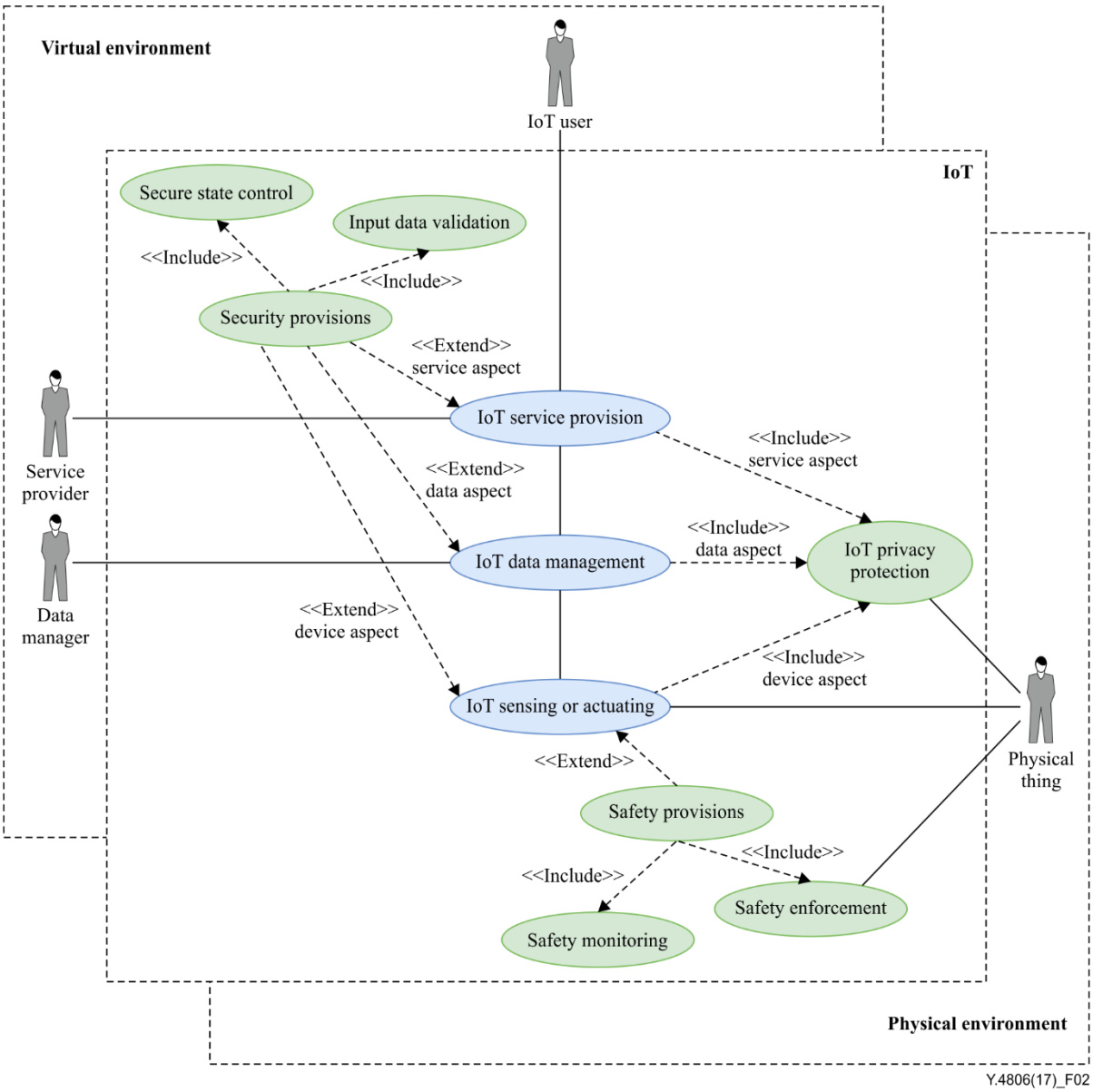

Figure 2 – The general use case model of the IoT extended with security and safety mechanisms

The shortcomings related to the use of conventional safety and security measures in the IoT domain may ultimately result in the security threats listed in Table 2.

Table 2 – The list of security threats in the IoT that are capable of affecting safety

Threat reference number	Description	Example
T-1	Intentional tampering or bypassing the restrictions provided by safety mechanisms.	Forgery of the data from the sensors used for monitoring the environmental safety conditions.
T-2	Disabling or deactivation of the separate safety mechanisms due to the malicious actions of the virtual adversary.	Breaking the authentication for safety system management due to using of weak or predefined password.
T-3	Exploiting the lack of, or inappropriate security checks that, if properly implemented, would detect the actions that are, or likely to be, misleading or deceptive (social engineering, request forgery, etc.).	Cross-site request forgery attack on the operator's console based on the web application technology leading to the unauthorized launch of physical operation.
T-4	Exploiting the lack of, or inappropriate security enforcement, that was constrained by safety requirements or requirements linked to the nature of physical processes and related to the thing application.	Avoiding use of antimalware technologies at the industrial servers because of the concern about unexpected delays in operations resulting in the infiltration of these servers with malware.
T-5	Disabling or deactivation of security mechanisms due to the malicious actions of the virtual adversary.	Unauthorized management by exploiting vulnerabilities in authentication mechanism as for T-2. Exhausting the resources by the intentionally frequent requests to the system thus making the security controls go beyond the system operational capacity and forcing the user to switch them off.

