IEC TR 80001-2-9

Edition 1.0 2017-01

TECHNICAL REPORT

Application of risk management for it-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

IEC TR 80001-2-9:2017-01(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 80001-2-9

Edition 1.0 2017-01

TECHNICAL REPORT

Application of risk management for it-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 11.040.01, 35.240.80

ISBN 978-2-8322-3907-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 80001-2-9, which is a technical report, has been prepared by subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice, and ISO technical committee 215: Health informatics.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
62A/1097/DTR	62A/1128/RVDTR

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

Terms defined in Clause 3 of this standard are printed in SMALL CAPITALS.

A list of all parts of the 80001 series, published under the general title *Application of risk management for IT-networks incorporating medical devices*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

This document outlines a process for supporting CONFIDENCE in the use of the 80001 series by developing security ASSURANCE cases (henceforth SECURITY CASEs) to complement a security RISK MANAGEMENT process. IEC 80001-1 provides the roles, responsibilities and activities necessary for RISK MANAGEMENT.

IEC TR 80001-2-2 provides additional guidance in relation to how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT process and stakeholder communications and agreements phases. IEC TR 80001-2-2 contains an informative set of common, descriptive SECURITY CAPABILITIES intended to be the starting point for a security-centric discussion between the vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sizes of RESPONSIBLE ORGANIZATIONS (henceforth called healthcare delivery organizations – HDOs) as each evaluates RISK using the SECURITY CAPABILITIES and decides what to include or not to include according to their RISK tolerance, intended use and available resources. This information may be used by HDOs as input to their IEC 80001-1 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. IEC TR 80001-2-1 provides step-by-step guidance in the RISK MANAGEMENT PROCESS. IEC TR 80001-2-2 SECURITY CAPABILITIES encourages the disclosure of more detailed SECURITY CONTROLS.

IEC TR 80001-2-8 identifies SECURITY CONTROLS from key security standards which aim to provide guidance to HDOs, MEDICAL DEVICE manufacturers (MDMs) when adapting the framework outlined in IEC TR 80001-2-2 and establishing each of the SECURITY CAPABILITIES presented here. A SECURITY CAPABILITY, as defined in IEC TR 80001-2-2, represents a broad category of technical, administrative and/or organizational SECURITY CONTROLS[1)] required to manage RISKS to confidentiality, integrity, availability and accountability of data and systems. IEC TR 80001-2-8 presents these categories of SECURITY CONTROLS prescribed for a system to establish SECURITY CAPABILITIES to support the maintenance of confidentiality and the protection from intentional or unintentional intrusion that may lead to compromises in integrity or system/data availability. IEC TR 80001-2-8 provides HDOs and MDMs with a catalogue of technical, management, operational and administrative controls. IEC TR 80001-2-8 presents the 19 SECURITY CAPABILITIES, their respective “requirement goal” and “user need” (identical to that in IEC TR 80001-2-2) with a corresponding list of SECURITY CONTROLS from a number of security standards.

This document integrates the information and guidance contained in IEC TR 80001-2-2 and IEC TR 80001-2-8 together to provide guidance to HDOs and MDMs for identifying, developing, interpreting, updating and maintaining security ASSURANCE cases. Although other means of establishing CONFIDENCE in a particular property (e.g. security) exist, this document provides one such way in assuring CONFIDENCE in the establishment of IEC TR 80001-2-2 SECURITY CAPABILITIES through the use of SECURITY CASES. The purpose of the SECURITY CASE is to provide CONFIDENCE in the establishment of the IEC TR 80001-2-2 SECURITY CAPABILITIES for networked MEDICAL DEVICES. This is achieved by applying a SECURITY PATTERN to each of the 19 SECURITY CAPABILITIES. The objectives of the SECURITY PATTERN are as follows:

– to reduce the time required to develop the SECURITY CASE by providing a repeatable and systematic step-by-step, RISK based blue-print;
– provide a means to re-use components of the SECURITY PATTERN either within a SECURITY CASE or from one SECURITY CASE to another;
– to reduce the complexity often associated with the development of SECURITY CASES;
– provide a visible traceability matrix linking the SECURITY CONTROLS to the security threats and vulnerabilities identified during RISK MANAGEMENT;

---

1) For the purpose of consistency throughout this document, the terms SECURITY CONTROLS refer to the technical, management, administrative and organizational controls/safeguards prescribed to establish SECURITY CAPABILITIES.

– reduce the likelihood of missing a step in the ARGUMENT;
– improve the readability of the SECURITY CASE;
– provide CONFIDENCE regarding the integrity of the EVIDENCE collected based on the information presented in the ARGUMENT.

The process of developing the SECURITY CASE is not intended to replace a RISK MANAGEMENT process nor does it generate new processes, rather, the SECURITY CASE should complement the RISK MANAGEMENT process with a reference to, or, inclusion of the following supporting documentation by MDMs and HDOs:

– information regarding the intended use of the MEDICAL DEVICE, operational environment, network structure, interfaces, boundaries etc.;
– information regarding system description, security objectives and assets to be protected;
– justification for selection of SECURITY CAPABILITIES;
– justification for non-selection of SECURITY CAPABILITIES;
– assets being protected by specific SECURITY CAPABILITY;
– RISK acceptability criteria policy;
– all identified unacceptable threats/vulnerabilities;
– threat / vulnerability / RISK log;
– impact / threat scenario / consequence information;
– reference to source for selection of SECURITY CONTROLS (e.g. IEC TR 80001-2-8 tables).

The above information becomes part of, and remains with the SECURITY CASE from concept phase through to development, operation and retirement. Supporting information such as this can aid in better design choices, better maintenance during operation and more efficient and informative feedback practices.

This document is not intended to provide exhaustive guidance for the application of a RISK MANAGEMENT process nor does it mandate the use of any particular RISK MANAGEMENT process however IEC 80001-1 provides guidance on how to carry out RISK MANAGEMENT for medical IT-networks. Similarly, ISO 14971 provides guidance for the process of conducting RISK MANAGEMENT for MEDICAL DEVICES. For RISK MANAGEMENT processes such as RISK/benefit analysis, which is not covered in this document, HDOs refer to IEC 80001-1:2010, 4.4.5 and MDMs refer to ISO 14971,6.5.

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

1 Scope

This part of 80001 establishes a SECURITY CASE framework and provides guidance to health care delivery organizations (HDO) and MEDICAL DEVICE MANUFACTURERS (MDM) for identifying, developing, interpreting, updating and maintaining SECURITY CASES for networked MEDICAL DEVICES. Use of this part of 80001 is intended to be one of the possible means to bridge the gap between MDMs and HDOs in providing adequate information to support the HDOs RISK MANAGEMENT of IT-NETWORKS. This document leverages the requirements set out in ISO/IEC 15026-2 for the development of ASSURANCE cases[2)]. It is not intended that this SECURITY CASE framework will replace a RISK MANAGEMENT strategy, rather, the intention is to complement RISK MANAGEMENT and in turn provide a greater level of ASSURANCE for a MEDICAL DEVICE by:

– mapping specific RISK MANAGEMENT steps to each of the IEC TR 80001-2-2 SECURITY CAPABILITIES, identifying associated threats and vulnerabilities and presenting them in the format of a SECURITY CASE with the inclusion of a re-useable SECURITY PATTERN;
– providing guidance for the selection of appropriate SECURITY CONTROLS to establish SECURITY CAPABILITIES and presenting them as part of the SECURITY CASE pattern (IEC TR 80001-2-8 provides examples of such SECURITY CONTROLS);
– providing EVIDENCE to support the implementation of a SECURITY CONTROL, hence providing CONFIDENCE in the establishment of each of the SECURITY CAPABILITIES.

The purpose of developing the SECURITY CASE is to demonstrate CONFIDENCE in the establishment of IEC TR 80001-2-2 SECURITY CAPABILITIES. The quality of artifacts gathered and documented during the development of the SECURITY CASE is agreed and documented as part of a RESPONSIBILITY AGREEMENT between the relevant stakeholders. This document provides guidance for one such methodology, through the use of a specific SECURITY PATTERN, to develop and interpret SECURITY CASES in a systematic manner.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*[3)]

---

2) These requirements are adapted for networked MEDICAL DEVICES where the sole critical property is “security” and where the CLAIM relates to the establishment of the IEC TR 80001-2-2 SECURITY CAPABILITIES with the inclusion of a specific security ARGUMENT PATTERN.

3) IEC TR 80001-2-2 contains many additional standards, policies and reference materials which are also indispensible for the application of this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp.

3.1.1
ASSURANCE
grounds for justified CONFIDENCE that a CLAIM has been or will be achieved

[SOURCE: ISO/IEC 15026-1:2013, 3.1.1]

3.1.2
ARGUMENT
connected series of CLAIMS intended to establish an overall CLAIM

[SOURCE: GSN Community Standard Version 1:2011, 0.3]

3.1.3
CLAIM
proposition being asserted by the author that is a true or false statement

[SOURCE: GSN Community Standard Version 1:2011, Glossary]

3.1.4
CONFIDENCE
quality or state of being certain that the ASSURANCE case is appropriately and effectively structured, and correct

[SOURCE: Definition by: Grigorova, S., & Maibaum, T. S. E. (2013, November). Taking a page from the law books: Considering evidence weight in evaluating assurance case confidence. In *Software Reliability Engineering Workshops (ISSREW), 2013 IEEE International Symposium on* (pp. 387-390). IEEE. Definition: page 388]

3.1.5
EVIDENCE
information or objective artefacts being offered in support of one or more CLAIMS

[SOURCE: GSN Community Standard Version 1:2011, Glossary]

3.1.6
MEDICAL DEVICE
any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
   – diagnosis, prevention, monitoring, treatment or alleviation of disease,
   – diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
   – investigation, replacement, modification, or support of the anatomy or of a physiological process,

- supporting or sustaining life,
- control of conception,
- disinfection of MEDICAL DEVICES,
- providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry Products which can be considered to be MEDICAL DEVICES in some jurisdictions but for which there is not yet a harmonized approach, are:

- aids for disabled/handicapped people;
- devices for the treatment/diagnosis of diseases and injuries in animals;
- accessories for MEDICAL DEVICES (see Note to entry 3);
- disinfection substances;
- devices incorporating animal and human tissues which can meet the requirements of the above definition but are subject to different controls.