8 Security capabilities for supporting safety in the Internet of things

8.1 Security capabilities initial list

The following security and privacy protection capabilities are listed in clause 8.7 of [ITU-T Y.4401]:

– Communication security capability [C-7-1]
– Data management security capability [C-7-2]
– Service provision security capability [C-7-3]
– Security integration security capability [C-7-4]
– Mutual authentication and authorization security capability [C-7-5]
– Security audit security capability [C-7-6].

In this Recommendation, those specific security capabilities listed above that can support safety in the Internet of things are further investigated. This consideration is valuable for the implementation of a safer, more secure Internet of things and as an example of basic IoT capabilities for the analysis and design of the technical requirements for different things across the IoT domains.

8.2 Instantiation of security capabilities to address threats

8.2.1 Communication security capability [C-7-1]

Provides input validation capability at the communication channel layer, including checks of sources, protocols and flows of information between the connected things, to mitigate threats [T-3].

Provides a reliable communication capability, including resistance to channel overflow and denial of service attacks, to mitigate threats [T-1], [T-2], [T-5].

Maintains the integrity and authenticity of commands and data at the communication channel layer, including protocol data encryption, to mitigate the threats [T-2], [T-3], [T-5].

8.2.2 Data management security capability [C-7-2]

Provides input validation capability at the data interpretation layer, including checks of the commands for IoT applications, their parameters and semantics (to determine possible physical effect), to mitigate threats [T-3].

Maintains the integrity and non-repudiation of commands and data at the IoT application layer, including application data encryption, checksum computation and signing, to mitigate threats [T-3], [T-4], [T-5].

8.2.3 Service provision security capability [C-7-3]

Provides a monitoring mechanism as a dedicated contract-based service(s), including the isolation of obtained data and the analysis of monitored components, isolation of emergency policy enforcement and an alarm mechanism, isolation and independent execution of the entire monitoring mechanism, facilitating the mitigation of threats [T-3], [T-4], [T-5].

8.2.4 Security integration security capability [C-7-4]

Provides the ability to integrate different rules and policies for input validation at different layers if diverse technologies are employed by these layers, facilitating the mitigation of threats [T-1], [T-2], [T-3], [T-5].

Provides the ability to integrate different rules and policies for security control at different layers if diverse technologies are employed by these layers, facilitating the mitigation of threats [T-1], [T-2], [T-4], [T-5].

8.2.5 Mutual authentication and authorization security capability [C-7-5]

Provides the capability to authenticate and authorize subjects before they attempt to manage and control the protection mechanisms, facilitating the mitigation of threats [T-2], [T-5].

8.2.6 Security audit capability [C-7-6]

Provides the ability to monitor attempts to manage and control the protection mechanisms, mitigating threats [T-2], [T-5].

Provides attack detection capability, including detection of probing, infrastructure attacks, remote attacks, insider attacks and system misuse, to mitigate threats [T-1], [T-3].

Provides the ability to monitor the load on equipment and communication channels, including the detection of both unintentional overload and denial of service attacks, to mitigate threats [T-1], [T-2], [T-5].

Provides the ability to detect attacks on recovery and response capabilities to mitigate threats [T-1], [T-2], [T-5].

Further details for mapping the security threats with the possible security capabilities are provided in Appendix I.

Appendix I

Development of requirements according to identified threats

(This appendix does not form an integral part of this Recommendation.)

I.1 Smart traffic lights

Originally designed as standalone hardware, traffic signals are now becoming the part of the complex of networked systems. Traffic controllers not only use the time-specific schedule but also analyse the data supplied by sensors, communicate with other controllers placed on the nearby intersections and support remote control for better traffic regulation.

Thus, smart traffic lights systems should employ the security capabilities to ensure the utmost safety of the road traffic coordinated by this system.

A typical smart traffic lights system, as shown in Figure I.1 of [b-WOOT], includes one, or sometimes more, traffic controllers for every intersection, a required number of traffic signals, sensors for car detection and inspection of the intersections (induction loops, microwave, ultrasonic, radar sensors and surveillance cameras), units for wired or wireless communications and detached or on-board safety control units for every traffic controller.

The traffic controller in terms of the IoT is the main 'thing' immediately involved in the traffic regulation. The traffic controller determines the state of the traffic lights thus potentially affecting the safety of the road traffic.

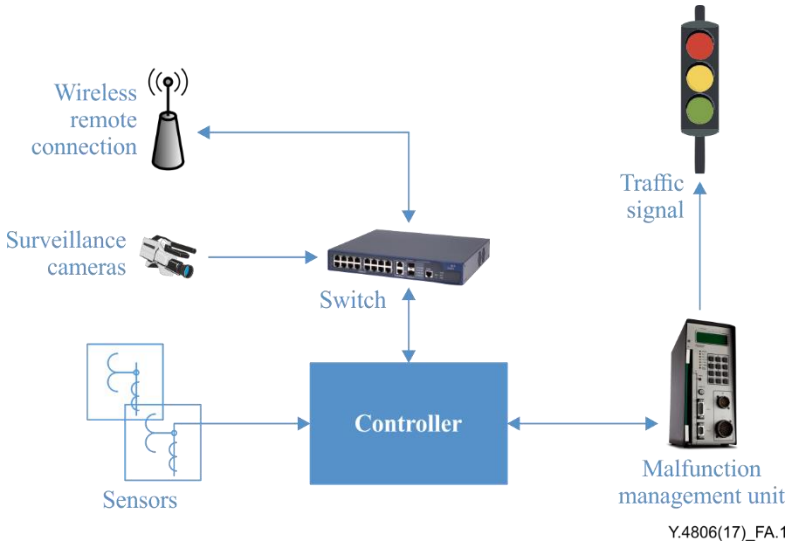

Figure I.1 – Smart traffic lights system

Safety for both connected and standalone traffic lights is usually provided by installing a special malfunction management unit that is a hardware safety mechanism. This unit is responsible for forcing the controller and appropriate traffic signals into a safe state in the case of detection of a potentially dangerous configuration. Thus, the mechanism acts as a filter allowing only the predefined states and changing all other states to the known one. In most cases, the unit just overrides the controller and puts it in the default state (i.e., flashing red light), ensuring that safety downgrades to not more than its minimum acceptable level. Returning the controller to its normal functioning may require the manual intervention. This is the case for the implementation of remote management and control of the safety mechanism, which may become a target for attack.

The set of security threats affecting safety is instantiated for the traffic controller in Table I.1, considering that the minimum acceptable impact level represents putting the light into the default state (i.e., flashing red light).

The following impact levels are set for the threats:

– High: safety downgrades to the non-acceptable level, i.e., it is possible to put the traffic lights at an intersection to a dangerous configuration;

– Medium: safety downgrades to the minimum acceptable level, i.e., it is possible to put the traffic lights at an intersection to the default configuration;

Table I.1 – Security threats affecting safety for the traffic controller

General security threat affecting safety for the IoT	Threat for smart traffic controller	Description	Impact level
[T-1]	[T-STL-1]	Malfunction management unit is installed improperly, in an incorrect way making tampering with or bypassing of the malfunction management unit possible. This threat has no impact vector from the virtual environment	High: Safety downgrade to non-acceptable level.
[T-2]	[T-STL-2]	Remote deactivation of malfunction management unit in the case where it exposes some virtual interface to the controller or to other units connected to external network. This threat has an impact vector acting from the virtual environment only if the mentioned interface exists.	High: Safety downgrade to non-acceptable level.
[T-3]	[T-STL-3]	The lack of, or inappropriate security validation of input data from any kind of installed sensors and surveillance cameras.	Medium: Safety downgrade to the minimum acceptable level.
[T-3]	[T-STL-4]	The lack of, or inappropriate security validation of input data from remote management unit connected by wired or wireless means.	Medium: Safety downgrade to the minimum acceptable level.
[T-4]	[T-STL-5]	The lack of, or inappropriate control of consistency and proper handling of the data from multiple sources (e.g., sensors, surveillance cameras and remote management units) that leads to the inappropriate results forcing the known safe state.	Medium: Safety downgrade to the minimum acceptable level.
[T-5]	[T-STL-6]	Remote deactivation of security mechanisms via exposed management interfaces.	Medium: Safety downgrade to the minimum acceptable level.
[T-5]	[T-STL-7]	Remote deactivation of security mechanisms by exploiting their vulnerabilities.	Medium: Safety downgrade to the minimum acceptable level.

While the impact level of the threats related to the disabling of safety mechanisms is high, these threats have a low probability. The other threats with medium impact level may lead to placing the controller into the known safe state. On the other hand, any downgrade of the safety level should be considered as potentially unwanted event and thus should be prevented. For these reasons, all the described threats should be addressed with appropriate security requirements.

Table I.2 summarizes the details needed to establish the requirements for traffic controller software resistance to security threats that could affect safety. It contains references to the threat, system

component or channel that may be exposed to an attack, assumptions that may be invalid and thereby facilitate an attack, the defect or vulnerability that is likely to be exploited, prior countermeasures and the requirements to withstand an attack.

Drawing on the knowledge of the specific details from a given smart traffic light system, further analysis can be conducted to obtain the specific requirements for this system. Some assumptions may be eliminated, other details clarified and then requirements may be refined until a detailed specification of protection measures for the given system are obtained.

Table I.2 – Security requirements for the traffic controller

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-STL-1]	Reasonable behavior of maintenance technician Malfunction management unit unexposed to any unauthorized physical access	Absence of control	–	As this threat has no impact vector from the virtual environment, no technical requirements shall be put in place
[T-STL-2]	Reasonable user behavior Management interface unexposed to a malicious adversary	Improperly implemented or configured authentication and authorization, including default credentials and weak password	Using dedicated communication channel to access the management interface of the safety mechanism, if such interface exists	In the case where a management interface for safety mechanism exists: Implement the authentication and authorization of remote actors before they attempt to manage and control the safety mechanisms [C-7-5] Implement the monitoring of attempts to manage and control the safety mechanisms [C-7-6] Provide the instructions for proper configuration of these mechanisms [C-7-4]
[T-STL-3]	Absence of any kind of vulnerability that may cause faulty behavior of the controller	Improperly implemented data handling	–	Implement filtering at the communication layer for network flows and sources to ensure that assumptions about probable connections are valid (Capability [C-7-1]) Implement filtering at the application layer to ensure that assumptions about connected virtual environment are valid (Capability [C-7-2]) Perform integration testing and validation paying the special attention to fuzzing the input at the different layer of the system (Capability [C-7-4]) Implement application-specific audit with attack detection capabilities to monitor for improper behavior (Capability [C-7-6])