Note 3 to entry Accessories intended specifically by manufacturers to be used together with a 'parent' MEDICAL DEVICE to enable that MEDICAL DEVICE to achieve its intended purpose should be subject to the same GHTF procedures as apply to the MEDICAL DEVICE itself. For example, an accessory will be classified as though it is a MEDICAL DEVICE in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry Components to MEDICAL DEVICES are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'MEDICAL DEVICE'.

[SOURCE: IEC 80001-1:2010, 2.14]

3.1.7
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

Note 1 to entry This agreement can be a legal document, e.g. a contract.

[SOURCE: IEC 80001-1:2010, 2.21]

3.1.8
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

Note 2 to entry Adapted from IEC 60601-1:2005, 3.101.

[SOURCE: IEC 80001-1:2010, 2.22]

3.1.9
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, 2.23]

3.1.10
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

[SOURCE: IEC 80001-1:2010, 2.28]

3.1.11
SECURITY CAPABILITY
broad category of technical, administrative or organizational controls to manage RISKS to confidentiality, integrity, availability and accountability of data and systems

[SOURCE: IEC TR 80001-2-8:2016, 3.21]

3.1.12
SECURITY CASE
reasoned, auditable artefact created that supports the contention that its top-level CLAIM (or set of CLAIMS) is satisfied, including structured and explicit argumentation and its underlying EVIDENCE and explicit assumptions that support the CLAIM(s)

Note 1 to entry A SECURITY CASE contains the following and their relationships:

— one or more CLAIMS about the critical property security;

— ARGUMENTs that logically link the EVIDENCE and any assumptions to the CLAIM(s);

— a body of EVIDENCE and possibly assumptions supporting these ARGUMENTs for the CLAIM(s);

— justification of the choice of the top-level CLAIM and the method of reasoning.

[SOURCE: ISO/IEC 15026-1:2013, 3.1.3, modified — Adapted and amended definition of "ASSURANCE CASE" specifically addressing security as the critical property]

3.1.13
SECURITY CONTROL
management, operational, and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[SOURCE: FIPS Publication 199, Appendix A]

3.1.14
SECURITY PATTERN
a means of documenting and reusing successful security ARGUMENT structures

[SOURCE: Adapted and amended definition in Kelly, T.P., & McDermid, J.A. (1997). Safety Case Construction and Reuse using Patterns 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP' 97) (pp. 55-69): Springer London]

3.2 Abbreviated terms

ALOF	Automatic logoff
AUDT	Audit controls
AUTH	Authorization
CNFS	Configuration of security features
CSUP	Cyber security product upgrades
DIDT	Health DATA de-identification
DTBK	Data backup and disaster recovery
EMRG	Emergency access
IGAU	Health data integrity and authenticity
MLDP	Malware protection/recovery
NAUT	Node authentication
PAUT	Person authentication
PLOK	Physical locks on device
RDMP	Third party components and roadmaps
SAHD	System and application hardening
SGUD	Security guides
STCF	Health data storage confidentiality
TXCF	Transmission confidentiality
TXIG	Transmission integrity
MDM	MEDICAL DEVICE manufacturer
HDO	Healthcare delivery organization
SDLC	System/software development lifecycle

4 ASSURANCE case

An ASSURANCE case is a structured, EVIDENCE based ARGUMENT used to demonstrate CONFIDENCE that a system holds a particular critical property. ASSURANCE cases have been commonly applied to the safety domain, specifically addressing safety concerns for systems, however the use of ASSURANCE cases has expanded and nowadays address other critical properties such as dependability, reliability and security across a range of safety critical domains such as automotive, railway, defence, aviation etc. An ASSURANCE case is called a safety case when used to argue the safety of a system. Similarly they are referred to as SECURITY CASES and dependability cases when arguing security and dependability respectively.

A SECURITY CASE is required due to the associated security RISK related properties of certain MEDICAL DEVICES where CONFIDENCE is required to demonstrate security ASSURANCE of such MEDICAL DEVICES.

An ARGUMENT is a connected series of CLAIMS intended to establish an overall CLAIM. This hierarchy of CLAIMS presents the ARGUMENT of a SECURITY CASE. The ARGUMENT in a SECURITY CASE shows how a high-level CLAIM is supported by a number of child CLAIMS, which, in turn are supported by detailed presentation of EVIDENCE. It is the combination of CLAIMS and EVIDENCE that provide CONFIDENCE in the overall high level CLAIM for the SECURITY CASE. In demonstrating the security ASSURANCE of a MEDICAL DEVICE, it is difficult to see the adequacy of the EVIDENCE (e.g. test results) if no ARGUMENT supporting the CLAIM of the MEDICAL DEVICE exists. Presenting the ARGUMENT and EVIDENCE in a structured approach reduces the likelihood of uncertainty and allows for a better analysis of the achievement of the set of objectives (the CLAIMS).

The SECURITY CASE also provides a mechanism for capturing supporting information (by means of additional notations which can form part of an ARGUMENT) in the form of assumptions, justifications and context. This information supports rationale and decision making while developing, interpreting and updating the SECURITY CASE.

5 Use of this document

5.1 Intended use

The following subclause outlines the use of this document for MDMs and HDOs.

5.2 Intended audience

5.2.1 Intended purpose

This document is intended to supply MDMs and HDOs with guidance for the development, interpretation, updating and maintenance of SECURITY CASES. It specifically guides MDMs, HDOs and other stakeholders for supporting a security dialogue through the use of ASSURANCE cases as a shared approach between all stakeholders. This document details the application of SECURITY CASES by providing examples with the use of Goal Structure Notation (GSN) while acknowledging that other annotations and other means to communicate are also applicable.

5.2.2 MEDICAL DEVICE MANUFACTURERS (MDM)

This document provides guidance to MDMs for developing a SECURITY CASE to demonstrate CONFIDENCE in the achievement of IEC TR 80001-2-2 SECURITY CAPABILITIES for the purpose of providing HDOs with the appropriate level of information to adequately support the HDO's RISK MANAGEMENT of MEDICAL DEVICES on a MEDICAL DEVICE IT-network.

A SECURITY CASE should be treated as a 'living document' that is continuously developed maintained and updated during design, production and operation of a MEDICAL DEVICE maintaining the traceability between the SECURITY CONTROLS, security RISKs and their associated SECURITY CAPABILITIES CLAIMS. Treating a SECURITY CASE as a 'living' document during operation of a MEDICAL DEVICE will aid in gathering operational information and adoption to a changing threat landscape.

A MDM should commence development of the SECURITY CASE at the outset of the system/software development lifecycle (SDLC).

Using this document, a SECURITY CASE will provide a traceability matrix between identified security RISKs and relating SECURITY CONTROLS and SECURITY CAPABILITIES.

A SECURITY CASE can form part of a broader ASSURANCE case for a MEDICAL DEVICE addressing other system critical properties such as safety, reliability, usability etc.

A SECURITY CASE can be developed by MDMs to demonstrate the security ASSURANCE of a MEDICAL DEVICE to HDOs.

The SECURITY CASE may act as a support document to the Manufacture Disclosure Statement (MDS^2) which also utilizes IEC TR 80001-2-2 SECURITY CAPABILITIES.

In the event of an incident concerning a MEDICAL DEVICE, the SECURITY CASE is useful for analysis and also to provide information/feedback to HDOs.

5.2.3 Healthcare delivery organizations (HDO)

ASSURANCE cases can be applied to any level of an IT-network which can support the entire HDO IT-network addressing any network component e.g. the radiology network, network communication components, MEDICAL DEVICES, accessories and even components of devices.

HDOs can use the SECURITY CASE, as outlined in this document, to form part of a broader ASSURANCE case addressing additional critical properties such as safety, reliability, maintainability etc. Similarly, a SECURITY CASE for one MEDICAL DEVICE on an IT-network can form part of a larger MEDICAL DEVICES IT-network SECURITY CASE.

However, a CLAIM "The object xyz is secure" will not make sense in every case, e.g. on a device level, the achievement of required security ASSURANCE may depend on whether the device is protected by malware protection in the network infrastructure or users are for instance restricted access by organizational policies. In other words, acceptable security for a MEDICAL DEVICE IT-network requires the combined effort of the HDO, MDM and other stakeholders.

Security is not limited to technical measures and may also require administrative measures e.g. access controls at the users site or field monitoring and patch processes at MDMs site.

SECURITY CASES with their layered approach are a means to cope with such complex situations. In general, it is a best practice to start on a level that a HDO has chosen as its object to apply RISK MANAGEMENT to. This might be part of a medical IT-network and so the CLAIM might be "This part of the medical IT-network is secure". This CLAIM will then be supported by a set of ARGUMENTS which will eventually lead to a CLAIM for a single MEDICAL DEVICE that is part of the medical IT-network. However, this CLAIM for a specific MEDICAL DEVICE is not necessarily "the MEDICAL DEVICE xyz is secure" but instead the CLAIM may be for a specific (set of) property (properties) of the MEDICAL DEVICE. Typical properties of a MEDICAL DEVICE that relate to security are given in IEC TR 80001-2-2.

HDO's should use this document for one or more of the following:

a) evaluate a SECURITY CASE to determine the extent of achievement of the IEC TR 80001-2-2 SECURITY CAPABILITIES for a particular MEDICAL DEVICE; or

b) develop a complete SECURITY CASE for a MEDICAL DEVICE on an IT-network, as per Clause 5; or

c) further develop a received MDM SECURITY CASE to include additional specific threats/vulnerabilities related to the environment and also EVIDENCE of any operational or administrative controls implemented in the operational environment.

The information contained in a SECURITY CASE will support HDO decision makers in determining the following:

a) establishing suitability of a MEDICAL DEVICE for a specific environment;

b) identifying use-environment security RISKs which may require RISK treatment (based on information provided by a MDM SECURITY CASE);

c) knowledge and understanding of design choices taken by MDM;

d) knowledge of understanding of actions required by HDO to maintain a MEDICAL DEVICE as per the documented intended use;

e) improved knowledge and understanding of network RISK MANAGEMENT requirements based on MDMs information.

In the event of an incident concerning a MEDICAL DEVICE, the SECURITY CASE is useful for analysis of such incidents and also for the purpose of information sharing / feedback to MDMs.

5.2.4 Other stakeholders

Stakeholders (involved in conformity assessment, certification, regulation, acquisition or audit) can evaluate the SECURITY CASE to determine the extent of achievement of the top-level CLAIM (establishment of the SECURITY CAPABILITIES) by the MEDICAL DEVICE and whether this achievement is demonstrated within the allowable uncertainty or RISK and any related consequences. The results regarding the top-level CLAIM and its support along with related uncertainties and consequences constitute a basis for rationally managing RISK, achieving grounds for appropriate CONFIDENCE, and aiding in decision making.

6 General guidelines

6.1 General

The following guidelines apply when developing and interpreting a SECURITY CASE:

a) The components[4)] of a SECURITY CASE should be unambiguous, identifiable, and accessible.

b) Each component should be uniquely identified and should be able to have its origin identified, its history ascertained, and its integrity assured.

c) Detailed supporting artifacts, which have been developed elsewhere, should be identified in the "context[5)]" component and should be accessible.

d) For each component, the component's contents, the information related to it, and the other components with which it has relationships should be identifiable and accessible.

e) For each component, its description and required components, e.g. EVIDENCE for CLAIMS and related information such as test case results, should be identifiable and accessible.

f) Where a particular SECURITY CAPABILITY is deemed necessary[6)], a CLAIM relating to the establishment of that SECURITY CAPABILITY should be developed.

g) For each SECURITY CAPABILITY, a SECURITY PATTERN (as outlined in Clause 7) which comprises of a number of specific components should be utilized.

6.2 Overview of the SECURITY CASE framework

The following includes recommendations for the use of this document:

a) All 19 SECURITY CAPABILITIES should be considered for inclusion in the SECURITY CASE giving consideration to the 'user needs', intended use, operational environment, interfaces, identified RISKS functionality etc.

b) Where a SECURITY CAPABILITY is not required (due to any of the considerations in a)), justification for omission should be documented in the SECURITY CASE.

c) Selection of a SECURITY CAPABILITY is justified by the MEDICAL DEVICE assets protected by that SECURITY CAPABILITY.

d) Threats/vulnerabilities which are identified during RISK MANAGEMENT should be presented in the SECURITY CASE which is developed until an adequate solution for mitigation (SECURITY CONTROL) is identified.

e) The inclusion of the associated impact or consequence is also documented (as context) on the SECURITY CASE.

---

4) ISO/IEC 15026-2 uses the term "components" for the main parts of the SECURITY CASE to describe the structure and contents.

5) Context may include, but is not restricted to, definitions of the terms used, description of environment context, output from threat and vulnerability identification practices and the identities of entities responsible for a component's development or maintenance.

6) Based on communicated 'user needs' and results from requirements gathering and RISK management activities.

f) The SECURITY PATTERN includes the SECURITY CONTROLS that are selected to mitigate the associated threat or vulnerability (to support the SECURITY CAPABILITY). SECURITY CONTROLS required to establish the SECURITY CAPABILITIES may be selected from IEC TR 80001-2-8. IEC TR 80001-2-8 provides a catalogue of SECURITY CONTROLS for each SECURITY CAPABILITY.

g) Selection of SECURITY CONTROLS is based on the MEDICAL DEVICE intended use, operational environment, context and RISK acceptability criteria.

h) SECURITY CONTROLS should be applied until the residual RISK is deemed acceptable based on the RISK acceptability policy.

i) MDMs may document the EVIDENCE in the SECURITY CASE (e.g. test results, reports, etc.) or provide reference to it.

j) Determination, selection, acceptability and sharing of EVIDENCE is an agreement among the relevant stakeholders. Such information should be documented and may form part of a stakeholder RESPONSIBILITY AGREEMENT.

k) The sharing, extent and use of proprietary information within a SECURITY CASE should also be documented and form part of a stakeholder RESPONSIBILITY AGREEMENT.

l) It is recommended that MDMs using this framework supply the SECURITY CASE to HDOs with the MEDICAL DEVICE.

m) With this information, HDOs should identify their 'on-site' SECURITY CONTROLS (e.g. policies, procedures etc.) for the MEDICAL DEVICE on the IT-network. The SECURITY CASE is maintained in order to show any additional EVIDENCE in terms of additional of implementation of IT-network SECURITY CONTROLS.

n) The SECURITY CASE should form part of HDO RISK MANAGEMENT file (RMF) and should be maintained and updated as necessary. The SECURITY CASE may also be useful as a mechanism for feedback to MDMs in the case of an incident, identified unacceptable RISKS or change regarding the IT-network.

Clause 7 provides instructions for developing the SECURITY CASE with the inclusion of a SECURITY PATTERN.

6.3 Notation

6.3.1 Components of a SECURITY CASE

This clause outlines the components of a SECURITY CASE in notation form along with associated extensions. All components are required in developing the SECURITY CASE. A SECURITY CASE requires a structured ARGUMENT (hierarchy of CLAIMS) supported by EVIDENCE. There are numerous formats and notation types that can be used for developing the SECURITY CASES. As an example, this document uses Goal Structure Notation (GSN) to present the SECURITY CASE. GSN is not a tool but a mature notation, standardised and widely used [6].[7] This notation has also been extended to allow for abstractions to support patterns of re-usable reasoning.

6.3.2 Goal

A goal is a CLAIM or proposition to be assured about a particular MEDICAL DEVICE and is a true-false statement. It may be accompanied with supporting components such as "Assumption", "Justification" or "Context". Within the SECURITY CASE, CLAIMS are supported by sub-CLAIMS where the set of sub-CLAIMS make up the body of the ARGUMENT. Figure 1 below shows the SECURITY CASE top-level CLAIM. The ARGUMENT describes the relationship between the CLAIM and the EVIDENCE and is therefore critical for the establishment of CONFIDENCE in the EVIDENCE obtained.

---

[7] Numbers in square brackets refer to the bibliography.

This SECURITY CASE framework utilizes a SECURITY PATTERN. The use of a SECURITY PATTERN provides a repeatable process to develop the SECURITY CASE while maintaining the structure for the SECURITY CASE. An instantiated SECURITY PATTERN may be reusable from one SECURITY CASE to another or within a SECURITY CASE.

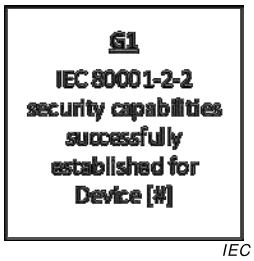


Figure 1 – Example GOAL (top-level)

6.3.3 Strategy

The strategy describes the nature of the reasoning that exists between a CLAIM and its sub-CLAIMS. Figure 2 shows the strategy which is used in the SECURITY CASE framework to link the top-level CLAIM to the ARGUMENT.

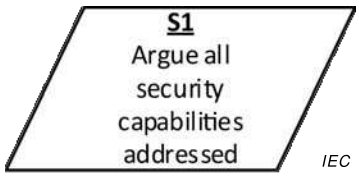


Figure 2 – Example strategy

6.3.4 Justification

Because the choice of a CLAIM is critical to meet the objective of the SECURITY CASE some CLAIMS will require justification for their selection. In order to provide CONFIDENCE in the reason for selection (or non-selection) and establishment of SECURITY CAPABILITIES, justification for non-selection of SECURITY CAPABILITIES is required in every case. Where it is justified that a particular SECURITY CAPABILITY is not required, the SECURITY PATTERN will not be developed any further. Figure 3 shows an example of how justification uses the RISK analysis results to justify the non-selection of a particular SECURITY CAPABILITY.

Figure 3 – Example justification

6.3.5 Context

Because the choice of a top-level CLAIM and its property is critical in order to meet the objective of a SECURITY CASE, the context in which the CLAIM or reasoning step is made should be captured. A top-level CLAIM shall have an associated context outlining the user need, intended use, operational environment etc. Figure 4 shows an example of a context component with reference to system description, interfaces, boundaries and assets.