Table I.2 – Security requirements for the traffic controller

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-STL-4]	Reasonable user behavior Remote access interface unexposed to a malicious adversary	Improperly implemented or configured authentication and authorization, including default credentials and weak password Improperly implemented data handling	–	Implement filtering at the communication layer for network flows and sources to ensure that assumptions about probable users are valid (Capability [C-7-1]) Implement filtering at the application layer according to domain area to ensure that assumptions about user behavior are valid and this behavior meet the necessary restrictions (Capability [C-7-2]) Implement the authentication and authorization of remote actors before they attempt to manage and control the controller [C-7-5] Implement the monitoring of attempts to manage and control the controller [C-7-6] Provide the instructions for proper configuration of these mechanisms [C-7-4]
[T-STL-5]	Absence of any kind of vulnerability that may cause faulty behavior of the controller	Improperly implemented data handling	–	Implement filtering at the communication layer for network flows and sources to ensure that assumptions about probable connections are valid (Capability [C-7-1]) Implement filtering at the application layer to ensure that assumptions about connected virtual environment are valid (Capability [C-7-2]) Perform integration testing and validation paying the special attention to fuzzing the input at the different layer of the system (Capability [C-7-4]) Implement application-specific audit with attack detection capabilities to monitor for improper behavior (Capability [C-7-6])

Table I.2 – Security requirements for the traffic controller

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-STL-6]	Reasonable user behavior Management interface unexposed to a malicious adversary	Improperly implemented or configured authentication and authorization, including default credentials and weak password	Using dedicated communication channel to access the management interface of the security mechanisms, if such interface exists	In the case where the management interface for security mechanisms exists: Implement the authentication and authorization of remote actors before they attempt to manage and control the security mechanisms [C-7-5] Implement the monitoring of attempts to manage and control the security mechanisms [C-7-6] Provide the instructions for proper configuration of these mechanisms [C-7-4]
[T-STL-7]	Communications are reliable Management interface unexposed to a malicious adversary	Weak communication infrastructure Improperly implemented management and control for security mechanisms	Using dedicated communication channel to access the management interface of the security mechanisms, if such interface exists	Implement reliable and resistant to attacks communication infrastructure (Capability [C-7-1]) Implement security mechanisms as a set of loosely-coupled components, independent from other software (Capability [C-7-3]) Implement monitoring the load on the equipment and communication channels (Capability [C-7-6])

I.2 Industrial control system

Safety monitoring of the industrial control system is usually performed in the physical environment. Due to diversity of the industrial control systems, implementation of such safety monitoring mechanisms can vary from being completely absent to deployment of highly reliable safety instrumented systems (SIS). Such systems were implemented primarily to guarantee the functional safety of process execution. Safety instrumented systems must be deployed independently from all other control systems that control the same equipment in order to ensure SIS functionality is not compromised. Most safety engineers would prefer to have no integration between safety and control systems at all, as shown in the 'Environment monitoring' and 'Safety enforcement' rectangles in Figure I.2. Safety enforcement receives data from independently implemented monitoring mechanisms or from the industrial control system and performs the necessary actions in order to keep the system functioning within the necessary conditions.

At the same time, even for highly dangerous areas, not all facilities adhere to the strict separation of safety and control for safety protection. The approach for a particular company depends on the business strategy and tolerance for risk. If safety is a top priority at any cost, separate control and safety systems remain the best option, while the adoption of a platform integrating control and safety systems might be preferred to maximize the cost savings.

The impact vector of the physical environment from within the virtual informational environment is outlined in Figure I.2. The common protection mechanisms (input validation, environment and system monitoring) are also placed in Figure I.2.

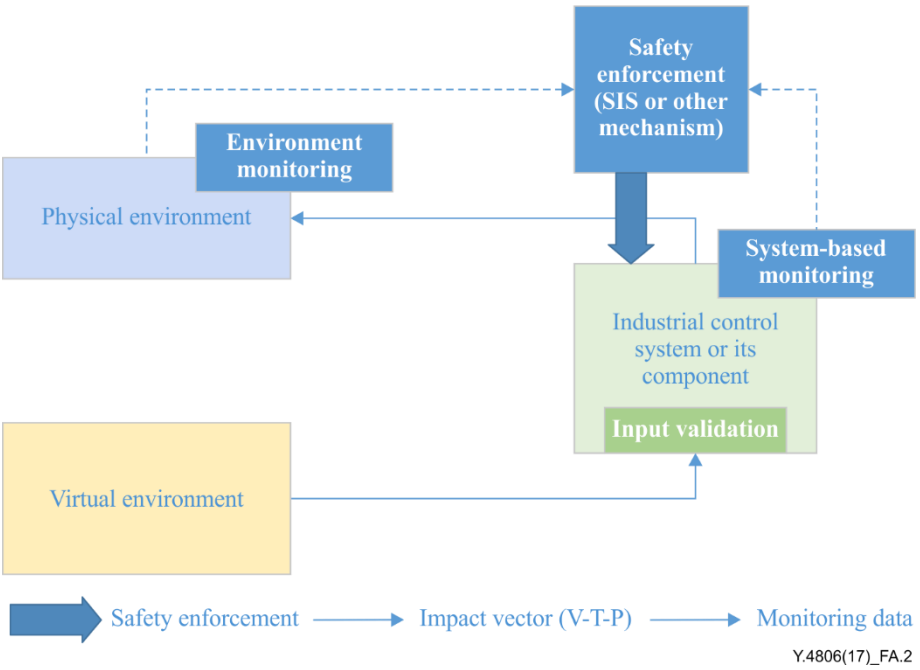

Figure I.2 – The V-T-P impact vector with possible protection mechanisms

The mentioned threats may be interpreted for the industrial domain of the IoT as described in Table I.3.

Table I.3 – Security threats affecting safety for the industrial control system

General security threat affecting safety for the IoT	Threat for smart traffic controller	Description	Impact level
[T-3] **[T-5]**	[T-ICS-1]	The lack of, or inappropriate, input validation that might be used to monitor attempts of system misuse, attacks on the virtual informational channel or on the user (social engineering, request forgery, etc.). If input validation is still implemented, it may be the target of an attack.	Medium, in the case where SIS is in place and functions correctly.
[T-2]	[T-ICS-2]	System monitoring may be disabled because of a successful attack. This is an argument for the use of detached (environment) monitoring, although in the case of a targeted attack the external SIS may be deactivated. This substantiate the need for securing the SIS.	High, in the case where SIS functionality is compromised
[T-1]	[T-ICS-3]	The monitoring data or results may be tampered with false data to force the wrong decision about the current safety status. The complexity of this attack depends on the architecture of the system and safety mechanisms, but it should also be taken into account.	High, in the case where SIS functionality is compromised
[T-2]	[T-ICS-4]	The safety enforcement mechanism may be disabled.	High, in the case where SIS functionality is compromised
[T-1]	[T-ICS-5]	The channels used for safety enforcement may be compromised.	High, in the case where SIS functionality is compromised
[T-4]	[T-ICS-6]	Keeping the continuous process execution does not allow forcing the control system into a secure state (e.g., deleting the files that are suspected to be infected with malware etc.) This may lead to control of the process by malicious agent.	Medium, in the case where SIS is in place and functions correctly.

The threats that are connected to the compromise of safety mechanisms, have a potentially high level of impact on safety, while other threats might have a medium risk since they are partially mitigated by safety mechanisms.

Table I.4 summarizes the data necessary to establish the requirements for industrial control systems to resist security threats that could affect safety. It contains references to the threat, system component or channel that may be exposed to an attack, assumptions that may be invalid and thereby facilitate an attack, the defect or vulnerability that is likely to be exploited, prior countermeasures and the requirements to withstand an attack.

Drawing on the knowledge of the specific details from a given system, further analysis can be conducted to obtain the specific requirements for this system. Some assumptions may be eliminated, other details clarified and then requirements may be refined until a detailed specification of protection measures for the given system is obtained.

Table I.4 – Security requirements for the industrial control system

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-CPS-1]	Reasonable user behavior. Absence of cyberattack vectors which may cause physical damage.	Lack or inappropriateness of input validation. Bypassing input validation	Recheck assumptions about the user. Validation of the input control mechanisms according to domain area.	Implement filtering at the communication layer for network flows and sources to ensure that assumptions about probable users are valid (Capability [C-7-1]) Implement filtering at the application layer according to domain area to ensure that assumptions about user behavior are valid and this behavior meet the domain area restrictions (Capability [C-7-2]) Perform integration testing and validation for the combination of rules and policies regarding input validation at the different layer of the system (Capability [C-7-4]) Implement application-specific audit with attack detection capabilities to monitor for improper behavior (Capability [C-7-6])
[T-CPS-2]	Non-exposure of the monitoring mechanisms to attacks	Poor protocols and supporting infrastructure Poor monitoring implementation Tight integration of monitoring system with the system under monitoring	Recheck the physical protection and reliability of the sensors, implement tampering detection measures.	Implement reliable and resistant to attacks communication infrastructure (Capability [C-7-1]) Implement reliable and resistant to attacks algorithms of monitoring management and control (Capability [C-7-2]) Implement monitoring mechanisms as a set of loosely-coupled components, independent from the system itself and connected with the system by explicitly defined interfaces (Capability [C-7-3]) Implement mutual authentication and authorization for the procedures of management and control (Capability [C-7-5]) Implement the audit of the procedures of management and control, attack detection mechanism and monitoring the load on the equipment and communication channels (Capability [C-7-6])

Table I.4 – Security requirements for the industrial control system

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-CPS-3]	Non-exposure of the channels to cyberattacks.	Non-tamper proof monitoring	Recheck assumptions about access to the channels and the integrity of the data.	Implement dependable and tamperproof protocols for exchanging the monitoring data (Capability [C-7-1]) Implement reliable and resistant to attacks algorithms of monitoring management and control (Capability [C-7-2]) Perform integration testing and validation for the combination of rules and policies regarding monitoring at the different layer of the system (Capability [C-7-4])
[T-CPS-4]	Non-exposure of the safety enforcement mechanism to cyberattacks.	Safety enforcement mechanism vulnerable and exposed to unauthorized access	Verify the resistance of the safety enforcement mechanism to cyberattacks	Implement reliable and resistant to attacks communication infrastructure (Capability [C-7-1]) Implement reliable and resistant to attacks algorithms of monitoring management and control (Capability [C-7-2]) Implement monitoring mechanisms as a set of loosely-coupled components, independent from the system itself and connected with the system by explicitly defined interfaces (Capability [C-7-3]) Implement mutual authentication and authorization for the procedures of management and control (Capability [C-7-5]) Implement the audit of the procedures of management and control, attack detection mechanism and monitoring the load on the equipment and communication channels (Capability [C-7-6])