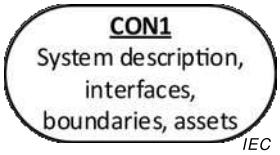


Figure 4 – Example context

6.3.6 Solution (EVIDENCE)

An ARGUMENT continues until a CLAIM or sub-CLAIM is supported by EVIDENCE to support the truth of that CLAIM. Asserted EVIDENCE for all ARGUMENTs within the SECURITY CASE provides CONFIDENCE in the top-level goal (CLAIM). Figure 5 shows an example of EVIDENCE relating to the identified threats and vulnerabilities.

Figure 5 – Example solution (EVIDENCE)

6.3.7 Stakeholder

This is a form of context symbol which is used to indicate the stakeholders outlining any communicated SECURITY CAPABILITIES associated in some way with the goal to which it is attached. Figure 6 shows an example of a stakeholder component with reference to SECURITY CAPABILITIES that may have been specified by HDO.

Figure 6 – Example stakeholder

6.3.8 Notation extensions

Table 1 below further expands the notation with a set of notation extensions.

Table 1 – Notation extensions

Extension	Description
	SupportedBy Line with rendered arrowhead indicating an inferential or evidential relationship.
	InContextOf Line with hollow arrowhead indicating a contextual relationship.
	An arrow with a black dot indicates multiplicity (zero to many) expressed in *n*.
	A diamond expressing the need for further development with sub-CLAIMS or EVIDENCE.
	This indicates the need to instantiate or replace a component with an actual document or findings etc.
	A black diamond indicates optionality.

7 Developing the SECURITY CASE

This clause outlines the steps required to develop a SECURITY CASE to demonstrate CONFIDENCE in the establishment of IEC TR 80001-2-2 SECURITY CAPABILITIES. Figure 7 and Table 2 (SECURITY CASE leading components) and Figure 8 and Table 3 (SECURITY CASE pattern) below presents the reusable SECURITY PATTERN steps in their hierarchical format.

The SECURITY PATTERN (Steps 10 through Step 24 below) should be repeated (each with uniquely identifiable ID's) for each of the 19 SECURITY CAPABILITIES from IEC TR 80001-2-2 to develop the entire SECURITY CASE by demonstrating CONFIDENCE in each of the SECURITY CAPABILITIES. CONFIDENCE is demonstrated when residual RISK meets the criteria of the specified RISK acceptability policy through the implementation of SECURITY CONTROLS.

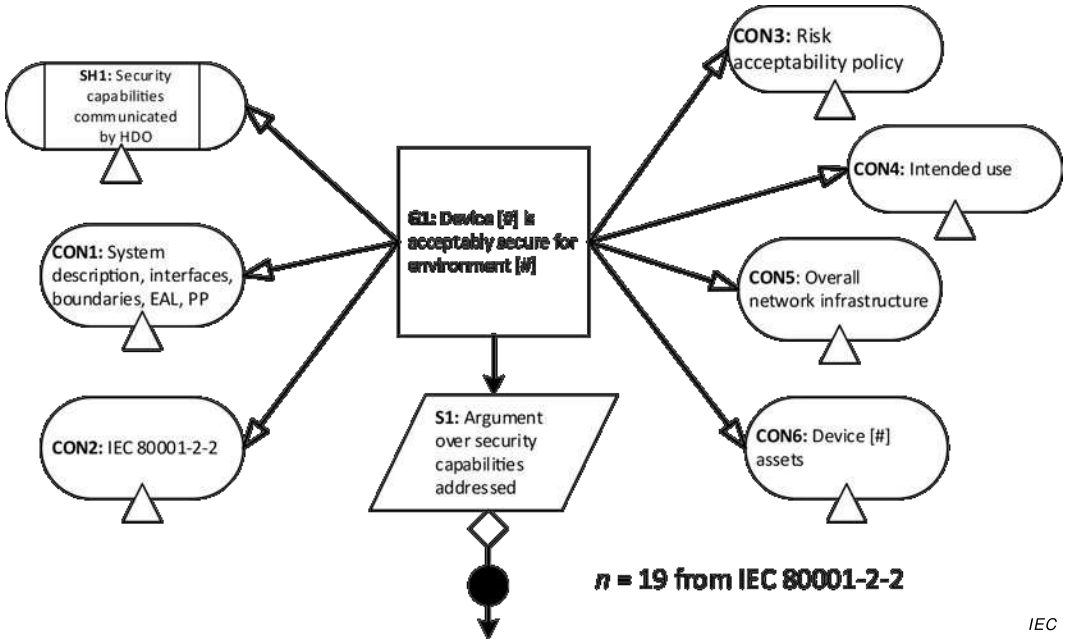


Figure 7 – Leading components – Steps 1 through 9

Table 2 – SECURITY CASE steps 1 through 9

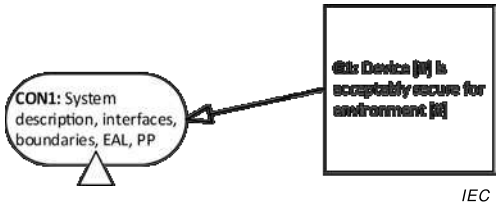
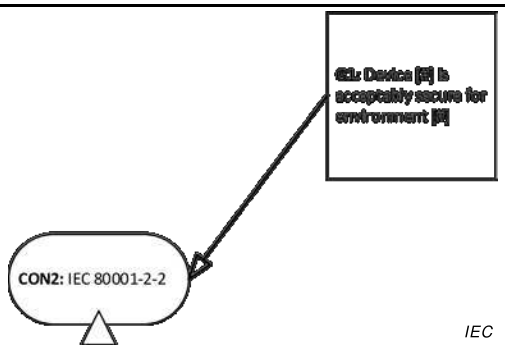
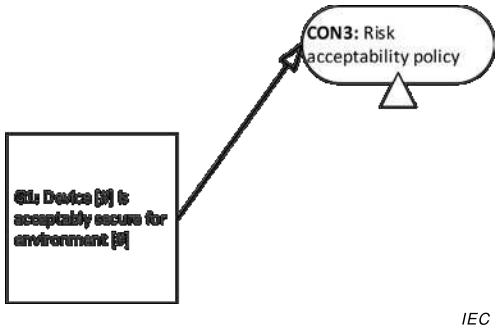
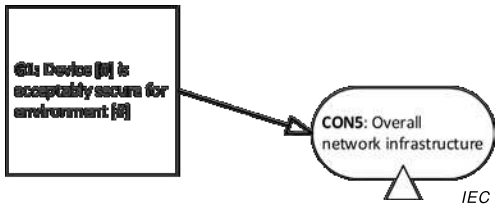
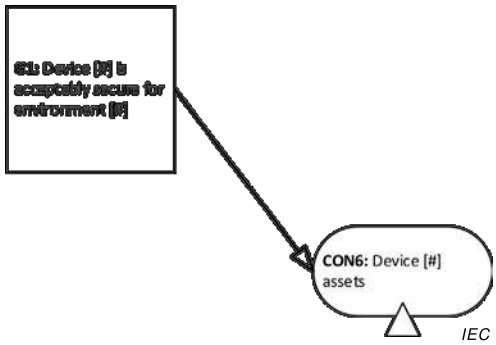
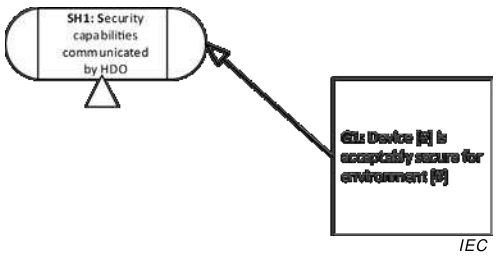
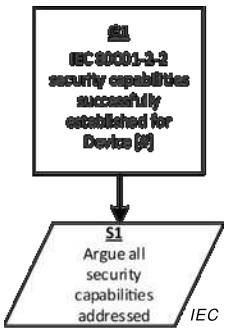
Step	ID	Description	Notation
1	G1	***Goal*** **State the top CLAIM** This is the top goal for the SECURITY CASE which CLAIMS that a particular device, device [#], is secure for a particular environment, environment [#].	 IEC
2	CON1	***InContextOf*** **What is Device [#]?** This context component should describe the MEDICAL DEVICE, interfaces, boundaries etc. Where a protection profile (PP) is required, or an evaluation ASSURANCE level (EAL) is assigned to a MEDICAL DEVICE, this should be included here as a rationale for selection/application of SECURITY CONTROLS.	 IEC
3	CON2	***InContextOf*** **What are the SECURITY CAPABILITIES?** Reference to parent standard for SECURITY CAPABILITIES – IEC TR 80001-2-2.	 IEC
4	CON3	***InContextOf*** **What is acceptable RISK for Device [#]?** This context information should detail acceptable RISK and reference a RISK acceptability criteria policy.	 IEC
5	CON4	***InContextOf*** **What is the intended use for Device [#]?** This context component should outline information pertaining to the intended use of the MEDICAL DEVICE [#], operational environment, network structure, etc.	 IEC
6	CON5	***InContextOf*** **What is the platform for Device [#]?** This context component should outline information pertaining to assumptions relating to the intended platform hosting MEDICAL DEVICE [#].	 IEC

Table 2 – SECURITY CASE steps 1 through 9 *(continued)*

Step	ID	Description	Notation
7	CON6	***InContextOf*** What assets is Device [#] protecting? This context information should detail all identified assets for Device [#].	
8	SH1	***Stakeholder*** What SECURITY CAPABILITIES (if any) were communicated by HDO for Device [#]? Information regarding HDO or HDO security requirements should be included (referenced to) here.	
9	S1	***Strategy*** What strategy is adopted to support G1? Apply a strategy to address all 19 security from IEC TR 80001-2-2 capabilities.	