Table I.4 – Security requirements for the industrial control system

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-CPS-5]	Non-exposure of the safety enforcement channel to cyberattacks.	Safety enforcement mechanism vulnerable and exposed to unauthorized access	Verify the resistance of the safety enforcement channels to tampering and denial of service.	Implement reliable and resistant to attacks communication infrastructure (Capability [C-7-1]) Implement monitoring mechanisms as a set of loosely-coupled components, independent from the system itself and connected with the system by explicitly defined interfaces (Capability [C-7-3]) Implement monitoring the load on the equipment and communication channels (Capability [C-7-6])

I.3 Smart wearable devices for industrial safety and productivity management

Connected smart wearable devices are among the emerging technologies in the industrial applications of the IoT. There are two main goals for using these devices: first for on-site monitoring and informational support of the operational engineer equipped with device(s) and secondly for central monitoring of the facility equipment, processes and safety conditions including the state of the worker using the data supplied by device(s).

For the on-site monitoring and control purposes, connected smart wearable devices, such as glasses or a helmet optionally combined with wearable sensors, take advantage of augmented reality technology. This technology enables operating engineers to overlay maps, schematics and thermal images to "see through" walls, pipes and other solid objects.

For the central monitoring purposes, connected smart wearable devices stream video, voice communication, worker's location and information from optional wearable sensors to the controlling platform. These devices are capable of providing in real time the status of workers/site, pinpoints on the map, voice communication functionality and optional information like worker's heart rate or environmental conditions.

Other advantages also facilitate the growing popularity of smart wearable devices at industrial facilities. There is no need of a walkie-talkie or mobile phone in the case of use a smart helmet, thus, it allows keeping hands free and increases personal safety. The possibility of video collaboration with experts in remote locations results in faster repairs and saves the expense of flying an expert to the site to help. Employees at remote sites can communicate and share video of what they see with experienced workers to get advice on how to diagnose and fix problems. In this way, enterprises can improve the cost-effectiveness of their field service and remote operations by employing a larger ratio of less-experienced workers to experienced ones or specialists, thus saving labor costs.

The streamed video can be stored as evidence that a job was performed correctly or that everything looks fine during an inspection. Such video records can be valuable if customers make allegations against the field service company. The video record is important for other industries as well,

notably insurance adjusters, real estate appraisers, construction inspectors and couriers to prove package delivery.[1]

The following safety related concerns exist for connected smart wearable devices at industrial facilities.

1. Both on-site and central monitoring require the continual supply of data for analysis and immediate reaction to possible emergencies. One of the advantages of smart wearable devices at industrial facilities is that the time for reaction by experienced workers is reduced. For example, thermal vision provides workers with thermal characteristics of objects or items in the workplace that need maintenance or additional monitoring and the workers equipped with the appropriate control capabilities may fix the problem immediately.

   In the case of connected wearable devices, the monitoring data delivered via wireless channels are exposed to attacks. If the integrity and authenticity of data are not provided, fraudulent data injected by a malicious adversary and appropriate reactions to these data by personnel may threaten the equipment, process and even cause safety hazards. The physical presence of the adversary at the facility is not required; the attack may be performed if he can traverse the path in a virtual environment to access the device. This is possible, for example, if the device has an interface for remote maintenance.

2. Often smart wearable devices are considered as personal protective equipment (PPE) intended to reduce worker's exposure to hazards when engineering controls and administrative controls are not feasible or effective to reduce these risks to acceptable levels. For example, thermal vision equips users with the ability to see temperature data in their real-world environment. This prevents them from interacting with something at an unsafe temperature. At the same time, any PPE has the serious limitation that it does not eliminate the hazard at the source and may result in employees being exposed to the hazard if the equipment fails. This failure, in particular, may take place in the case of attack via the communication interfaces of this device.

This is the case for security analysis and threat modelling.

This example neither refines the type of wearable device nor describes the concrete interfaces and types of communication technologies. While covering the whole range of devices, this example does not refer the threats in detail and provides only a rough estimation of possible impact.

The following levels of impact on safety are considered:

- High impact: the data provided by the smart wearable device to the worker on site, or to the central monitoring system, is maliciously changed, tampered with, or contains misleading information due to some other reason.
- Medium impact: the smart wearable device is not capable of providing the data to the worker on site or to the central monitoring system, or cannot do so in the required time frame, due to interference in its functioning or in communications and surrounding infrastructure
- Low impact: the data provided by the smart wearable device, such as process parameters, video stream, status of workers on site is disclosed to the unauthorized third-party

Thus, the impact levels are set according to the integrity, availability and confidentiality of data supplied by the device. For some cases, the impact level may be defined in some other way. For this general example, it is believed that providing the fraudulent data is more dangerous for safety than preventing these data from being accessed and accordingly the prevention of data disclosure might have less priority (for safety) than keeping its integrity and availability.

---

1 http://www.gartner.com/newsroom/id/2618415

Table I.5 lists security threats affecting safety for an industrial control system, while Table I.6 lists security requirements for connected smart wearable devices for industrial safety and productivity management.