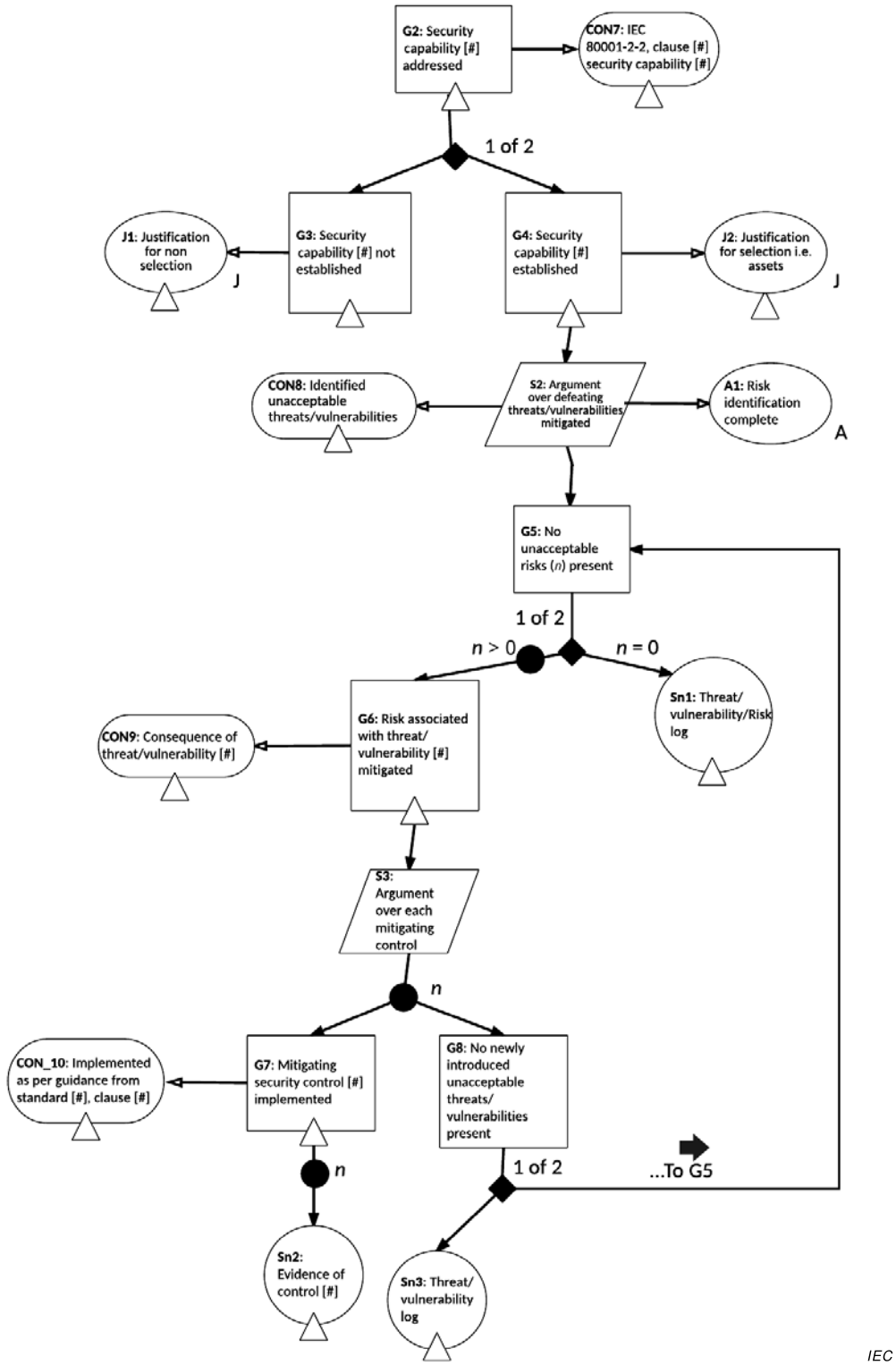


Figure 8 – SECURITY CAPABILITY pattern

Table 3 – SECURITY CASE steps 10 through 26

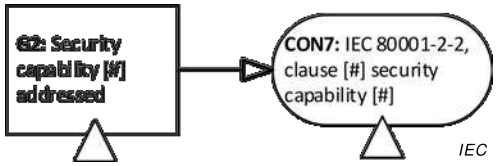
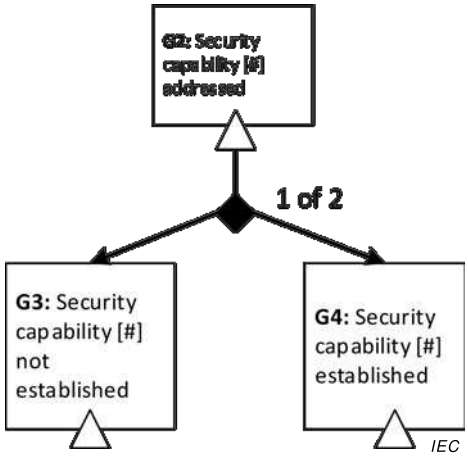
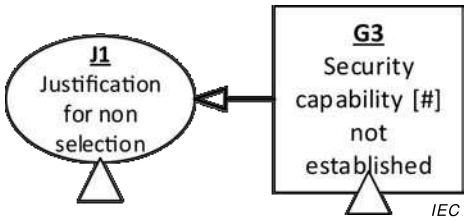
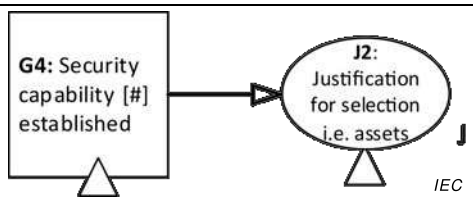
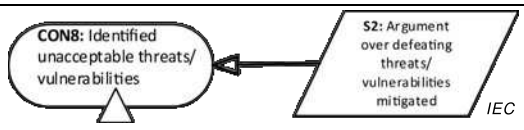
Step	ID	Description	Notation
10	G2	***Goal*** **Address SECURITY CAPABILITY [#]** For each SECURITY CAPABILITY, a CLAIM to specifically address each one should be included. The arrow with a black dot indicates there are 19 (*n*) SECURITY CAPABILITIES which should be addressed individually.	
11	CON7	***InContextOf*** **What is SECURITY CAPABILITY [#]** Include or make reference to the description of SECURITY CAPABILITY [#] including requirement goal, user need.	
12	G3 **Or** G4	***Goal – Optionality*** **Assert to establish or omit the SECURITY CAPABILITY** Either G3 or G4 child-goal should be developed here. The black diamond represents optionality (G3 or G4).	
13	J1	***Justification*** **Why is SECURITY CAPABILITY [#] not required?** The reason SECURITY CAPABILITY [#] has not been selected should be included as a justification for the CLAIM G3.	
14	J2	***Justification*** **Why is SECURITY CAPABILITY [#] required?** Details of the asset(s) which SECURITY CAPABILITY [#] protects should be included here as justification for G4.	
15	CON7	***InContextOf*** **What threats/vulnerabilities were identified?** For SECURITY CAPABILITY [#], include (or make reference to) all defeating threats/ vulnerabilities identified.	

Table 3 – SECURITY CASE steps 10 through 26 *(continued)*

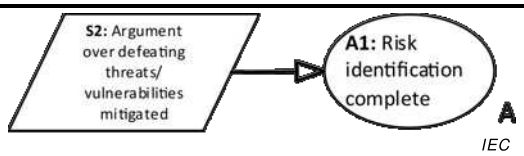
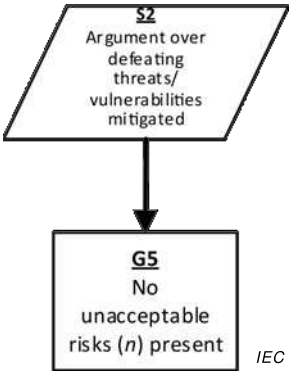
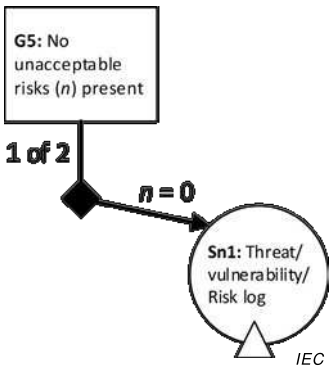
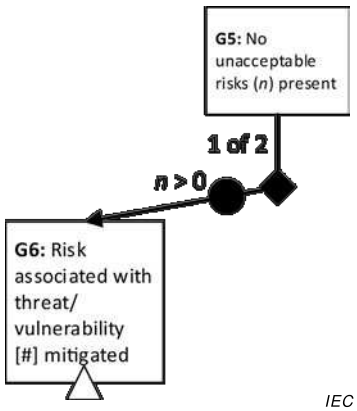
Step	ID	Description	Notation
16	A1	***Assumption*** **Support the validity of S2** S2 relies on the assumption that the process of RISK identification has been carried out. This may include responsible person name, date RISK identification commenced, completed etc.	
17	G5	***Goal*** **For the identified threats/vulnerabilities, what level of RISK remains?** CLAIM that no unacceptable RISKs remain for SECURITY CAPABILITY [#].	
18	Sn1 OR	***Optionality/Solution*** **Where no unacceptable RISKs exist, EVIDENCE should be provided to support this.** (n=0) In order to provide CONFIDENCE in this assertion (G5), solution Sn1 should be instantiated. Records of threat/vulnerability log should be included to indicate no remaining unacceptable RISKs. For all remaining RISKs requiring RISK reduction, G6 should be developed.	
19	G6	***Optionality/Goal*** **Where unacceptable RISK exists, what threats/vulnerabilities require RISK reduction?** Each threat/vulnerability presenting unacceptable RISK should be explicitly stated here to be addressed in the following sub-goals. When developing the SECURITY CASE there may be a number of CLAIMS in parallel to this depending on the number of threats and vulnerabilities requiring RISK treatment. This is indicated by the arrow with a black dot and $n > 0$.	

Table 3 – SECURITY CASE steps 10 through 26 *(continued)*

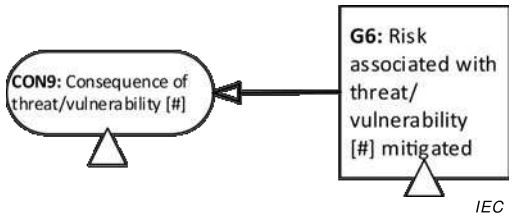
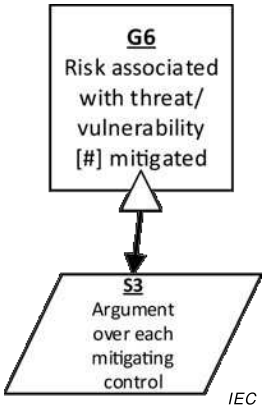
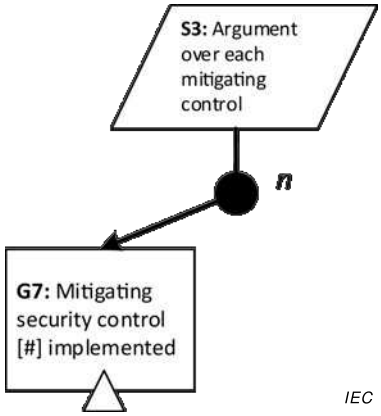
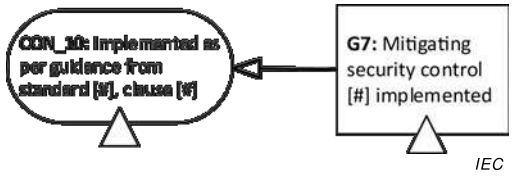
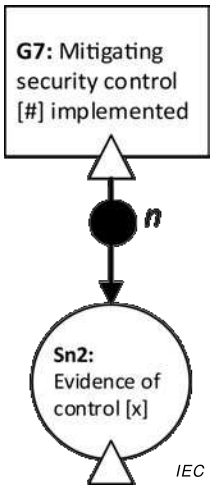
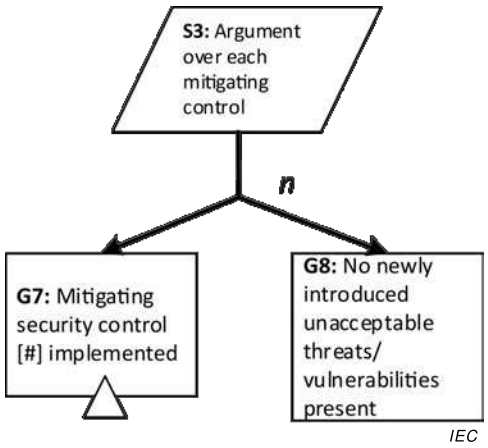
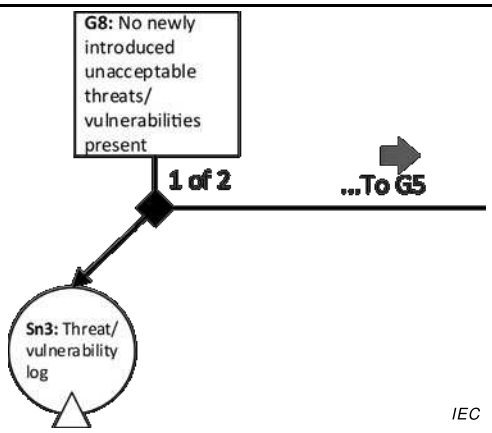
Step	ID	Description	Notation
20	CON9	***InContextOf*** **What is the associated consequence of this?** Details of consequence associated with identified threats/vulnerabilities (and unacceptable RISK) should be included (or referenced to) in context of G6.	
21	S3	***Strategy*** **Change the strategy to address the SECURITY CONTROLS** The strategy of the ARGUMENT should change to address RISK control measures for threat/vulnerability [#].	
22	G7 **G8**	***Goal*** **What SECURITY CONTROLS reduce the RISK associated with threat/vulnerability [#]?** For each mitigating SECURITY CONTROL, assert that SECURITY CONTROL [#] has been implemented. **AND** When developing the SECURITY CASE there may be a number of CLAIMS in parallel to this. SECURITY CONTROLS should be applied until the residual RISK is deemed to be acceptable.	
23	CON_10	***InContextOf*** Identify the source for the selected SECURITY CONTROL to support CLAIM G7. Include (or reference) the source of the SECURITY CONTROL selected.	

Table 3 – SECURITY CASE steps 10 through 26 *(continued)*

Step	ID	Description	Notation
24	Sn2	***Solution*** **Provide EVIDENCE of the implementation of the SECURITY CONTROL** For each mitigating SECURITY CONTROL, provide reference or traceability to verification report(s).	
25	G8	***Goal*** **Have any new unacceptable threats /vulnerabilities been introduced with the implementation of SECURITY CONTROL [#]?** For each mitigating SECURITY CONTROL, assert that newly introduced threats/vulnerabilities are not present.	
26	Sn3	***Solution*** **No newly introduced unacceptable threats / vulnerabilities identified** Provide EVIDENCE to show that all RISKs have been reduced to an acceptable level. NOTE Where a new threat / vulnerability is introduced, revert to CLAIM G5 and repeat the steps in the SECURITY CASE.	

The complete SECURITY CASE structure is shown in Figure 9. The components shaded represent the resuable SECURITY PATTERN.

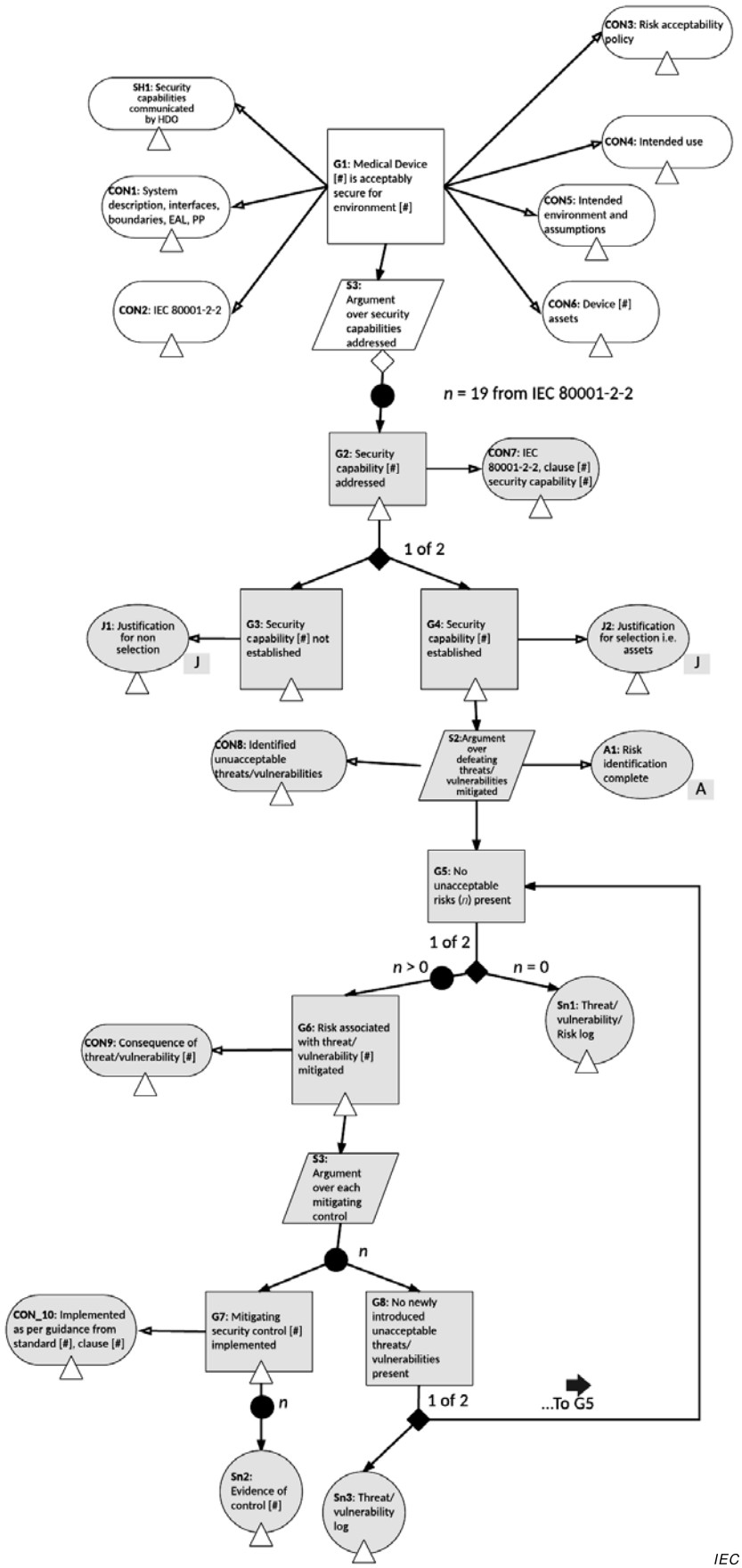


Figure 9 – SECURITY CASE structure

8 SECURITY CASE change management

A SECURITY CASE should be treated as a live document reflecting the current state of the security of a MEDICAL DEVICE or a MEDICAL DEVICE IT-network. For the purposes of traceability, change management procedures should be applied to reflect this SECURITY CASE lifecycle. A simple change management or document revision system would suffice in maintaining this. Where it is simply the context or EVIDENCE that changes this should be made clear by the reference or citations shown within the context or solution components.