Table I.5 – Security threats affecting safety for the industrial control system

General security threat affecting safety for the IoT	Threat for connected smart wearable device at the industrial facility	Description	Impact level
[T-3]	[T-SWI-1]	Compromise of wireless connections using rogue devices or devices infiltrated with malware	High impact: the data integrity may be compromised in case the data authenticity control is NOT in place, such as in case of Man in the Middle attack Note: Other impact levels may be expected according to the attack as follow: – Medium impact: the data may become unavailable both for the worker on site and central monitoring system – Low impact: the unencrypted data may be disclosed to unauthorized person
[T-3]	[T-SWI-2]	Interception of short-distance communications	Low impact: the unencrypted data may be disclosed to unauthorized person
[T-3]	[T-SWI-3]	Hindering wireless communications by suppressing or interfering with radio signal	Medium impact: the data may become unavailable both for the worker on site and central monitoring system
[T-3]	[T-SWI-4]	Exploiting remote control interfaces of the wearable device for getting control on it	High impact: the data integrity may be compromised EVEN IF the data authenticity control is in place
[T-3]	[T-SWI-5]	Exploiting the vulnerabilities of application level protocols for injecting the wrong data into information flows from device to the central monitoring system and back	High impact: the data integrity may be compromised if the data authenticity control is NOT in place Note: Other impact levels may be expected according to the attack as follow: – Medium impact: the data may become unavailable both for the worker on site and central monitoring system
[T-3]	[T-SWI-6]	Exploiting the vulnerabilities of application level protocols for hindering the data exchange between the device and central monitoring system	Medium impact: the data may be unavailable both for the worker on site and central monitoring system

Table I.5 – Security threats affecting safety for the industrial control system

General security threat affecting safety for the IoT	Threat for connected smart wearable device at the industrial facility	Description	Impact level
[T-4]	[T-SWI-7]	General remote attack on smart wearable device or its malware infection	High impact: the data integrity may be compromised EVEN IF the data authenticity control is in place
[T-5]	[T-SWI-8]	Interception of network traffic due to compromise of network infrastructure	High impact: the data integrity may be compromised in case the data authenticity control is NOT in place NOTE: Other impact levels may be expected according to the attack as follows: – Medium impact: the data may become unavailable both for the worker on site and central monitoring system – Low impact: the unencrypted data may be disclosed to unauthorized person

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-SWI-1] Compromise of wireless connections using rogue devices or devices infiltrated with malware	Absence or impossibility of installation of rogue wireless access points Impossibility of compromising devices that support wireless communications	Lack or inappropriateness of enforcement the wireless communications control.	Enforce the policy for the inventory and control of the wireless access points inside the perimeter where smart wearable devices are used	Implement input validation capability at the communication channel layer, including checks of wireless access points (Capability [C-7-1]) Implement the integrity and authenticity of commands and data at the communication channel layer, including protocol data encryption (Capability [C-7-1]) Implement input validation capability at the data interpretation layer, including checks of the commands and data (Capability [C-7-2]) Maintain the integrity and non-repudiation of commands and data at the smart device layer, including data encryption, checksum computation and signing (Capability [C-7-2]) Implement continuous monitoring for the rogue and unintended wireless access points (Capability [C-7-3], Capability [C-7-6]) Perform integration testing and validation for the combination of rules and policies regarding wireless communications (Capability [C-7-4])

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-SWI-2] Interception of short-distance communications	Short distance communications are unexposed to attacks	Lack or inappropriateness of enforcement the short-distance communications control	Avoid the use of legacy versions of short-distance communications (protocols, specifications, etc.) Ensure that used short distance communications employ all security features defined by their specifications	Implement checks of sources, protocols and flows of information using the available features of the short-distance communications (Capability [C-7-1]) Implement the integrity and authenticity of commands and data using the available features of the short-distance communications (Capability [C-7-1]) Implement the basic input validation at the smart wearable device, including checks of the commands and data (Capability [C-7-2]) Ensure the integrity and non-repudiation of commands and data validation at the smart wearable device using data encryption, checksum computation and signing (Capability [C-7-2]) Implement monitoring of short distance communications and their proper use where their features and specific properties allow such monitoring (Capability [C-7-3]) Ensure the ability to integrate the used security features of short-distance communications with other rules and policies enforcing security control (Capability [C-7-4]) Implement attack detection for the short distance communications where the features and specific properties of these communications require and allow this detection (Capability [C-7-5])

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
[T-SWI-3] Hindering wireless communications by suppressing or interfering with radio signal	There is no other sources of signal that could intentionally or accidently interfere with wireless communications	Lack or inappropriateness of enforcement the policy facilitating the stable radio signal	Enforce the policy for the control of non-interfering wireless communications and set the responsibility for enforcement of this policy	Check the radio signal at the frequency range intended for the valid communications (Capability [C-7-1]), Capability [C-7-3]) Implement detection of characteristics possibly related to the intentional or unintentional interference or hindering the valid radio signal (Capability [C-7-5])
[T-SWI-4] Exploiting remote control interfaces of the wearable device for getting control on it	Absence of any kind of vulnerability that may cause improper behavior of the smart wearable device Remote access interface unexposed to a malicious adversary	Improperly implemented data or command handling at the device	–	Ensure validation of sources, protocols and flows of information between the smart wearable device and external agents (Capability [C-7-1]) Maintain the authenticity of data at the communication channel layer (Capability [C-7-1]) Ensure data and command validation for the smart wearable device (Capability [C-7-2]) Ensure the integrity and non-repudiation of commands and data for the smart wearable device (Capability [C-7-2]) Implement a monitoring mechanism for ensuring the accountability and authenticity of all communications with smart wearable device(s) (Capability [C-7-3]) Ensure the proper and valid protection provided by different rules and policies for input validation at the device, channel and infrastructure layer (Capability [C-7-4]) Implement attack detection, including detection of probing, infrastructure attacks,

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
				remote attacks, insider attacks and misuse of smart wearable device (Capability [C-7-5])
[T-SWI-5] Exploiting the vulnerabilities of application level protocols for injecting the data into information flows from device to the central monitoring system and back	Absence of application level protocol vulnerabilities Remote access interface unexposed to a malicious adversary	Improper data or command handling by the protocol or its implementation	-	Ensure validation of sources, protocols and flows of information between the smart wearable device and external agents (Capability [C-7-1]) Maintain the integrity and authenticity of data at the communication channel layer (Capability [C-7-1]) Ensure data and command validation at the smart wearable device and central monitoring system (Capability [C-7-2]) Ensure the integrity and non-repudiation of commands and data at the smart wearable device and central monitoring system (Capability [C-7-2]) Implement a monitoring mechanism as a dedicated contract-based service(s), including the isolation of data obtaining and the analysing of monitoring components, isolation of emergency policy enforcement and an alarm mechanism, isolation and independent execution of the entire monitoring mechanism (Capability [C-7-3]) Ensure the proper and valid protection provided by different rules and policies for

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
				input validation at the device, channel and infrastructure layer (Capability [C-7-4]) Implement attack detection, including detection of probing, infrastructure attacks, remote attacks, insider attacks and misuse of smart wearable device (Capability [C-7-5])
[T-SWI-6] Exploiting the vulnerabilities of application level protocols for hindering the data exchange between the device and central monitoring system	Absence of application level protocol vulnerabilities Remote access interface unexposed to a malicious adversary	Improper data or command handling by the protocol or its implementation	-	Maintain the integrity and authenticity of data at the communication channel layer (Capability [C-7-1]) Ensure data and command validation at the smart wearable device and central monitoring system (Capability [C-7-2]) Ensure the integrity and non-repudiation of commands and data at the smart wearable device and central monitoring system (Capability [C-7-2]) Ensure the proper and valid protection provided by different rules and policies for input validation at the device, channel and infrastructure layer (Capability [C-7-4])
[T-SWI-7] General remote attack on smart wearable device or its malware infection	Absence of any kind of vulnerability that may cause improper behavior of the smart wearable device	Improperly implemented or configured authentication and authorization, including default credentials and weak password General vulnerabilities in command and data handling by the smart wearable device	Enforce the access, control and management policy for the smart wearable device	Maintain the integrity and non-repudiation of commands and data at the smart wearable device layer, including application data encryption, checksum computation and signing (Capability [C-7-2]) Implement a monitoring mechanism as a dedicated contract-based service(s), including the isolation of data obtaining and

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
	Remote access interface(s) unexposed to a malicious adversary			the analysing of monitoring components, isolation of emergency policy enforcement and an alarm mechanism, isolation and independent execution of the entire monitoring mechanism (Capability [C-7-3]) Ensure the proper integration of different rules and policies for security control at different layers if diverse technologies are employed by these layers (Capability [C-7-4])
[T-SWI-8]	Communications are reliable Management interface unexposed to a malicious adversary	Weak communication infrastructure Improperly implemented management and control for network infrastructure	Use the dedicated communication channel to access the management interface of the network devices, if such interface exists	Implement a reliable communication infrastructure, including resistance to channel overflow and denial of service attacks (Capability [C-7-1]) Ensure the integrity, authenticity and non-repudiation of commands and data at the communication channel layer, including protocol data encryption for communication infrastructure management (Capability [C-7-1], Capability [C-7-2]) Ensure the proper integration of different rules and policies for communication infrastructure management (Capability [C-7-4]) Implement the authentication and authorization of subjects before they attempt to manage and control the communication infrastructure (Capability [C-7-5]) Implement the mechanism or the ability to monitor attempts to manage and control the communication infrastructure (Capability

Table I.6 – Security requirements for the connected smart wearable device for industrial safety and productivity management

Threat	Possible wrong assumptions about things or environment	Type of defect exploited by an adversary	Prior countermeasures	Requirements
				[C-7-6]) Implement the mechanism to monitor the load on equipment and communication channels, including the detection of both unintentional overload and denial of service attacks (Capability [C-7-6])

Bibliography

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. https://www.iso.org/standard/66435.html

[b-GARTNER] Gartner, Inc., *Gartner Says Smartglasses Will Bring Innovation to Workplace Efficiency*. https://www.gartner.com/newsroom/id/2618415

[b-NIST CPS] Cyber Physical Systems Public Working Group. *Framework for Cyber-Physical Systems*, Release 1.0, May 2016. https://s3.amazonaws.com/nistsgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

[b-NISTIR 7298Rev2] NISTIR 7298 Revision 2. *Glossary of Key Information Security Terms*, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[b-WOOT] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek and J. Alex Halderman (2014). *Green Lights Forever: Analysing the Security of Traffic Infrastructure. Proceedings of the 8th USENIX Workshop on Offensive Technologies*. https://jhalderm.com/pub/papers/traffic-woot14.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound-programme and television-transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018