The SECURITY CASE can be revised by 1) editing a component of the SECURITY CASE, 2) adding a new component or 3) removing a component.

Examples of when a SECURITY CASE should be revised include the following non-exhaustive scenarios:

a) the supporting information used to inform the development of the SECURITY CASE changes e.g. changes to the intended use of a MEDICAL DEVICE, operational environment, interfaces etc.;

b) an incident occurs which requires reporting and/or mitigation;

c) a MEDICAL DEVICE is added to a MEDICAL DEVICE IT-network;

d) a MEDICAL DEVICE is removed from a MEDICAL DEVICE IT-network;

e) additional SECURITY CAPABILITIES or other SECURITY CONTROLS are required to further protect MEDICAL DEVICE assets;

f) additional SECURITY CAPABILITIES or other SECURITY CONTROLS are required as a result of a change to the MEDICAL DEVICE IT-network;

g) additional security capabilities or other SECURITY CONTROLS are required as a result of new threats/vulnerabilities arising from already established SECURITY CONTROLS;

h) additional SECURITY CAPABILITIES or other SECURITY CONTROLS are required as a result of ongoing RISK MANAGEMENT activities, where new RISKS with potential to impact a MEDICAL DEVICE or MEDICAL DEVICE IT-network are identified.

Annex A
(informative)

Exemplar SECURITY PATTERNS

A.1 General

The following are examples of a SECURITY PATTERN for the SECURITY CAPABILITIES person authentication (PAUT), automatic logoff (ALOF) and audit controls (AUDT). Figure A.1, Figure A.2 and Figure A.3 reference IEC TR 80001-2-8 as the resource for selection of SECURITY CONTROLS. IEC TR 80001-2-8 presents a catalogue of SECURITY CONTROLS from a number of security standards. These SECURITY CONTROLS can be used to establish each of IEC TR 80001-2-2 SECURITY CAPABILITIES.

These examples are not exhaustive in covering a MEDICAL DEVICE or an entire medical IT-network. Rather, they show a "core path" to a specific property of a MEDICAL DEVICE, a SECURITY CAPABILITY, and further develop to details of the MEDICAL DEVICE that are related to that SECURITY CAPABILITY. It is assumed that showing this core path provides an example that is useful for both HDOs and MDMs.

A.2 Exemplar SECURITY PATTERN for person authentication (PAUT) — SECURITY CAPABILITY PAUT established by MDM for a medical system[8)]

A.2.1 Goal G6: Replay attack mitigated

Context CON9: Attacker attempts to replay login

Goal G7: Detect replay attacks

Solution Sn4: Implement the control as defined in ISO/IEC 15408-2 – FTP_RPL

A.2.2 Goal G8: 'Man-in-the-middle' attack mitigated

Context CON11: Attacker attempts to intercept communication

Goal G9: Detect 'man-in-the-middle' attacks

Solution Sn5: Implement the cryptography control as defined in IEC 62443-3-3, SR 4.3

A.2.3 Goal G10: Brute force attack mitigated

Context CON13: Attacker attempts to brute force passwords

Goal G12: Detect brute force attacks

Solution 1, Sn6: Implement 'unsuccessful login attempt' control as defined in IEC 62443-3-3, SR 1.11

Solution 2, Sn6: Implement 'Strength of password-based authentication control as defined in IEC 62443-3-3, SR 1.7

---

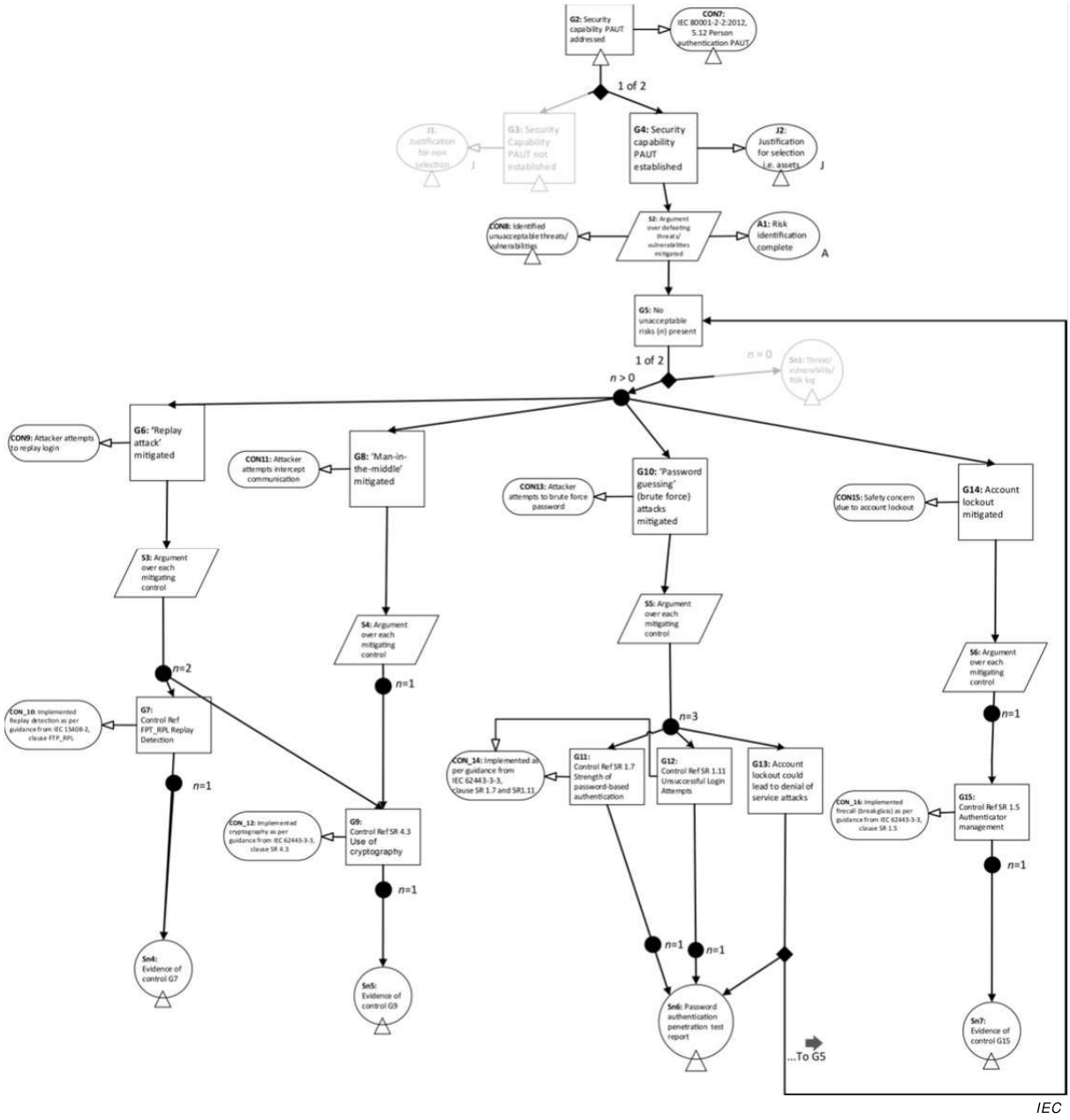
8) In this example, lightly shaded components (CLAIMS, EVIDENCE) represent components that do not require development.

A.2.4 Goal G13, G14: Denial of service attacks due to account lockout controls mitigated

Context CON15: Safety concerns introduced due to security account lockout controls

Goal G15: Account lockout mitigated

Solution Sn7: Implement 'Authenticator management' control as defined in IEC 62443-3-3, SR 1.5



NOTE Watermarked components in this figure represent those from the pattern that have not been developed from the security pattern for this particular example.

Figure A.1 – Exemplar SECURITY PATTERN for PAUT

A.3 Exemplar SECURITY PATTERN for automatic logoff (ALOF) established for a thin client terminal system[9)]

A.3.1 Goal: Patient safety RISK with short session timeouts in OR mitigated

Context: The default timeout of 30 min gives a concern to a MEDICAL DEVICE used in operating room (OR) where medical staff is busy with the patient and less frequently work on the terminal station causing it to timeout while the patient is still being treated.

Goal: Control session timeout based on location

Solution: Define longer session timeout, but only for systems located in the OR. This can be accepted because this area has physical access control.

A.3.2 Goal: Patient safety RISK with restoring sessions in the OR and ICU mitigated

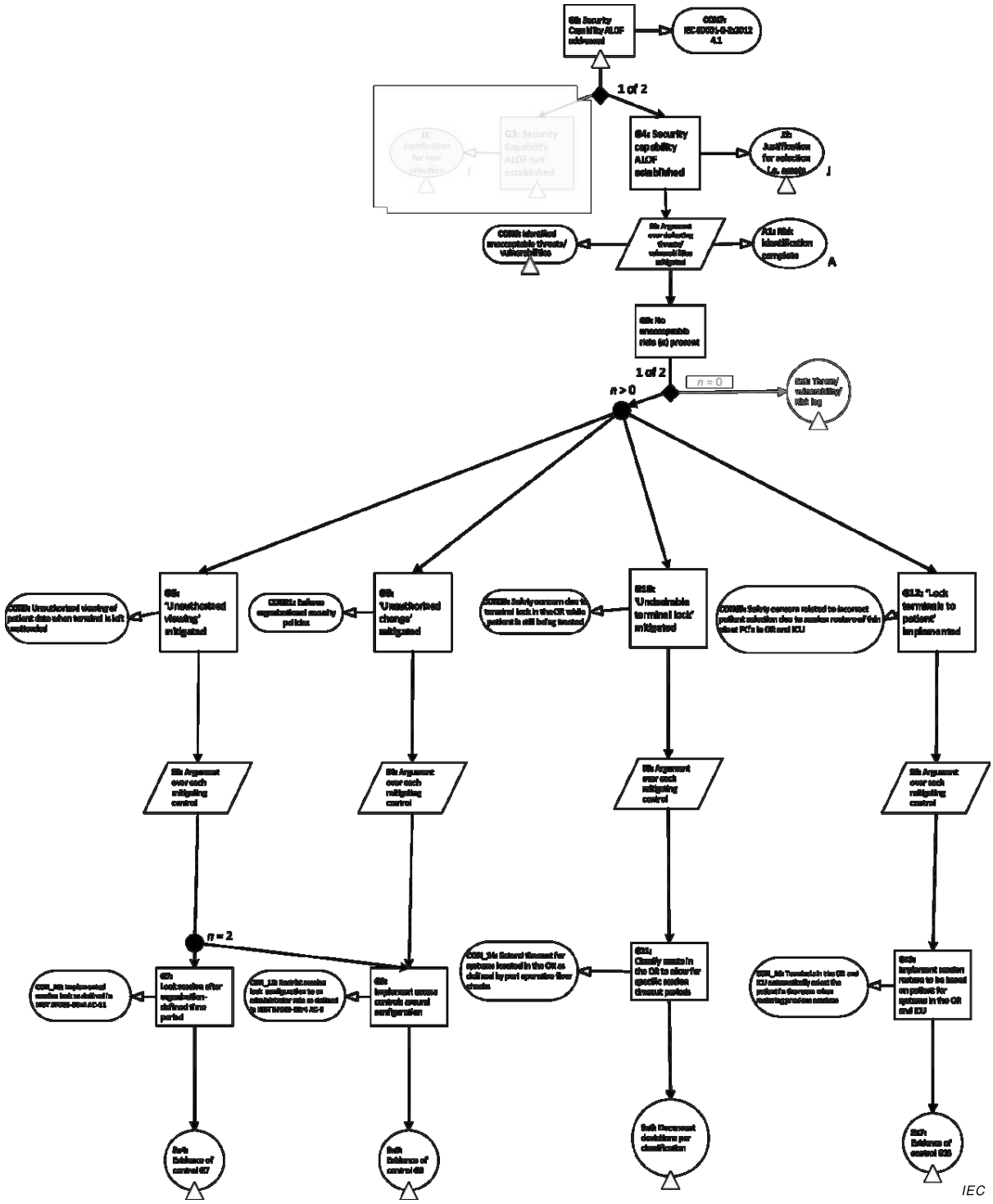
Context: The advantage of a thin client solution is the ability to log off on one terminal station and resume work on another. But in an OR and intensive care unit (ICU) setting this could lead to safety concerns if for instance an anaesthetist is assisting in two rooms and the system would restore the session of the wrong patient.

Goal: Control sessions based on location

Solution: Thin client terminal stations such as electronic medical record (EMR) systems in an OR and ICU should always present the patient being treated in that room instead of completely restoring the session of the user logging into the system

---

9) In this example, lightly shaded components (CLAIMS, EVIDENCE) represent components that do not require development.



NOTE Watermarked components in this figure represent those from the pattern that have not been developed from the security pattern for this particular example.

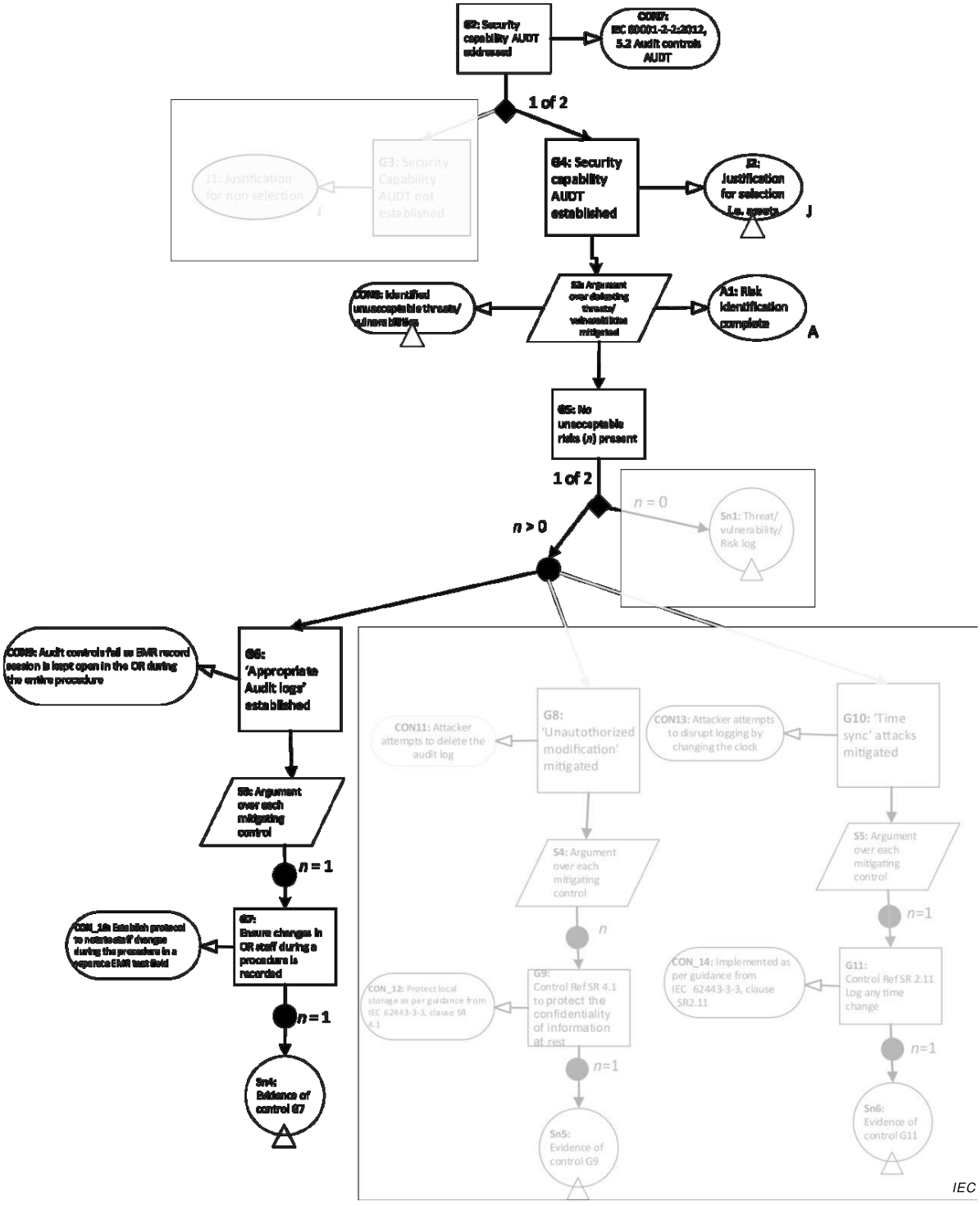
Figure A.2 – Exemplar SECURITY PATTERN for ALOF

A.4 Exemplar SECURITY PATTERN for audit controls (AUDT) for a system or a device in a HDO facility such as a pharmacy system or an EMR, where multiple people require access to the same data set— Goal G6: Keep a correct audit trail of attending staff in the OR while sessions are kept open

Context: Within the OR, the session is kept open and locked to the patient. If the person who opened the session has to leave the OR (e.g. their shifts ends) there shall be a record of the handover without closing the session.

Goal: Keep a correct log of people access the medical record.

Solution: Establish protocol whereby a change in medical staff during a procedure shall be recorded in a text field.



NOTE In this example, watermarked notations represent components of the SECURITY CASE which were shared from a MDM.

Figure A.3 – Exemplar SECURITY PATTERN for AUDT

Bibliography

[1] IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities*

[2] IEC TR 80001-2-1:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples*

[3] IEC TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*

[4] ISO/IEC 15026-1:2013 *Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary*

[5] ISO/IEC 15026-2:2011 *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*

[6] GSN Community Standard Version 1, Consulting (York) Ltd. (2011), http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

[7] HIMSS/NEMA Standard HN 1-2013, *Manufacturer Disclosure Statement for MEDICAL DEVICE Securit*

[8] ISO 14971, *Medical devices – Application of risk management to medical devices*

[9] IEC 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*

[10] ISO/IEC 15408-2*, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*

[11] IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[12] Grigorova, S., & Maibaum, T. S. E. (2013, November). Taking a page from the law books: Considering evidence weight in evaluating assurance case confidence. In *Software Reliability Engineering Workshops (ISSREW), 2013 IEEE International Symposium on* (pp. 387-390). IEEE. Definition: page 388]

[13] FIPS, PUB. "199." Standards for Security Categorization of Federal Information and Information Systems 2 (2004)

[14] Kelly, T.P., & McDermid, J.A. (1997). Safety Case Construction and Reuse using Patterns 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP' 97) (pp. 55-69): Springer London

[15] IEC 80001 (all parts), *Application of risk management for IT-networks incorporating medical devices*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch