VDE SPEC

Medical Devices – Risk Management: Framework of a Computerized Risk Analysis Format for Transmission and Submission (MD-CRAFTS)

VDE SPEC 90025 V1.0 (en)

VDE

Foreword

Publication date of this VDE SPEC: 09.07.2024

No draft has been published for the present VDE SPEC.

This document was prepared by the VDE SPEC project group "MD Crafts" of VDE Association for Electrical, Electronic & Information Technologies (Verband der Elektrotechnik Elektronik Informationstechnik e.V.) (www.vde.com).

This VDE SPEC resulted from the project "KIMEDS" (funding code 13GW0552A)", funded by The German Federal Ministry of Education and Research (BMBF).

This VDE SPEC was developed according to the VDE SPEC procedure in a project group and not necessarily with the involvement of all interested parties.

This VDE SPEC is **not** part of the VDE set of regulations or the German set of standards. In particular, this VDE SPEC is **not** a technical rule within the meaning of Section 49 EnWG.

The authors of this VDE SPEC are:

- Hans Wenner, VDE e.V. (chair)
- Dr. Georg Heidenreich, Siemens Healthineers AG (co-chair)
- Dr. Dörthe Arndt, TU Dresden
- Philipp Bank, KLS Martin SE & Co. KG
- Piotr Gorczyca, TU Dresden
- Pascal Kettmann, TU Dresden
- Dr. Stephan Mennicke, TU Dresden
- Dr. Martin Neumann, infoteam Software AG
- Dr. Hannes Straß, TU Dresden
- Dr. Sarah Tsurkan, TU Dresden
- Uwe Zeller, Zeller-Ingenieurdienstleistung

Executive Summary

Medical device risk management per EU MDR is a highly regulated activity, supported by established international standards. One artifact of risk management is the device risk management file which contains a list of “risks” – describing the evaluation and control of unintended scenarios potentially leading to harm. This document specifies a structured representation of such a device risk management file for the digital capturing, exchange, and archive of medical device risk information.

Contents

List of figures

1 Scope

1.1 Purpose

This document describes a structured, electronic exchange format for risk assessment and control information. This exchange format supports documentation of risk management for a given medical device according to ISO 14971. This document does not describe how to perform risk management in general, neither the chronological sequence nor the logical procedure.

1.2 Field of application

This document applies to the development, review, conformity assessment and maintenance of medical devices with respect to risk management activities. The respective file is called the Digital Risk Management File (DRMF). Stakeholders (e.g. device manufacturers, authorities) can document, archive, review and transfer structured information on risk (including risk assessment and risk control) for a given medical device using the format specified in this document.

1.3 Overview

Clause 3 defines the terms used in this specification and Clause 4 describes the acronyms and abbreviations.

Clause 5 describes a static, object-oriented model of the conceptual classes, their attributes and their relations towards a device Digital Risk Management File (DRMF) for a single medical device.

Clause 6 introduces the *Abstract Storage Format* with very basic requirements for device-related ("master") files.

Clause 7 describes the *Export File Format* based on requirements on top of the *Abstract File Format*, for representations of human-readable and machine-processable device information, for the purpose of temporary storage within a given organization and a given information processing environment.

Clause 8 is informative. Its first section introduces a series of consistency rules based on the conceptual model of the DRMF. The second section explains how to link conceptual model artifacts to HTML elements - in order to lay the foundations for representing the DRMF with HTML.

Clause 9 describes the *Exchange Format* on the basis of requirements on top of the *Export File Format* using HTML representations of a device Digital Risk Management File (DRMF). The purpose of the *Exchange Format* is human-readability, long-term storage and exporting a Digital Risk Management File (DRMF) out of the IT environment in which it was created, while preserving a structure and markup that relates to the DRMC conceptual model - for the purpose of digital processing.

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.

Unless otherwise stated, the references within this document refer to the dates as stated in this section (dated reference). The websites were last accessed 2024-02-19.

- [MDR] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)
- [ISO14971] ISO 14971 – Medical Devices – Application of Risk Management to Medical Devices, 2019
- [ISO24971] ISO/TR 24971 – Medical Devices – Guidance on the Application of ISO 14971, 2020
- [NCIt] National Cancer Institute Thesaurus (NCIt): reference terminology and ontology. NCIt provides responsive, science-based terminology concepts used in NCI semantic infrastructure and information systems. Available for download at https://ncit.nci.nih.gov/.
- [w3c] World Wide Web Consortium (W3C) – (https://www.w3.org/)
- [html] W3C HTML Specification (https://html.spec.whatwg.org/)

- [rdfa1] W3C RDFa Primer (https://www.w3.org/TR/rdfa-primer/)
- [rdfa2] rdfa.info (https://rdfa.info/)
- [riskman-ontology] The RISKMAN Ontology (https://w3id.org/riskman/docs/)
- [generic-rdfa] Statistics regarding the use of generic RDFa among all websites (https://w3techs.com/technologies/details/da-genericrdfa)
- [css] W3C CSS Specification (https://www.w3.org/Style/CSS/Overview.en.html)
- [rdfa] W3C RDF (https://www.w3.org/RDF/)

3 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:

– ISO Online browsing platform: available at https://www.iso.org/obp

– IEC Electropedia: available at https://www.electropedia.org/

3.1 ISO 14971 Terms

3.1.1
Harm

injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO 14971, 3.3, which refers to ISO/IEC Guide 63, 3.1]

3.1.2
Hazard

potential source of harm

[SOURCE: ISO 14971, 3.4, which refers to ISO/IEC Guide 63, 3.2]

3.1.3
Hazardous situation

circumstance in which people, property or the environment is/are exposed to one or more hazards

[SOURCE: ISO 14971, 3.5, which refers to ISO/IEC Guide 63, 3.3]

3.1.4
Intended use, intended purpose

use for which a product, process, or service is intended according to the specifications, instructions and information provided by the manufacturer

[SOURCE: ISO 14971, 3.6, which refers to ISO/IEC Guide 63, 3.4]

3.1.5
Objective evidence

data supporting the existence of verity of something

[SOURCE: ISO 14971, 3.11, which refers to ISO 9000:2015, 3.8.3, modified]

3.1.6
P1

probability of the occurrence of a hazardous situation

Note to entry: In concrete documentation instances, P1 may be detailed further by specifying separate probabilities, with each single one related to a specific hazard

[SOURCE: ISO 14971, C.1]

3.1.7
P2

probability of a hazardous situation leading to harm

[SOURCE: ISO 14971, C.1]

3.1.8
Residual risk
risk remaining after risk control measures have been implemented

[SOURCE: ISO 14971, 3.17, which refers to ISO/IEC Guide 63, 3.9]

3.1.9
Risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 14971, 3.18, which refers to ISO/IEC Guide 63, 3.10, modified]

3.1.10
Risk analysis
systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO 14971, 3.19, which refers to ISO/IEC Guide 63, 3.11]

3.1.11
Risk control
process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

[SOURCE: ISO 14971, 3.21, which refers to ISO/IEC Guide 63, 3.12]

3.1.12
Safety
freedom from unacceptable risk

[SOURCE: ISO 14971, 3.26, which refers to ISO/IEC Guide 63, 3.16]

3.1.13
Severity
measure of the possible consequences of a hazard

[SOURCE: ISO 14971, 3.26, which refers to ISO/IEC Guide 63, 3.17]

3.1.14
State of the art
developed stage of technical capability at a given time as regards products, processes, and services, based on the relevant consolidated findings of science, technology, and experience

Note to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the “generally acknowledged state of the art”.

[SOURCE: ISO 14971, 3.28, which refers to ISO/IEC Guide 63, 3.18]

3.2 MDR Terms

3.2.1
Intended purpose
the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation

[SOURCE: MDR (EU Regulation 2017/745), Art. 2, (12)]

3.2.2
Instructions for use
information provided by the manufacturer to inform the user of a device’s intended purpose and proper use and of any precautions to be taken

[SOURCE: MDR (EU Regulation 2017/745), Art. 2, (14)]

3.3 Introduced Terms

3.3.1
Analyzed risk
combination of one or more domain-specific hazard(s) with one hazardous situation and one harm with reference to a device context and a specification of an initial risk level

Note 1 to entry: The specified risk level refers to the severity of the harm and the probability of the harm occurring in the given hazardous situation.

Note 2 to entry: The probability of the risk level can be given implicitly by specifying P1 and P2 separately within the analyzed risk.

Note 3 to entry: The risk level makes implicit reference to the device-specific risk matrix.

3.3.2
Assurance SDA
SDA where the purpose is to make a safety assurance

3.3.3
Assurance SDAI
SDAI of an assurance SDA

3.3.4
Controlled risk
structured artifact that relates one analyzed risk with one or more SDA(s) and specifies a resulting residual risk

Note to entry: Controlled Risks may make (direct or indirect) references to P1 and P2 when specifying residual risks.

3.3.5
Device component
a (physical or logical) part of a device

3.3.6
Device context
information concerning the use context of a device, including, but not limited to, (1) intended use/intended purpose, (2) instructions for use, and (3) intended environment of use

3.3.7
Device function
functional device capability at application level

3.3.8
Domain-specific hazard
structured artifact that centers around one hazard having the potential to cause one or more harm(s) in the context of a domain-specific function and component

Note 1 to entry: This artifact is intended to be reusable across different devices from the same domain, e.g. domain “radiology”.

Note 2 to entry: A domain-specific hazard can feature in one or more analyzed risks (by potentially contributing to one or more hazardous situation(s)).

3.3.9
Event
atomic occurrence or incident that (possibly when linked in a sequence with other events) may spawn a hazardous situation from a domain specific hazard

3.3.10
Implementation manifest
concrete piece of objective evidence (or a reference to such) that an SDA has been implemented, e.g. reference to a line of code or a particular section in the device manual

3.3.11
Intended environment of use
environment or environmental conditions in which the device is intended to be used

3.3.12
Risk matrix
matrix (two-dimensional table) displaying all combinations of probability and severity classes without determining which of those combinations are acceptable

3.3.13
Risk SDA
SDA where the purpose is to control a risk

3.3.14
Risk SDAI
SDAI of a Risk SDA

3.3.15
Risk level
combination of probability and severity

Note 1 to entry: In combination with a specific harm, this constitutes a risk.

Note 2 to entry: When specifying risk levels in documentation, the necessary harm to constitute a risk is given indirectly via analyzed risk.

3.3.16
Safety assurance
a credible reference (or list of such) to the state of the art of achieving safety with respect to a certain class of hazards, e.g. referring to an international norm such as IEC 60601

3.3.17
SDA (Safe design argument)
reusable artifact embodying or expressing one possible method or approach towards a specific goal

3.3.18
SDAI (SDA implementation)
structured artifact specifying a concrete implementation or realization of a specific SDA

3.3.19
Use-Context
intended/reasonably foreseeable environment the device can be used in, that may affect a related risk

4 Abbreviations / Acronyms

4.1 General

The Requirements and Recommendations are built as follows:

Context	Delimiter	Rigor	Delimiter	Description
XXX	_	DEF or REQ or INF	_	Text

No “Space” allowed – “underscore” used instead.

4.2 Description of Identifiers used in this document

4.2.1 Explanation of Rigor

4.2.1.1 DEF

Definition of a term, used in the defined structured format. When using a defined term, the term must be used in accordance with this definition.

4.2.1.2 REQ

Required content in the structured Risk Management File, i.e. at least one instance must be present.

4.2.1.3 INF

Recommendation: it is recommended to implement this specification; however, it is not required for conformance.

4.2.2 Example

EXF_REQ_HTML refers to a mandatory requirement in Chapter “Exchange Format”, describing “HTML”.

4.2.3 Conformance

In the context of this document, the adherence to “REQ” (Requirement) is required to achieve conformance with the defined structured format. It is advisable to follow the recommendations, too.

The fulfilment of all requirements and recommendations does not indicate whether the risk analysis as such is complete.

5 Conceptual Model

5.1 Introduction

This clause introduces the overall conceptual model

- applying the established standard ISO 14971 “Medical Devices – Risk Management”,
- and introducing some further practical concepts -
- in order to describe the meaning and purpose of elements used for documenting the risk analysis and risk control measures.

With the aim of generating a comprehensive and consistent Digital Risk Management File (DRMF) (“file”), the definitions given in this clause are expressed as requirements towards the responsible entity acting as the device manufacturer (“manufacturer”),
where the DRMF file owner – for the purposes of this specification – is a role typically taken by an assigned expert (natural person).

A common misunderstanding is that ISO 14971 uses the same term for a general concept and a specific instance of that concept. This can be confusing to users, and additional terminology can help clarify this discrepancy.

Examples of a concept and instance:

- Risk, which has the definition “combination of the probability of occurrence of harm and the severity of that harm”, yet in practice, manufacturers routinely identify a Risk as an instance of an identified hazard leading to a specific harm;
- Harm, which is defined as an abstract “injury or damage to the health of people, or damage to property or the environment”, but in practice, manufacturers must identify a specific instance of Harm, such as “Serious Burn” or “Death”.

As a solution, this clause introduces some larger container concepts with associated terms in order to resolve these inconsistencies.

5.2 Foundations

5.2.1 MOD_REQ_HARM

The manufacturer shall model each identified unintended “injury or damage” (harm) resulting from the intended or foreseeable ways of using a device, as an instance of *Harm*.

So as a first step in applying ISO 14971, we clearly need to distinguish from a concept (“class”) and its “instances” (of *Harm*) in the scope of the specific device.

Note: Using a vocabulary with rather general terms for injury or damage can avoid unnecessary fragmentation of the risk analysis. As an example, when considering different health effects resulting from ‘the same’ physical contusion caused by some identified motoric drive, the risk manager may select one specific (‘most severe possible outcome’) for characterizing the harm of contusion by that motor.

5.2.2 MOD_DEF_COMP

The manufacturer shall model each relevant element of the device’s static composition as an instance of *DeviceComponent*. The term “system” may be used to denote the device as a whole. Abstract terms, related to a family of devices, can be used to describe a *DeviceComponent* that is commonly used within multiple device types.

5.2.3 MOD_DEF_FUNCTION

The manufacturer shall model each relevant element of the device’s dynamic behavior as an instance of *DeviceFunction*. Abstract terms, related to a family of devices, can be used to describe a *DeviceFunction* that is commonly implemented by multiple device types.

Note: This can include internal functions, user-initiated functions, service functions, automatic device activities, startup, shutdown, stand-by, or even device capabilities and features like e.g. communication, processing or storage/retrieval.

5.2.4 MOD_REQ_HAZARD

The manufacturer shall model each identified hazard.

Note 1: A *Hazard* is a potential source of *Harm*. Example: Flammable material is a *Hazard*. Flammable material is likely to catch fire (hazardous situation) and exposure to fire can cause *Harm*. A *Hazardous Situation* is a circumstance - e.g. a fire by burning flammable material.

Note 2: The above-mentioned dual-use of *class* and *object* also occurs with the definition of *Hazard* – defined as "the potential to cause that abstract *Harm*" (hazard) – and its use in the normative part of that standard: While the instances of *Hazard* describe the identified capabilities of the device to cause a potential *Harm*, there are more specific instances of Harm in the context of an identified device.

Note 3: Since the term risk describes a combination of quantifications of probability and severity ("risk level") of a situation linked to harm or damage, the following specification provides an additional construct examining the conjunction of exactly one *Hazard* instance and its contribution to one potential *Harm*.

5.2.5 MOD_REQ_DSH

The manufacturer shall model for each combination of potential *Harm*, *Hazard*, *Function*, or *Component*, which is relevant for the type of device, one instance of *DomainSpecificHazard*.

Note 1: This document introduces the concept of *DomainSpecificHazard* as the "container" object to represent the domain knowledge about hazards related to the general functioning and composition of a type of medical device. The concept of *DomainSpecificHazard* is the basis for linking potential *Harm* to relevant *Hazard* instances.

Note 2: As further instruments for supporting risk analysis, the *DomainSpecificHazard* captures *DeviceComponent* and *DeviceFunction* as practical elements of the static composition or dynamic behaviour of the device design. Manufacturers (i.e. risk managers) can arbitrarily chose the granularity of instances of *Harm* and *Hazard* in order to better appropriately structure the resulting list of *DomainSpecificHazards*.

Note 3: This model supports the collection of domain-specific knowledge from a specific device. *DomainSpecificHazard* does not reflect the time-sequence of causes, events, and any resulting impact.

Note 4: When beginning a new Digital Risk Management File (DRMF), the file initially can be pre-populated with instances of *DomainSpecificHazards*, collecting all instances of potential *Harm*, *Hazard* and *HazardousSituation*, *DeviceComponent* and *DeviceFunction* that are relevant for the device's domain.

5.3 Risk evaluation

As a result of risk assessment, each relevant *DomainSpecificHazard* can be linked to the set (one or multiple) of concrete *HazardousSituation* (instances) which result from that hazard.

5.3.1 MOD_DEF_SITUATION

The manufacturer shall model each device state (of use) possibly resulting in *Harm* as an instance of *HazardousSituation*.

Note: In order to document the relation between an identified *HazardousSituation*, which had been identified during risk analysis of a given *DomainSpecificHazard*, to a specific *Harm* and the resulting risk level we need the concept of *AnalyzedRisk* as a "container structure".

5.3.2 MOD_DEF_ARI

In the context of a given *DomainSpecificHazard*, the manufacturer shall model each

- relevant hazardous situation, together with
- the resulting specific *Harm*, and
- the initial risk assessment (risk level),

as an instance of *AnalyzedRisk*.

Note 1: *AnalyzedRisk* serves as the basis for analyzing the resulting *Risk* (given by the *Harm* and the risk level) from the *HazardousSituation* considered in the context of some *DomainSpecificHazard*.

Note 2: When analyzing all risks related to a new Digital Risk Management File (DRMF), new instances of *AnalyzedRisk* capture the progress of assessing the specific hazardous situations and the resulting harms and unmitigated (initial) risk levels for each of the pre-populated *DomainSpecificHazards*.

5.4 Risk control

5.4.1 MOD_DEF_COR

In the context of a given *AnalyzedRisk*, the manufacturer shall model

- any control measures and the
- residual risk

as an instance of *ControlledRisk*.

Note 1: A *ControlledRisk* specifies *how to* lower risk and refers to the technical solution of that risk reduction. Such technical solutions are specified or referenced by RiskSDAs which are referenced by the respective *ControlledRisk*.

Note 2: When controlling all risks related to a new Digital Risk Management File (DRMF), for each of the existing instances of *AnalyzedRisk*, one new instance of *ControlledRisk* captures the progress of adding mitigations and assessing the resulting residual risk level.

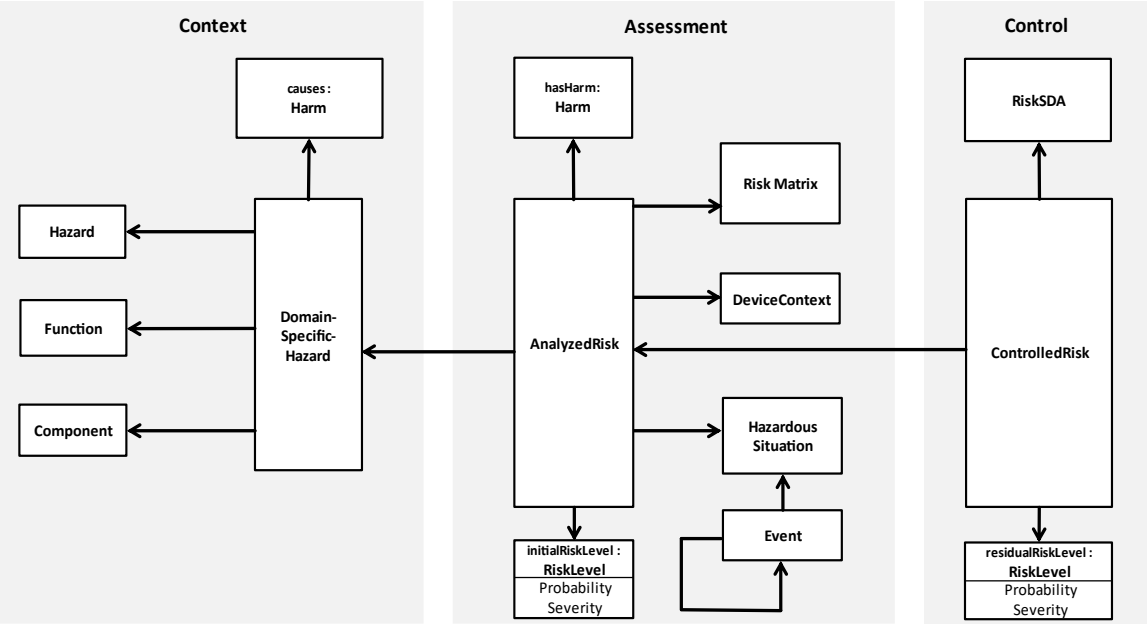


Figure 1 – Risk file concepts (informative)

5.4.2 MOD_DEF_SDA

For each *ControlledRisk* the manufacturer shall model the risk control reasoning as one instance of *RiskSDA* which manages the

- *cause* – of the problem being addressed.
- *goal* – of the intended result of risk reduction, i.e. lower probability and/or lower severity, and the
- *problem* – expressing the specific technical condition, which is being addressed by the control measure, and the
- *strategy* of effective risk reduction.

Note 1: *RiskSDAs* represent the elements of a hierarchical safety reasoning as described by the Assurance Case method (see ISO 15026). One *RiskSDA* instance combines the goal and the strategy of a given assurance case. An example could be the claim that seat belts in an airplane prevent and lower the severity of bodily injuries, caused by uncontrolled touch-down, combined with a reasoning how that is achieved.

Note 2: The *cause* is one of the events leading to the *problem*. In the context of *ControlledRisk* it can be set with the *HazardousSituation* addressed by the associated *DomainSpecificHazard*. In the general case of nested SDAs, the *cause* is any unexpected event contributing to the *problem* addressed by that *RiskSDA*. An example could be the *HazardousSituation* of an uncontrolled airplane touch-down.

Note 3: The *goal* describes the intended result of risk reduction. For RiskSDAs, this attribute is meant in an inverse fashion: The effective goal is to *reduce* the risk. An example could be the prevention of bodily injury and lowering its severity when a passenger is being restrained by a seat-bealt during the crash of an airplane.

Note 4: The *problem* is an abstraction of *Hazard*. In the context of *ControlledRisk* it can be set with the *Hazard* addressed by the related *DomainSpecificHazard*. In the general case of nested SDAs, the *problem* is any adverse technical condition that is addressed by the controls implemented by that *RiskSDA*. An example could be the *Hazard* of uncontrolled movements and accelerations resulting from uncontrolled airplane touch-downs.

5.4.3 MOD_DEF_STRATEGY

For each *RiskSDA* the manufacturer shall model the risk control as one instance of *Strategy* which manages the

- *argument*, describing how the combination of supporting measures (*Assurance*) prevents harm or lowers its severity, and the
- *solution*, presenting external references to design and implementations of control measures, and a
- list of *Assurance* instances supporting the reasoning.

Note 1: The *argument* attribute is related to the *cause* of the parent *SDA* and either has the value PREVENT or ALLEVIATE. An example could be that ("seat belts") ALLEVIATE the severity of bodily injury resulting from unintended movements of an airplane hull after uncontrolled airplane touch-downs.

Note 2: The *solution* attribute manages an external reference into some device life-cycle repository. The device information in the risk file header can be used to define the scope (i.e. the target IT system) of the references used here.

5.4.4 MOD_DEF_ASSURANCE

For each *Strategy* the manufacturer shall model a list of supporting sub-goals, each modelled as an instance of *Assurance* that manages

- *name*, briefly describing the sub-goal which supports the parent *Strategy*,
- *text*, specifying the sub-goal in a detailed and comprehensive way,
- *code*, with an identification of either a refined SDA or some external measure.

Note 1: The *code* attribute can be used to establish nested SDAs, in that its value is a reference to a (nested) SDA.

6 Abstract Storage Format

6.1 Introduction

This clause specifies general requirements for representations suitable for storing, communicating, or archiving device risk control information. The file for which the risk control information format is specified in this clause is called the *general file*.

One application of the *general file* can be the temporary, local storage (e.g. by the manufacturer) for subsequent electronic editing, storing or processing by the same organization.

The formatting requirements for the purposes of archive and export are specified in subsequent clauses and further restrict the specifications of this clause. Therefore, the requirements in this clause are a prerequisite for archive and export. Note that, prior to archive or export, the *general file* can be generated even if some attributes or references are still missing (due to incomplete information) or if some references are not globally resolved.

The entity who is technically responsible for creating the general file is called *manufacturer*.

6.2 General Requirements

6.2.1 ASF_REQ_DEVICE_HEADER

The manufacturer shall create the general file with the tag "device" including a structure with at least

- a tag "entity", naming some identification of the legal entity responsible for placing the device on the EU market, and
- a tag "project", naming the project performing risk control for the device, and

- a tag “version”, naming the device’s internal release version.

Note: The project name can also include a department name, and/or a product name, and/or a sub-system name, as used within the manufacturer’s internal organization.

6.2.2 ASF_REQ_DEVICE_VERSION

The manufacturer shall include in the general file the device’s release version name such that it includes at least the major release in the sense of regulatory submissions.

Note: Changes in the version string indicate significant changes in the device’s design or documentation that have an impact to risk analysis or risk control.

6.2.3 ASF_REQ_PRIM_KEY (Primary Key)

For each object representation of the classes *HazardousSituation*, *DomainSpecificHazard*, *AnalyzedRisk*, *ControlledRisk* and, *RiskSDA* in the general file, the manufacturer shall assign a tag “id” with some key value which is unique throughout the *general file*. The manufacturer shall – for each of the above classes – include in the *general file* a registry listing all objects representations allowing for comprehensive data storage and exchange, independently of additional files or services.

Note: More attributes can be used for any “secondary” keys which are resolved by some additional (external) IT-systems like e.g. index, repository, database, or tool. This includes the use of OIDs, references, pointers, addresses and similar obtained from and resolved by external sources (like e.g. index, repository, (ALM) database, or development tool).

6.2.4 ASF_INF_REG_KEY (Registry Key)

For each entity representation of *Component*, *Context*, *Function*, *Harm* and, *Hazard* in the general file, the manufacturer should assign a tag “id” with some key value which is unique throughout the *general file*. The manufacturer should – for each of the above entity types – include in the general file a registry, listing all entity representations allowing for unique references which are independent of additional files or services.

Note: Registries list terms which have no identity despite their name. Terms can have neither attributes nor any instances different than the term’s name.

7 Requirements for Export

7.1 Introduction

Archived files and export files are intended to be used for a long time and in different technical environments, therefore they cannot make assumptions regarding viewing tools. At the same time, file formats for archive and export ensure reproducible content and layout. Device Digital Risk Management Files (DRMF) being *exported* from a project repository (operated by a manufacturer, say) to other parties (tester/reviewer, Notified Body, authority) cannot rely on assumptions about specific tools for viewing, data extraction and compilation. The same holds for the format of device Digital Risk Management Files (DRMF) to be *archived* for a long time.

In most legislations, the *printout view* of any document submitted is the relevant basis for reviewing and approving (market access) of some device. This chapter tries to combine the features of the legally binding *printout view* with a machine-readable format that still captures the device risk control information, including all concepts, attributes and relationships that can be expressed by the conceptual model presented in clause five of this specification.

This chapter specifies requirements for a syntax (here: *format*) used to export and archive device Digital Risk Management Files (DRMF) for use by external parties (e.g. auditors, Notified Bodies, authorities).

The term *instance* refers to an entity in the device Digital Risk Management File (DRMF), representing of one of the objects of the conceptual model (Context, Component, Function, Harm, Hazard, HazardousSituation, DomainSpecificHazard, AnalyzedRisk, ControlledRisk, RiskSDA).

In this clause, device Digital Risk Management Files (DRMF) formatted to support archive or export are called *export files*. The entity who is technically responsible for creating export files for device Digital Risk Management Files (DRMF) adhering to this VDE SPEC is called *manufacturer*.

7.2 Definitions

7.2.1 RFE_REQ_ENCODING

The manufacturer shall format export files using encoding formats and character-sets supported by widely available viewers.

7.2.2 RFE_INF_ENCODE_UTF

The manufacturer should format export files using the UTF-8 encoding format (from unicode.org).

7.2.3 RFE_REQ_HUMAN

The manufacturer shall create export files in a format such that widely available tools easily

- display content (names, attributes) within the visible foreground, and
- process relevant markup instructions and transform the visual display accordingly – eliminating the markup instructions, and
- transform hyperlink information into user-clickable links which allow to navigate to the target or to view the target content, and
- transform structural nesting information into nested layouts.

7.2.4 RFE_REQ_SEE_ALL

The manufacturer shall create export files in a format such that in the initial setting – when the export file is opened by the intended viewing tool – each element is visibly displayed and the printout from the initial view will capture all elements, too.

Note: Displaying an outer frame (e.g. as a “solid” “border”) may be created such that it can be used to verify a comprehensive display on screen or printout.

7.2.5 RFE_REQ_MACHINE

The manufacturer shall create export files conforming to the *abstract file* requirements in the preceding clause.

Note: This ensures that the logical structure of risk control instances is preserved – for further processing by dedicated tools.

7.2.6 RFE_REQ_NO_EXT_KEYS

Despite special cases where a mitigation is expressed by a key or reference into some software-lifecycle-tool (database or document), where an external key is permitted, the manufacturer shall not use keys, references, pointers, addresses to arbitrary external information systems and similar. Instead, the manufacturer shall create export files which use – for each attribute of the entities in the export file – either

- a literal text string, or
- a term from publicly available vocabularies which can be seen as state-of-the-art, or
- an internal reference to some instance within the same export file.

Note: As a consequence of the above requirement, a new primary key scheme is required (see below), because representations of conceptual entities (as defined above) do NOT depend on technical (volatile) identifiers which are resolved by arbitrary (access-restricted or obscure) IT-systems.

7.2.7 Envelope

Envelope formats specify a separation of original export file content from additional descriptions regarding the further processing of the export file in a way that leaves the original export file content unaltered. In this clause, the original export file content is called *content*, and the additional descriptive data is called *data*.

7.2.7.1 RFE_REQ_ENVELOPE

Any author responsible for adding an envelope shall at least include

- the UTC calendar date and time, when the envelope was added; in a text string in yyyyMMddThhmmZ (ISO 8601, UTC, zero padding) format, and
- the content checksum using MD5 or SHA256 or SHA512; in a text string, and

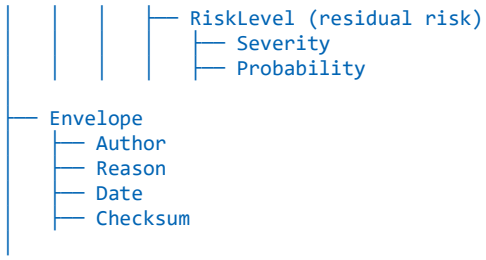
- any kind of textual identification (any name) of the author of the envelope; in a text string, and
- some information regarding the purpose of the archive, export, or processing of the export file; in a text string.

Note 1: Any additional markup via extra elements or extra attributes is not permitted by this specification.

Note 2: Envelopes can be nested in a hierarchical way, such that the statement of the newer (outer) envelope also addresses any statement made by older (inner) envelopes. In that situation, all content and older envelopes *within* the new envelope are referred to as *content* and only the outer (new) envelope is called *envelope*. With nested envelopes and by using the purpose data in each of these envelopes, a kind of processing life-cycle can be pre-served for later auditing. An example life-cycle may cover approval (e.g. by device manufacturer's management), archive, export, receipt by external entity, audit, approval (e.g by some external entity).

Note 3: An informative representation of the recommended string format in the export file is given below.

```
Risk Management File
├── Device
│   ├── Manufacturer name
│   ├── Project name
│   ├── Version name
│   ├── UDI
│   ├── urlRequirement
│   ├── urlSolution
│
├── list of Components
│   ├── Component id
│   ├── Component name
│
├── list of Contexts
│   ├── Context id
│   ├── Context name
│
├── list of Functions
│   ├── Function id
│   ├── Function name
│
├── list of Harms
│   ├── Harm id
│   ├── Harm name
│
├── list of Hazards
│   ├── Hazard id
│   ├── Hazard name
│
├── list of HazardousSituations
│   ├── HazardousSituation id
│   │   ├── HazardousSituation (list)
│
├── list of ControlledRisks
│   ├── ControlledRisk id
│   ├── AnalyzedRisk
│   │   ├── AnalyzedRisk id
│   │   ├── DomainSpecificHazard id
│   │   │   ├── Context
│   │   │   ├── Component
│   │   │   ├── Function
│   │   │   ├── Harm
│   │   │   ├── Hazard
│   │   │   ├── list of Targets
│   │   │   │   ├── Target name (e.g 'user')
│   │   │
│   │   ├── HazardousSituation
│   │   │
│   │   ├── Harm
│   │   │
│   │   ├── RiskLevel (unmitigated risk)
│   │   │   ├── Severity
│   │   │   ├── Probability
│   │   │
│   │   ├── isMitigatedBy
│   │   │   ├── SDA
│   │   │   │   ├── Strategy
│   │   │   │   │   ├── Assurance
│   │   │   │
```



8 Using HTML with RDFa (informative)

8.1 General

This clause introduces the use of HTML and RDFa as a flexible, human/machine-readable export format of digital Risk Management Files (RMFs), built upon World Wide Web Consortium (W3C) [w3c] standards.

The first section specifies recommendations regarding the integrity of the *Export File* with regard to the conceptual model introduced in previous clauses.

The second section specifies recommendations regarding the encoding of the *Export File* in support of automated processing of the results of risk analysis.

Subsequent sections explain a technique to link elements of HTML to selected concepts of the conceptual model which is being represented by a structured ontology. This way, the native elements of HTML can be totally decoupled from semantics, such that they just represent the layout and rendering.

The entity responsible for creating HTML *export files* for device Digital Risk Management Files (DRMF) adhering to this document is called *manufacturer*.

8.2 Integrity recommendations

8.2.1 General

This section specifies the integrity rules for the relationships between instances of the conceptual model in *export files*.

8.2.2 INT_INF_HAZ

The manufacturer should generate the *export file*, such that for each *DomainSpecificHazard* instance there is exactly one *Hazard* instance:

$$hasHazard: DomainSpecificHazard \mapsto Hazard$$

8.2.3 INT_INF_COMP

The manufacturer should generate the *export file*, such that for each *DomainSpecificHazard* instance there is exactly one *Component* (including 'System'):

$$hasComponent: DomainSpecificHazard \mapsto Component \cup \{'System'\}$$

8.2.4 INT_INF_FUNC

The manufacturer should generate the *export file*, such that for each *DomainSpecificHazard* instance there is exactly one *Function* (including 'General'):

$$hasFunction: DomainSpecificHazard \mapsto Function \cup \{'General'\}$$

8.2.5 INT_INF_HASI

The manufacturer should generate the *export file*, such that Each *AnalyzedRisk* is assigned to exactly one *HazardousSituation*:

$$hasHazardousSituation: AnalyzedRisk \mapsto HazardousSituation$$

8.2.6 INT_INF_ANALYZEDRISK

The manufacturer should generate the *export file*, such that each *AnalyzedRisk* has exactly one "parent" *DomainSpecificHazard*:

$$hasDomainSpecificHazard: AnalyzedRisk \mapsto DomainSpecificHazard$$

Note: Per structure of *Export Files*, any *DomainSpecificHazard* appears in exactly one *AnalyzedRisk*.

8.2.7 INT_INF_HARM

The manufacturer should generate the *export file*, such that for each *AnalyzedRisk* instance there is exactly one *Harm* instance:

$$hasHarm: AnalyzedRisk \mapsto Harm$$

8.2.8 INT_INF_PRE_EVAL

The manufacturer should generate the *export file*, such that each *AnalyzedRisk* has exactly one *Risk* prior to mitigation:

$$hasInitialRisk: AnalyzedRisk \mapsto Risk$$

8.2.9 INT_INF_MITIGATED

The manufacturer should generate the *export file*, such that each *ControlledRisk* has at least one *RiskSDA*:

$$\forall\, c \in Controlled\ Risk \rightarrow \exists\, r \in RiskSDA \wedge isMitigatedBy(c) = r$$

8.2.10 INT_INF_POST_EVAL

The manufacturer should generate the *export file*, such that each *ControlledRisk* has exactly one *Risk* after considering mitigation:

$$hasResidualRisk: ControlledRisk \mapsto Risk$$

8.2.11 INT_INF_CONTROL

The manufacturer should generate the *export file*, such that each *ControlledRisk* has exactly one *AnalyzedRisk* to mitigate:

$$hasAnalyzedRisk: ControlledRisk \mapsto AnalyzedRisk$$

Note: Implementations may also use *control* as the mapping.

8.2.12 INT_INF_COMPLETE

The manufacturer should generate the *export file*, such that each *AnalyzedRisk* is mitigated by exactly one *ControlledRisk*:

$$hasAnalyzedRisk^{-1}: AnalyzedRisk \mapsto ControlledRisk$$

8.3 Encoding of the risk analysis

8.3.1 General

This section describes attributes of elements of the conceptual model towards encoding the digital risk file in a way that supports automated processing.

Note: The recommended attribute values are based on IMDRF Adverse Event Terminology (IMDRF AET). These terminologies are hierarchical and define nodes and leafs for use in documentation, but also inner nodes, which are more general than leaves. For the purposes of this document, inner nodes from IMDRF AET can be used as well.

8.3.2 INT_INF_IMDRF_HEALTH (IMDRF AET Health Effects)

The manufacturer should create instances of conceptual class *DomainSpecificHazard* in the *export file* with at least one textual “imdrf_aete” element capturing the IMDRF AET term from Annex E “Clinical Signs” or Annex F “Health Effects”.

$$hasHarmCode: DomainSpecificHazard \mapsto AET_E \cup AET_F$$

8.3.3 INT_INF_IMDRF_CAUSE (IMDRF AET Cause)

The manufacturer should create instances of conceptual class *AnalyzedRisk* in the *export file* with at least one textual “imdrf_aetc” element capturing the IMDRF AET term from Annex C “Cause”

$$hasCauseCode: AnalyzedRisk \mapsto AET_C$$

8.3.4 INT_INF_IMDRF_PROBLEM (IMDRF AET Device Problem)

The manufacturer should create instances of conceptual class *AnalyzedRisk* in the *export file* with one or multiple textual “imdrf_aeta” elements capturing the IMDRF AET term from Annex A “Device Problem”.

$$hasProblemCode: AnalyzedRisk \mapsto AET_A$$

8.3.5 INT_INF_ENC_COMP (Encoded Component)

The manufacturer should create instances of conceptual class *DomainSpecificHazard* in the *export file* with at least one textual “imdrf_aetg” element capturing the IMDRF AET G code specifying the component.

$$hasComponentCode: DomainSpecificHazard \mapsto AET_G$$

The following section introduces and recommends the use of HTML and RDFa as a flexible, human/machine-readable exchange format of Digital Risk Management File (DRMF), built upon World Wide Web Consortium W3C [w3c] standards.

8.4 HTML

The HyperText Markup Language HTML [html] format is one of the most popular file formats for serialization and data exchange. It precisely describes parsing rules and is widely supported by software, which can easily extract and render the encoded information.

Additionally, it is important to note that HTML is a standard maintained by the World Wide Web Consortium (W3C) [w3c]. The W3C is an international community that develops open standards to ensure the long-term growth and accessibility of the world wide web. The standardization of HTML by the W3C contributes to the consistency and interoperability of web documents across various platforms and devices. This ensures that HTML documents are created and interpreted consistently, promoting a more reliable and universally compatible web environment.

Rendering is performed by “Web Browsers” – software that (among other tasks, mainly) renders HTML documents in a well-defined way according to standardized rendering rules (W3C). Nowadays, internet browsers are provided out of the box in most of the common electronic devices as PCs, smartphones, tablets, smart TVs, etc.

Additionally, HTML allows for customization by Cascading Style Sheets (CSS) [css]. This in turn enables end-users to customize how they display the HTML documents in alignment with their needs.

8.5 RDF(a) (Semantic Web Technologies)

As established previously, data encoded in HTML can easily be serialized, parsed, exchanged as well as displayed and customized. However, plain HTML does not specify how to extract knowledge from the documents. Provided that knowledge could be encoded within HTML files and later be easily extractable would allow for validation and reasoning over the encoded knowledge.

Resource Description Frameworks in Attributes (RDFa) [rdfa1][rdfa1] aids in achieving this goal by adding metadata that encodes relationships between entities as so called RDF subject-predicate-object “triples”.

The added metadata is not visible when HTML documents are rendered. It can however be easily extracted (distilled) from the HTML files and later used for various purposes, among others (and most importantly in the case of ensuring safety/security) for data validation, consistency/correctness/completeness checks, or querying.

The *Export Format* described in this clause is based on HTML and RDFa guarantees human/machine readability and rich support of off-the-shelf software. The flexibility of the approach guarantees that only minimal prerequisites are necessary for it to be successfully implemented.

Recall that RDF [rdf] encodes data in the form of subject-predicate-object “triples”. These triples can be thought of as directed graphs, with “subject” and “object” representing nodes and “predicate” a directed labelled edge between them. This is presented in Figure 2.

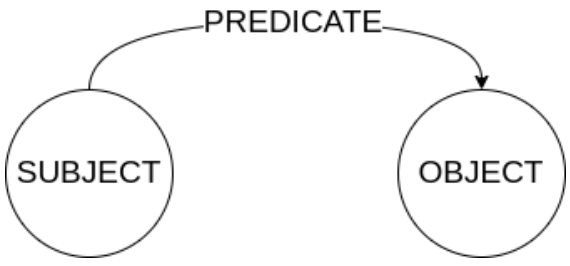


Figure 2 – Graph representation of an RDF triple

Frequently used RDFa attributes are:

- `typeof`
- `property`

With help of the `typeof` “predicate”, one can specify that the “subject” is of type “object”. To ease understanding, assume an imaginary scenario in which a Domain Specific Hazard of ID “DSH#001” appears in a RMF. Using RDF the fact that “DSH#001” is of type “DomainSpecificHazard” can be (pseudo-)encoded as follows:

```
"DSH#001" typeof "DomainSpecificHazard"
```

or graphically as in Figure 3.

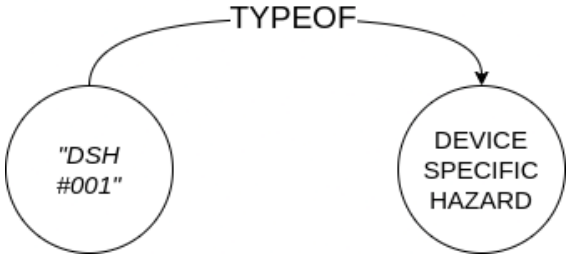


Figure 3 – Graph representation of the typeof triple

Using the `property` annotation one can specify any predicate. Assume that in our scenario, the hazard related with “DSH#001” is “Chemical”. A custom “has hazard” predicate could be use as follows:

```
"DSH#001" has hazard "Chemical"
```

or graphically as in Figure 4.

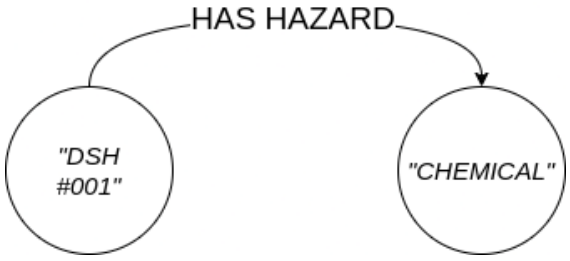


Figure 4 – Graph representation of the has hazard (property) triple.

The following listing presents how to encode such information in HTML using RDFa annotations.

```
<div vocab="http://schema.org/" typeof="DomainSpecificHazard">
      <h3 property="id">DSH#001</h3>
      <div property="hasHazard" typeof="schema:Hazard">
        <h4 property="name">Chemical</h4>
      </div>
</div>
```

(Note that in the above listing another RDFa attribute `vocab` is used to specify the namespace of the used vocabulary. For the sake of simplicity, this has been set to the most generic namespace identifier `"http://schema.org/"`.)

In the example we see that the outer `<div>` element is of type “DomainSpecificHazard”. It has two properties, namely “id” and a hazard object. The hazard object in turn has a “name” property with a value “Chemical”. Figure 5 shows the rendered HTML. Figure 6 presents the extracted data and their relations.

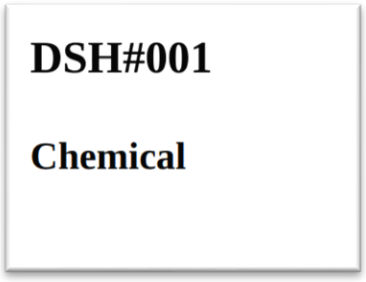


Figure 5 – Rendered HTML code

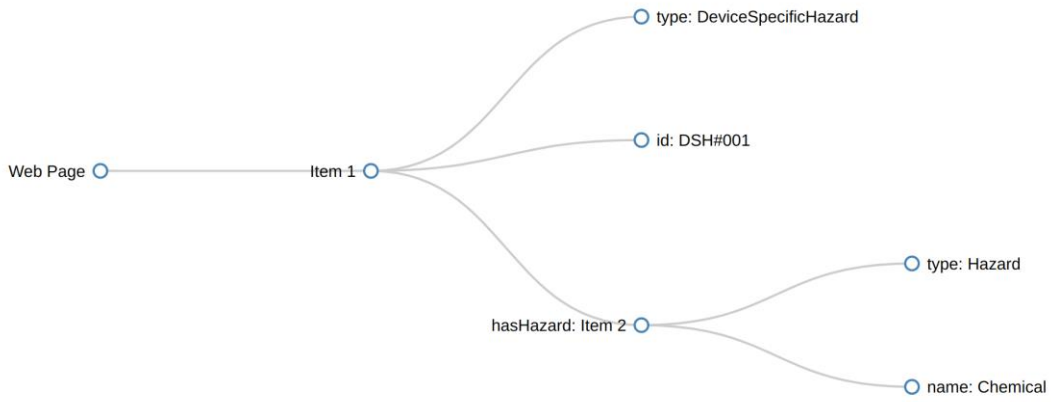


Figure 6 – Graphical representation of the rendered HTML code

Types of entities and relations (such as **hasHazard**) are defined in the RISKMAN ontology [riskman-ontology], which provides all necessary relations and classes required to conform to the digital RMF specified in this document.

This small example shows that the rendered HTML can successfully encode RDF data while being transparent for the end user who is interested only in the rendered outcome. In the following section we will see a much larger example, more like a real-life scenario.

8.6 Example

The following listing presents an example of a valid RMF encoding in HTML with RDFa annotations.

```
<!DOCTYPE html>
<html>
<head>
    <html prefix="riskman: https://w3id.org/riskman/ontology#" >
    <title>Risk Management File</title>
    <style>
        .container {
            width: 60%;
            margin: 0 auto;
            margin-top: 50px;
            text-align: center;
        }

        table,
        th,
        td {
            border: 1px solid black;
            border-collapse: collapse;
        }

        td {
            padding: 5px;
```

```
        }

        th {
            background-color: rgb(211, 211, 211);
        }

        .separator {
            border-top: 2px solid black;
        }
    </style>
</head>
<body>
    <div class="container">
        <table>
            <thead>
                <tr>
                    <th rowspan="4"></th>
                    <th colspan="13">Controlled Risk</th>
                </tr>
                <tr>
                    <th colspan="9">Analyzed Risk</th>
                    <th rowspan="3">Risk SDA</th>
                    <th rowspan="2" colspan="2">Residual Risk Level</th>
                </tr>
                <tr>
                    <th colspan="3">Domain Specific Hazard</th>
                    <th rowspan="2">Harm</th>
                    <th rowspan="2">Device Context</th>
                    <th rowspan="2">Event</th>
                    <th rowspan="2">Hazardous Situation</th>
                    <th colspan="2">Initial Risk Level</th>
                </tr>
                <tr>
                    <th>Hazard</th>
                    <th>Function</th>
                    <th>Component</th>
                    <th>Prob.</th>
                    <th>Sev.</th>
                    <th>Prob.</th>
                    <th>Sev.</th>
                </tr>
            </thead>
            <tbody>
                <!-- 1) -->
                <tr>
                    <td rowspan="3" resource="controlledRisk1" typeof="riskman:ControlledRisk">
                        <span property="riskman:hasID">1</span>
                        <link property="riskman:hasAnalyzedRisk" href="analyzedRisk1"/>
                        <link property="riskman:hasSDA" href="sda1"/>
                        <link property="riskman:hasResidualRiskLevel" href="residualRiskLevel1"/>
                    </td>
                    <td colspan="9" resource="analyzedRisk1" typeof="riskman:AnalyzedRisk">
                        <span property="riskman:hasName">Solvent removal risk of brain damage</span>
                        <link property="riskman:hasDomainSpecificHazard" href="domainSpecificHazard1"/>
                        <link property="riskman:hasHarm" href="harm1"/>
                        <link property="riskman:hasDeviceContext" href="deviceContext1"/>
                        <link property="riskman:hasHazardousSituation" href="hazardousSituation1"/>
                        <link property="riskman:hasInitialRiskLevel" href="initialRiskLevel1"/>
                    </td>
                    <td rowspan="3" resource="sda1" typeof="riskman:SDA">
                        <span property="riskman:hasName">Implementation of an automated solvent monitor
ing system</span>
                    </td>
                    <td rowspan="2" colspan="3" resource="residualRiskLevel1" typeof="riskman:RiskLevel
">
                        <span property="riskman:hasName">Residual Risk Level 1</span>
                        <link property="riskman:hasProbability" href="residualProbability1"/>
                        <link property="riskman:hasSeverity" href="residualSeverity1"/>
                    </td>
                </tr>
                <tr>
                    <td colspan="3" resource="domainSpecificHazard1" typeof="riskman:DomainSpecificHaza
rd">
                        <span property="riskman:hasName">Rotary evaporator solvent removal chemical haz
ard</span>
                        <link property="riskman:hasHazard" href="hazard1"/>
```

```
                    <link property="riskman:hasDeviceFunction" href="deviceFunction1"/>
                    <link property="riskman:hasDeviceComponent" href="deviceComponent1"/>
                </td>
                <td rowspan="2" resource="harm1" typeof="riskman:Harm">
                    <span property="riskman:hasName">Brain damage</span>
                </td>
                <td rowspan="2" resource="deviceContext1" typeof="riskman:DeviceContext">
                    <span property="riskman:hasName">Chemical manufacturing</span>
                </td>
                <td rowspan="2" resource="event1" typeof="riskman:Event">
                    <span property="riskman:hasName">Incomplete removal of volatile solvent used in
manufacturing</span>
                </td>
                <td rowspan="2" resource="hazardousSituation1" typeof="riskman:HazardousSituation">
                    <span property="riskman:hasName">Development of gas embolism</span>
                    <link property="riskman:hasPrecedingEvent" href="event1"/>
                </td>
                <td colspan="2" resource="initialRiskLevel1" typeof="riskman:RiskLevel">
                    <span property="riskman:hasName">Initial Risk Level 1</span>
                    <link property="riskman:hasProbability" href="initialProbability1"/>
                    <link property="riskman:hasSeverity" href="initialSeverity1"/>
                </td>
            </tr>
            <tr>
                <td resource="hazard1" typeof="riskman:Hazard">
                    <span property="riskman:hasName">Chemical</span>
                </td>
                <td resource="deviceFunction1" typeof="riskman:DeviceFunction">
                    <span property="riskman:hasName">Solvent removal</span>
                </td>
                <td resource="deviceComponent1" typeof="riskman:DeviceComponent">
                    <span property="riskman:hasName">Rotary evaporator</span>
                </td>
                <td resource="initialProbability1" typeof="riskman:Probability">
                    <span property="riskman:hasValue">3</span>
                </td>
                <td resource="initialSeverity1" typeof="riskman:Severity">
                    <span property="riskman:hasValue">4</span>
                </td>
                <td resource="residualProbability1" typeof="riskman:Probability">
                    <span property="riskman:hasValue">2</span>
                </td>
                <td resource="residualSeverity1" typeof="riskman:Severity">
                    <span property="riskman:hasValue">3</span>
                </td>
            </tr>
            <tr class="separator"></tr>
            <!-- 2 -->
            <tr>
                <td rowspan="3" resource="controlledRisk2" typeof="riskman:ControlledRisk">
                    <span property="riskman:hasID">2</span>
                    <link property="riskman:hasAnalyzedRisk" href="analyzedRisk2"/>
                    <link property="riskman:hasSDA" href="sda2"/>
                    <link property="riskman:hasResidualRiskLevel" href="residualRiskLevel2"/>
                </td>
                <td colspan="9" resource="analyzedRisk2" typeof="riskman:AnalyzedRisk">
                    <span property="riskman:hasName">Electrode cable risk of serious burns</span>
                    <link property="riskman:hasDomainSpecificHazard" href="domainSpecificHazard2"/>
                    <link property="riskman:hasHarm" href="harm2"/>
                    <link property="riskman:hasDeviceContext" href="deviceContext2"/>
                    <link property="riskman:hasHazardousSituation" href="hazardousSituation2"/>
                    <link property="riskman:hasInitialRiskLevel" href="initialRiskLevel2"/>
                </td>
                <td rowspan="3" resource="sda2" typeof="riskman:SDA">
                    <span property="riskman:hasName">Use polarized plugs</span>
                </td>
                <td rowspan="2" colspan="3" resource="residualRiskLevel2" typeof="riskman:RiskLevel
">
                    <span property="riskman:hasName">Residual Risk Level 2</span>
                    <link property="riskman:hasProbability" href="residualProbability2"/>
                    <link property="riskman:hasSeverity" href="residualSeverity2"/>
                </td>
            </tr>
            <tr>
                <td colspan="3" resource="domainSpecificHazard2" typeof="riskman:DomainSpecificHaza
rd">
```

```
                    <span property="riskman:hasName">Electrode cable electrosurgery hazard</span>
                    <link property="riskman:hasHazard" href="hazard2"/>
                    <link property="riskman:hasDeviceFunction" href="deviceFunction2"/>
                    <link property="riskman:hasDeviceComponent" href="deviceComponent2"/>
                </td>
                <td rowspan="2" resource="harm2" typeof="riskman:Harm">
                    <span property="riskman:hasName">Serious burns</span>
                </td>
                <td rowspan="2" resource="deviceContext2" typeof="riskman:DeviceContext">
                    <span property="riskman:hasName">Operating room setting</span>
                </td>
                <td rowspan="2" resource="event2" typeof="riskman:Event">
                    <span property="riskman:hasName">Electrode cable unintentionally plugged into p
ower line receptacle</span>
                </td>
                <td rowspan="2" resource="hazardousSituation2" typeof="riskman:HazardousSituation">
                    <span property="riskman:hasName">Line voltage appears on electrodes</span>
                    <link property="riskman:hasPrecedingEvent" href="event2"/>
                </td>
                <td colspan="2" resource="initialRiskLevel2" typeof="riskman:RiskLevel">
                    <span property="riskman:hasName">Initial Risk Level 2</span>
                    <link property="riskman:hasProbability" href="initialProbability2"/>
                    <link property="riskman:hasSeverity" href="initialSeverity2"/>
                </td>
            </tr>
            <tr>
                <td resource="hazard2" typeof="riskman:Hazard">
                    <span property="riskman:hasName">Electromagnetic energy</span>
                </td>
                <td resource="deviceFunction2" typeof="riskman:DeviceFunction">
                    <span property="riskman:hasName">Electrosurgery</span>
                </td>
                <td resource="deviceComponent2" typeof="riskman:DeviceComponent">
                    <span property="riskman:hasName">Electrode cable</span>
                </td>
                <td resource="initialProbability2" typeof="riskman:Probability">
                    <span property="riskman:hasValue">3</span>
                </td>
                <td resource="initialSeverity2" typeof="riskman:Severity">
                    <span property="riskman:hasValue">4</span>
                </td>
                <td resource="residualProbability2" typeof="riskman:Probability">
                    <span property="riskman:hasValue">1</span>
                </td>
                <td resource="residualSeverity2" typeof="riskman:Severity">
                    <span property="riskman:hasValue">2</span>
                </td>
            </tr>
            <tr class="separator"></tr>
            <tr>
                <td colspan="13" style="text-align: center;">...</td>
            </tr>
            <tr class="separator"></tr>
            <!-- 99 -->
            <tr>
                <td rowspan="3" resource="controlledRisk99" typeof="riskman:ControlledRisk">
                    <span property="riskman:hasID">99</span>
                    <link property="riskman:hasAnalyzedRisk" href="analyzedRisk99"/>
                    <link property="riskman:hasSDA" href="sda99"/>
                    <link property="riskman:hasResidualRiskLevel" href="residualRiskLevel99"/>
                </td>
                <td colspan="9" resource="analyzedRisk99" typeof="riskman:AnalyzedRisk">
                    <span property="riskman:hasName">Risk of death due to defibrillator battery run
ning out</span>
                    <link property="riskman:hasDomainSpecificHazard" href="domainSpecificHazard99"
/>
                    <link property="riskman:hasHarm" href="harm99"/>
                    <link property="riskman:hasDeviceContext" href="deviceContext99"/>
                    <link property="riskman:hasHazardousSituation" href="hazardousSituation99"/>
                    <link property="riskman:hasInitialRiskLevel" href="initialRiskLevel99"/>
                </td>
                <td rowspan="3" resource="sda99" typeof="riskman:SDA">
                    <span property="riskman:hasName">Indicate low battery level</span>
                </td>
                <td rowspan="2" colspan="3" resource="residualRiskLevel99" typeof="riskman:RiskLeve
l">
```

```
                    <span property="riskman:hasName">Residual Risk Level 99</span>
                    <link property="riskman:hasProbability" href="residualProbability99"/>
                    <link property="riskman:hasSeverity" href="residualSeverity99"/>
                </td>
            </tr>
            <tr>
                <td colspan="3" resource="domainSpecificHazard99" typeof="riskman:DomainSpecificHaz
ard">
                    <span property="riskman:hasName">Battery-level related defibrillator hazard</sp
an>
                    <link property="riskman:hasHazard" href="hazard99"/>
                    <link property="riskman:hasDeviceFunction" href="deviceFunction99"/>
                    <link property="riskman:hasDeviceComponent" href="deviceComponent99"/>
                </td>
                <td rowspan="2" resource="harm99" typeof="riskman:Harm">
                    <span property="riskman:hasName">Death</span>
                </td>
                <td rowspan="2" resource="deviceContext99" typeof="riskman:DeviceContext">
                    <span property="riskman:hasName">Emergency medical setting</span>
                </td>
                <td rowspan="2" resource="event99" typeof="riskman:Event">
                    <span property="riskman:hasName">Defibrillator battery life runs out</span>
                </td>
                <td rowspan="2" resource="hazardousSituation99" typeof="riskman:HazardousSituation
">
                    <span property="riskman:hasName">Cannot deliver shock when an arrythmia occurs<
/span>
                    <link property="riskman:hasPrecedingEvent" href="event99"/>
                </td>
                <td colspan="2" resource="initialRiskLevel99" typeof="riskman:RiskLevel">
                    <span property="riskman:hasName">Initial Risk Level 99</span>
                    <link property="riskman:hasProbability" href="initialProbability99"/>
                    <link property="riskman:hasSeverity" href="initialSeverity99"/>
                </td>
            </tr>
            <tr>
                <td resource="hazard99" typeof="riskman:Hazard">
                    <span property="riskman:hasName">Functionality</span>
                </td>
                <td resource="deviceFunction99" typeof="riskman:DeviceFunction">
                    <span property="riskman:hasName">Defibrillation</span>
                </td>
                <td resource="deviceComponent99" typeof="riskman:DeviceComponent">
                    <span property="riskman:hasName">Battery</span>
                </td>
                <td resource="initialProbability99" typeof="riskman:Probability">
                    <span property="riskman:hasValue">3</span>
                </td>
                <td resource="initialSeverity99" typeof="riskman:Severity">
                    <span property="riskman:hasValue">5</span>
                </td>
                <td resource="residualProbability99" typeof="riskman:Probability">
                    <span property="riskman:hasValue">2</span>
                </td>
                <td resource="residualSeverity99" typeof="riskman:Severity">
                    <span property="riskman:hasValue">5</span>
                </td>
            </tr>
        </tbody>
    </table>
</div>
</body>
</html>
```

Figure 7 shows how the above code is rendered in a Web Browser.

Figures below show the extracted data in the form of a graph. For readability reasons some of the nodes have been collapsed, but jointly all the figures capture the encoding from the above listing. In Figure 8 all nodes representing **ControlledRisk**s have been collapsed, in Figure 9, Figure 10, and Figure 11 nodes representing **ControlledRisk**s **1**, **2** and **99** are shown, respectively.

	Controlled Risk											
	Analyzed Risk									Risk SDA	Residual Risk Level	
	Domain Specific Hazard			Harm	Device Context	Event	Hazardous Situation	Initial Risk Level				
	Hazard	Function	Component					Prob.	Sev.		Prob.	Sev.
1	Solvent removal risk of brain damage											
	Rotary evaporator solvent removal chemical hazard			Brain damage	Chemical manufacturing	Incomplete removal of volatile solvent used in manufacturing	Development of gas embolism	Initial Risk Level 1		Implementation of an automated solvent monitoring system	Residual Risk Level 1	
	Chemical	Solvent removal	Rotary evaporator					3	4		2	3
2	Electrode cable risk of serious burns											
	Electrode cable electrosurgery hazard			Serious burns	Operating room setting	Electrode cable unintentionally plugged into power line receptacle	Line voltage appears on electrodes	Initial Risk Level 2		Use polarized plugs	Residual Risk Level 2	
	Electromagnetic energy	Electrosurgery	Electrode cable					3	4		1	2
...												
99	Risk of death due to defibrillator battery running out											
	Battery-level related defibrillator hazard			Death	Emergency medical setting	Defibrillator battery life runs out	Cannot deliver shock when an arrythmia occurs	Initial Risk Level 99		Indicate low battery level	Residual Risk Level 99	
	Functionality	Defibrillation	Battery					3	5		2	5

Figure 7 – Rendered code from above listing

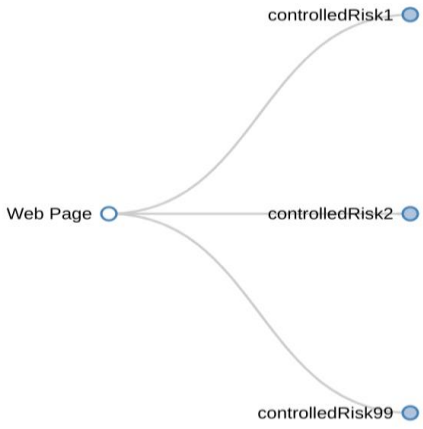


Figure 8 – Visualization of the extracted data. Controlled Risks #1, #2 and #99 have been collapsed to improve visibility.

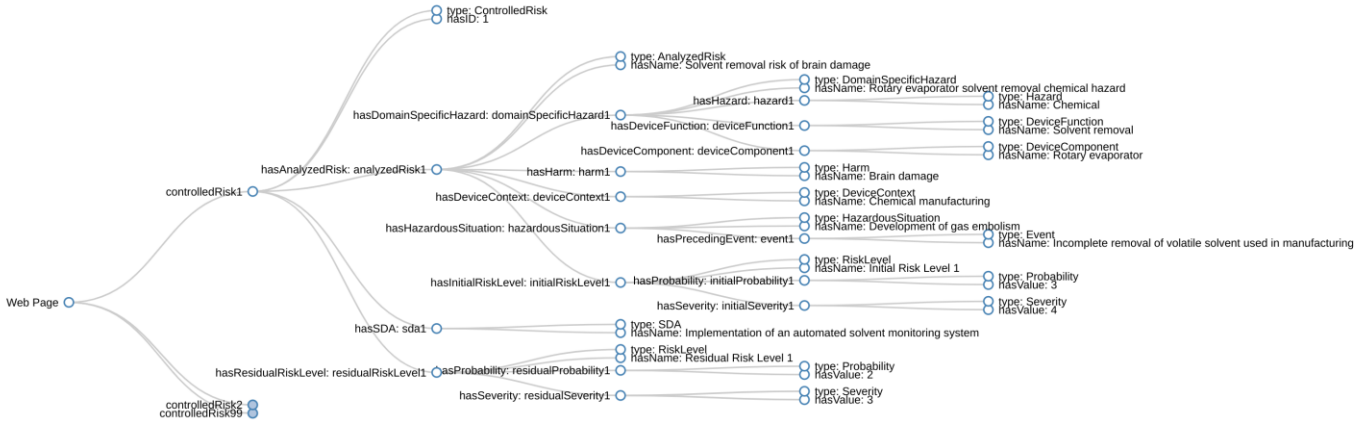


Figure 9 – Visualization of the extracted data with expanded Controlled Risk #1

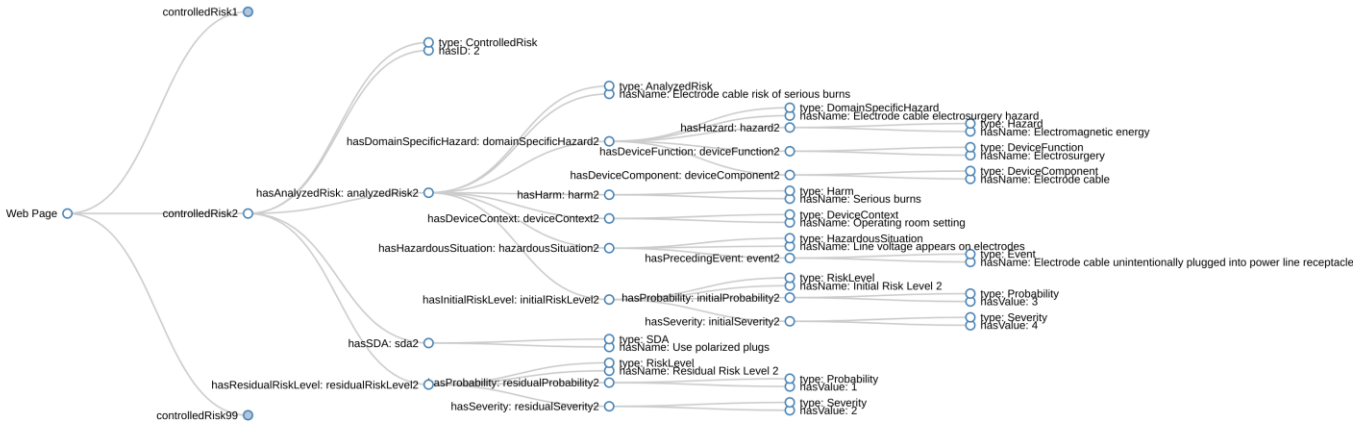


Figure 10 – Visualization of the extracted data with expanded Controlled Risk #2

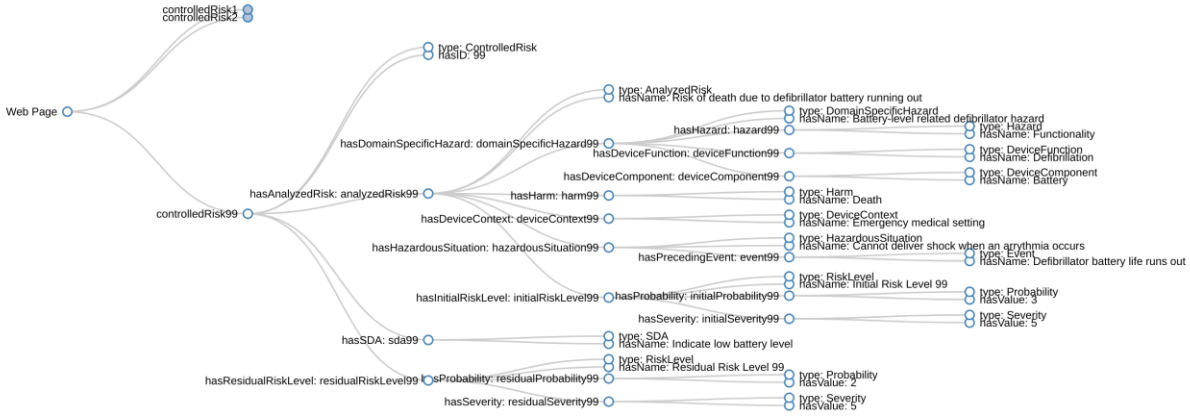


Figure 11 – Visualization of the extracted data with expanded Controlled Risk #99

The following listing presents the extracted data in RDF format. This format could be used for storing as well as for easy conversion into JSON or XML. Excerpts of code listings representing the **`ControlledRisk`** of id 1 have been presented in what comes after, in the 2 latter formats (JSON and XML), respectively.

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix riskman: <https://w3id.org/riskman#> .

_:controlledRisk1 a riskman:ControlledRisk ;
    riskman:hasID "1" ;
    riskman:hasAnalyzedRisk [
        rdf:type riskman:AnalyzedRisk ;
        riskman:hasName "Solvent removal risk of brain damage" ;
        riskman:hasDomainSpecificHazard [
            rdf:type riskman:DomainSpecificHazard ;
            riskman:hasName "Rotary evaporator solvent removal chemical hazard" ;
            riskman:hasHazard [
                rdf:type riskman:Hazard ;
                riskman:hasName "Chemical" ;
            ] ;
            riskman:hasDeviceFunction [
                rdf:type riskman:DeviceFunction ;
                riskman:hasName "Solvent removal" ;
            ] ;
            riskman:hasDeviceComponent [
                rdf:type riskman:DeviceComponent ;
                riskman:hasName "Rotary evaporator" ;
            ] ;
        ] ;
        riskman:hasHarm [
            rdf:type riskman:Harm ;
            riskman:hasName "Brain damage" ;
```

```
        ] ;
        riskman:hasDeviceContext [
            rdf:type riskman:DeviceContext ;
            riskman:hasName "Chemical manufacturing" ;
        ] ;
        riskman:hasHazardousSituation [
            rdf:type riskman:HazardousSituation ;
            riskman:hasName "Development of gas embolism" ;
            riskman:hasPrecedingEvent [
                rdf:type riskman:Event ;
                riskman:hasName "Incomplete removal of volatile solvent used in manufacturing" ;
            ] ;
        ] ;
        riskman:hasInitialRiskLevel [
            rdf:type riskman:RiskLevel ;
            riskman:hasName "Initial Risk Level 1" ;
            riskman:hasProbability [
                rdf:type riskman:Probability ;
                riskman:hasValue "3" ;
            ] ;
            riskman:hasSeverity [
                rdf:type riskman:Severity ;
                riskman:hasValue "4" ;
            ] ;
        ] ;
    ] ;
    riskman:hasSDA [
        rdf:type riskman:SDA ;
        riskman:hasName "Implementation of an automated solvent monitoring system" ;
    ] ;
    riskman:hasResidualRiskLevel [
        rdf:type riskman:RiskLevel ;
        riskman:hasName "Residual Risk Level 1" ;
        riskman:hasProbability [
            rdf:type riskman:Probability ;
            riskman:hasValue "2" ;
        ] ;
        riskman:hasSeverity [
            rdf:type riskman:Severity ;
            riskman:hasValue "3" ;
        ] ;
    ] .

_:controlledRisk2 a riskman:ControlledRisk ;
    riskman:hasID "2" ;
    riskman:hasAnalyzedRisk [
        rdf:type riskman:AnalyzedRisk ;
        riskman:hasName "Electrode cable risk of serious burns" ;
        riskman:hasDomainSpecificHazard [
            rdf:type riskman:DomainSpecificHazard ;
            riskman:hasName "Electrode cable electrosurgery hazard" ;
            riskman:hasHazard [
                rdf:type riskman:Hazard ;
                riskman:hasName "Electromagnetic energy" ;
            ] ;
            riskman:hasDeviceFunction [
                rdf:type riskman:DeviceFunction ;
                riskman:hasName "Electrosurgery" ;
            ] ;
            riskman:hasDeviceComponent [
                rdf:type riskman:DeviceComponent ;
                riskman:hasName "Electrode cable" ;
            ] ;
        ] ;
        riskman:hasHarm [
            rdf:type riskman:Harm ;
            riskman:hasName "Serious burns" ;
        ] ;
        riskman:hasDeviceContext [
            rdf:type riskman:DeviceContext ;
            riskman:hasName "Operating room setting" ;
        ] ;
        riskman:hasHazardousSituation [
            rdf:type riskman:HazardousSituation ;
            riskman:hasName "Line voltage appears on electrodes" ;
            riskman:hasPrecedingEvent [
```

```
                rdf:type riskman:Event ;
                riskman:hasName "Electrode cable unintentionally plugged into power line receptacle" ;
            ] ;
        ] ;
        riskman:hasInitialRiskLevel [
            rdf:type riskman:RiskLevel ;
            riskman:hasName "Initial Risk Level 2" ;
            riskman:hasProbability [
                rdf:type riskman:Probability ;
                riskman:hasValue "3" ;
            ] ;
            riskman:hasSeverity [
                rdf:type riskman:Severity ;
                riskman:hasValue "4" ;
            ] ;
        ] ;
    ] ;
    riskman:hasSDA [
        rdf:type riskman:SDA ;
        riskman:hasName "Use polarized plugs" ;
    ] ;
    riskman:hasResidualRiskLevel [
        rdf:type riskman:RiskLevel ;
        riskman:hasName "Residual Risk Level 2" ;
        riskman:hasProbability [
            rdf:type riskman:Probability ;
            riskman:hasValue "1" ;
        ] ;
        riskman:hasSeverity [
            rdf:type riskman:Severity ;
            riskman:hasValue "2" ;
        ] ;
    ] .

_:controlledRisk99 a riskman:ControlledRisk ;
    riskman:hasID "99" ;
    riskman:hasAnalyzedRisk [
        rdf:type riskman:AnalyzedRisk ;
        riskman:hasName "Risk of death due to defibrillator battery running out" ;
        riskman:hasDomainSpecificHazard [
            rdf:type riskman:DomainSpecificHazard ;
            riskman:hasName "Battery-level related defibrillator hazard" ;
            riskman:hasHazard [
                rdf:type riskman:Hazard ;
                riskman:hasName "Functionality" ;
            ] ;
            riskman:hasDeviceFunction [
                rdf:type riskman:DeviceFunction ;
                riskman:hasName "Defibrillation" ;
            ] ;
            riskman:hasDeviceComponent [
                rdf:type riskman:DeviceComponent ;
                riskman:hasName "Battery" ;
            ] ;
        ] ;
        riskman:hasHarm [
            rdf:type riskman:Harm ;
            riskman:hasName "Death" ;
        ] ;
        riskman:hasDeviceContext [
            rdf:type riskman:DeviceContext ;
            riskman:hasName "Emergency medical setting" ;
        ] ;
        riskman:hasHazardousSituation [
            rdf:type riskman:HazardousSituation ;
            riskman:hasName "Cannot deliver shock when an arrythmia occurs" ;
            riskman:hasPrecedingEvent [
                rdf:type riskman:Event ;
                riskman:hasName "Defibrillator battery life runs out" ;
            ] ;
        ] ;
        riskman:hasInitialRiskLevel [
            rdf:type riskman:RiskLevel ;
            riskman:hasName "Initial Risk Level 99" ;
            riskman:hasProbability [
                rdf:type riskman:Probability ;
```

```
                riskman:hasValue "3" ;
            ] ;
            riskman:hasSeverity [
                rdf:type riskman:Severity ;
                riskman:hasValue "5" ;
            ] ;
        ] ;
    ] ;
    riskman:hasSDA [
        rdf:type riskman:SDA ;
        riskman:hasName "Indicate low battery level" ;
    ] ;
    riskman:hasResidualRiskLevel [
        rdf:type riskman:RiskLevel ;
        riskman:hasName "Residual Risk Level 99" ;
        riskman:hasProbability [
            rdf:type riskman:Probability ;
            riskman:hasValue "2" ;
        ] ;
        riskman:hasSeverity [
            rdf:type riskman:Severity ;
            riskman:hasValue "5" ;
        ] ;
    ] .
```

```
{
  "@context": {
    "rdf": "http://www.w3.org/1999/02/22-rdf-syntax-ns#",
    "riskman": "https://w3id.org/riskman#"
  },
  "@graph": [
    {
      "@id": "_:analyzedRisk1",
      "@type": "riskman:AnalyzedRisk",
      "riskman:hasDeviceContext": {
        "@id": "_:deviceContext1"
      },
      "riskman:hasDomainSpecificHazard": {
        "@id": "_:domainSpecificHazard1"
      },
      "riskman:hasHarm": {
        "@id": "_:harm1"
      },
      "riskman:hasHazardousSituation": {
        "@id": "_:hazardousSituation1"
      },
      "riskman:hasInitialRiskLevel": {
        "@id": "_:initialRiskLevel1"
      },
      "riskman:hasName": "Solvent removal risk of brain damage"
    },
    {
      "@id": "_:controlledRisk1",
      "@type": "riskman:ControlledRisk",
      "riskman:hasAnalyzedRisk": {
        "@id": "_:analyzedRisk1"
      },
      "riskman:hasID": "1",
      "riskman:hasResidualRiskLevel": {
        "@id": "_:residualRiskLevel1"
      },
      "riskman:hasSDA": {
        "@id": "_:sda1"
      }
    },
    {
      "@id": "_:deviceComponent1",
      "@type": "riskman:DeviceComponent",
      "riskman:hasName": "Rotary evaporator"
    },
    {
      "@id": "_:deviceContext1",
      "@type": "riskman:DeviceContext",
      "riskman:hasName": "Chemical manufacturing"
    },
```

```
{
  "@id": "_:deviceFunction1",
  "@type": "riskman:DeviceFunction",
  "riskman:hasName": "Solvent removal"
},
{
  "@id": "_:domainSpecificHazard1",
  "@type": "riskman:DomainSpecificHazard",
  "riskman:hasDeviceComponent": {
    "@id": "_:deviceComponent1"
  },
  "riskman:hasDeviceFunction": {
    "@id": "_:deviceFunction1"
  },
  "riskman:hasHazard": {
    "@id": "_:hazard1"
  },
  "riskman:hasName": "Rotary evaporator solvent removal chemical hazard"
},
{
  "@id": "_:event1",
  "@type": "riskman:Event",
  "riskman:hasName": "Incomplete removal of volatile solvent used in manufacturing"
},
{
  "@id": "_:harm1",
  "@type": "riskman:Harm",
  "riskman:hasName": "Brain damage"
},
{
  "@id": "_:hazard1",
  "@type": "riskman:Hazard",
  "riskman:hasName": "Chemical"
},
{
  "@id": "_:hazardousSituation1",
  "@type": "riskman:HazardousSituation",
  "riskman:hasName": "Development of gas embolism",
  "riskman:hasPrecedingEvent": {
    "@id": "_:event1"
  }
},
{
  "@id": "_:initialProbability1",
  "@type": "riskman:Probability",
  "riskman:hasValue": "3"
},
{
  "@id": "_:initialRiskLevel1",
  "@type": "riskman:RiskLevel",
  "riskman:hasName": "Initial Risk Level 1",
  "riskman:hasProbability": {
    "@id": "_:initialProbability1"
  },
  "riskman:hasSeverity": {
    "@id": "_:initialSeverity1"
  }
},
{
  "@id": "_:initialSeverity1",
  "@type": "riskman:Severity",
  "riskman:hasValue": "4"
},
{
  "@id": "_:residualProbability1",
  "@type": "riskman:Probability",
  "riskman:hasValue": "2"
},
{
  "@id": "_:residualRiskLevel1",
  "@type": "riskman:RiskLevel",
  "riskman:hasName": "Residual Risk Level 1",
  "riskman:hasProbability": {
    "@id": "_:residualProbability1"
  },
  "riskman:hasSeverity": {
```

```
        "@id": "_:residualSeverity1"
      }
    },
    {
      "@id": "_:residualSeverity1",
      "@type": "riskman:Severity",
      "riskman:hasValue": "3"
    },
    {
      "@id": "_:sda1",
      "@type": "riskman:SDA",
      "riskman:hasName": "Implementation of an automated solvent monitoring system"
    }
  ]
}
```

```
<?xml version="1.0" encoding="utf-8"?>
<rdf:RDF
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:riskman="https://w3id.org/riskman#">

    <rdf:Description rdf:nodeID="controlledRisk1">
        <rdf:type rdf:resource="https://w3id.org/riskman#ControlledRisk"/>
        <riskman:hasID>1</riskman:hasID>
        <riskman:hasAnalyzedRisk rdf:nodeID="analyzedRisk1"/>
        <riskman:hasSDA rdf:nodeID="sda1"/>
        <riskman:hasResidualRiskLevel rdf:nodeID="residualRiskLevel1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="analyzedRisk1">
        <rdf:type rdf:resource="https://w3id.org/riskman#AnalyzedRisk"/>
        <riskman:hasName>Solvent removal risk of brain damage</riskman:hasName>
        <riskman:hasDomainSpecificHazard rdf:nodeID="domainSpecificHazard1"/>
        <riskman:hasHarm rdf:nodeID="harm1"/>
        <riskman:hasDeviceContext rdf:nodeID="deviceContext1"/>
        <riskman:hasHazardousSituation rdf:nodeID="hazardousSituation1"/>
        <riskman:hasInitialRiskLevel rdf:nodeID="initialRiskLevel1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="sda1">
        <rdf:type rdf:resource="https://w3id.org/riskman#SDA"/>
        <riskman:hasName>Implementation of an automated solvent monitoring system</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="residualRiskLevel1">
        <rdf:type rdf:resource="https://w3id.org/riskman#RiskLevel"/>
        <riskman:hasName>Residual Risk Level 1</riskman:hasName>
        <riskman:hasProbability rdf:nodeID="residualProbability1"/>
        <riskman:hasSeverity rdf:nodeID="residualSeverity1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="domainSpecificHazard1">
        <rdf:type rdf:resource="https://w3id.org/riskman#DomainSpecificHazard"/>
        <riskman:hasName>Rotary evaporator solvent removal chemical hazard</riskman:hasName>
        <riskman:hasHazard rdf:nodeID="hazard1"/>
        <riskman:hasDeviceFunction rdf:nodeID="deviceFunction1"/>
        <riskman:hasDeviceComponent rdf:nodeID="deviceComponent1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="harm1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Harm"/>
        <riskman:hasName>Brain damage</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="deviceContext1">
        <rdf:type rdf:resource="https://w3id.org/riskman#DeviceContext"/>
        <riskman:hasName>Chemical manufacturing</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="event1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Event"/>
        <riskman:hasName>Incomplete removal of volatile solvent used in manufacturing</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="hazardousSituation1">
```

```
        <rdf:type rdf:resource="https://w3id.org/riskman#HazardousSituation"/>
        <riskman:hasName>Development of gas embolism</riskman:hasName>
        <riskman:hasPrecedingEvent rdf:nodeID="event1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="initialRiskLevel1">
        <rdf:type rdf:resource="https://w3id.org/riskman#RiskLevel"/>
        <riskman:hasName>Initial Risk Level 1</riskman:hasName>
        <riskman:hasProbability rdf:nodeID="initialProbability1"/>
        <riskman:hasSeverity rdf:nodeID="initialSeverity1"/>
    </rdf:Description>

    <rdf:Description rdf:nodeID="hazard1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Hazard"/>
        <riskman:hasName>Chemical</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="deviceFunction1">
        <rdf:type rdf:resource="https://w3id.org/riskman#DeviceFunction"/>
        <riskman:hasName>Solvent removal</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="deviceComponent1">
        <rdf:type rdf:resource="https://w3id.org/riskman#DeviceComponent"/>
        <riskman:hasName>Rotary evaporator</riskman:hasName>
    </rdf:Description>

    <rdf:Description rdf:nodeID="initialProbability1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Probability"/>
        <riskman:hasValue>3</riskman:hasValue>
    </rdf:Description>

    <rdf:Description rdf:nodeID="initialSeverity1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Severity"/>
        <riskman:hasValue>4</riskman:hasValue>
    </rdf:Description>

    <rdf:Description rdf:nodeID="residualProbability1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Probability"/>
        <riskman:hasValue>2</riskman:hasValue>
    </rdf:Description>

    <rdf:Description rdf:nodeID="residualSeverity1">
        <rdf:type rdf:resource="https://w3id.org/riskman#Severity"/>
        <riskman:hasValue>3</riskman:hasValue>
    </rdf:Description>
</rdf:RDF>
```

8.7 Benefits

8.7.1 Human readability

The use of HTML (and also CSS) enables the presentation of RMFs in any way users see fit. Due to the technical part being hidden when data are rendered, users can choose to present RMF in their preferred way.

8.7.2 Machine readability

Data encoded in RDFa can be easily extracted and then verified/manipulated by any off-the-shelf software available.

8.7.3 Flexibility

Unlike with custom data encoding, users and software developers need not learn custom rules of encoding data (e.g. using custom XML/HTML tags). Instead, they can simply follow the well-defined rules of adding RDFa annotations to any (valid) HTML document.

Additionally, using HTML and RDFa ensures that no custom extraction tools are necessary to extract data encoded in the HTML document.

Note that when using custom tools and a custom data format, such an “ecosystem” would be sensitive to any changes of the underlying data model. This in turn would require the software developers producing the custom tools as well as the users’ encoding data in this custom format to work closely whenever such a change happens.

None of the above downsides apply in the face of HTML and RDFa encoding.

8.7.4 Backward-compatibility

The rendered HTML documents can easily be converted to PDF documents or printed to ensure compatibility with legacy (manual) verification methods.

8.7.5 Forward-compatibility

Because RDFa can make reference to specific vocabularies (e.g. via `vocab` as seen in the example above), other (in particular, future) approaches to digital risk management can be covered within this format. More precisely, if due to changes in practice or legislation, additional information becomes required for submitting risk management documentation, the respective annotations can simply be added via RDFa to HTML in the same manner as before. Updated or new ontologies can define the vocabulary needed for specifying the additional information and these updated/new ontologies can then be additionally employed in the document as above; the HTML/RDFa carrier/container format itself need not be changed.

8.7.6 Use of W3C standards

HTML and RDF(a) are both W3C standards. Adopting systems that adhere to W3C standards is crucial for ensuring interoperability and compatibility, fostering a cohesive and sustainable digital environment. W3C standards uphold universal guidelines, promoting accessibility, security, and a seamless user experience – essential elements in the development of robust and future-proof web technologies.

8.7.7 Out of the box tool support

Generic RDFa is used by 38.7% of all websites [generic-rdfa]. Therefore, an extensive support via software tools is provided for RDF(a), among which we can list:

- distillers (programs to extract RDF from HTML documents),
- reasoners (programs to perform inferences given data and certain reasoning rules),
- validators (programs to check data conformity against a given schema),
- query-services (programs providing standardized interface for users to express complex queries and extract specific information from RDF databases).

Complying to Semantic Web principles guarantees that tool support is provided. Hence it is not needed to develop custom tools for validation and verification purposes. Numerous software allows performing of specialized checks, far beyond standard validation and verification scenarios, which usually employ a given schema. Nevertheless, standard validation and verification needs can easily be satisfied.

9 HTML & RDFa Exchange Format

9.1 Introduction

This clause specifies requirements for the *Exchange Format* based on HTML with semantic markup using concepts expressed in the web-based ontology established by the KIMedS research project – funded by the German government department BMBF under grant (‘Förderkennzeichen’) 13 GW 0552 D.

9.2 Exchange Format (normative)

9.2.1 EXF_REQ_HTML

The manufacturer shall generate the *Exchange Format* - as a valid HTML file according to the W3C standard [html] and – according to the RDF standard [rdfa1] and – according to the XML specification (notably with balanced open/closing tags) and - as an *export file* as specified in this document.

Note 1: This specification uses the HTML element tag *div* for information containers which are described via attributes that refer to concepts expressed in an ontology according to RDF/a.

Note 2: This clause specifies recommended *class* attributes solely for the purpose of rendering. Manufacturers can use *class* attributes and the related style definitions in other suitable ways.

Note 3: This specification does not prohibit the use of other HTML attributes, unless explicitly mentioned in this document. As an example, the use of more *class* attributes is encouraged. The use of anchors and hyperlinks is encouraged.

Note 4: For tool tips (element info when the cursors hovers over it), the use of the attribute *title* is encouraged. None of the *title* attributes in this clause are meant to be normative or a mandatory part of a requirement.

9.2.2 EXF_INF_VOCAB

The manufacturer should generate the *Exchange Format* with a *vocabulary* name using a prefix:

```
<html prefix="riskman: https://w3id.org/riskman/ontology#" lang="en">
...
</html>
```

Note: “riskman:” is an example for a prefix specifying the name of a *vocabulary*. In that case, each reference to that ontology will use “riskman:” as a prefix. Multiple *prefix* attributes can be defined in order to combine multiple ontologies.

9.2.3 EXF_REQ_FILE

The manufacturer shall include as part of the *body* element the information about the device and all related *ControlledRisks* as follows: (with DEVICE_HEADER for the device information and CONTROLLED_RISK* as the placeholder for all *ControlledRisks* of that device)

```
<div class="cell aris" id="Device">
 DEVICE_HEADER
</div><br></br>
<div class="object" title="Risk Table" id=”Content”>
     CONTROLLED_RISK*
</div>
```

9.2.4 EXF_REQ_RDFA_TYPE

The manufacturer shall generate the *Exchange Format* with HTML elements using the attribute *typeof* referring to appropriate RDF/a concepts (classes) located under the ontology identified by the *vocabulary* .

Note: References to conceptual classes are qualified by a common *namespace* qualifier plus the concept name in “upper camel-case”.

9.2.5 EXF_REQ_RDFA_PROP

The manufacturer shall generate the *Exchange Format* with HTML elements using the attributes *property* referring to appropriate RDFa conceptual relations or data (properties), as specified by the ontology identified by the *vocabulary*.

Note: References to properties are qualified by a common *namespace* qualifier plus the property name in “lower camel-case”.

9.2.6 EXF_REQ_CORI

For the set of *ControlledRisks* to be represented in the *Exchange Format*, the manufacturer shall generate a table with – RIT_ID being the identifier of the *ControlledRisk*, – ANALYZED_RISK being the representation of the *AnalyzedRisk* controlled by some *ControlledRisk*, – SDA_VALUE being the representation of the *RiskSDA* used for risk control, as follows:

```
<div class="object" title="Risk Table" id="Content">

          ...

        // each Controlled Risk
        <div class="value" typeof="riskman:ControlledRisk" id="RIT_ID">
           <div class="value" property="riskman:hasAnalyzedRisk">ANALYZED_RISK</div>
           <div class="clos miti" property="riskman:hasSDA">SDA_VALUE</div>
           <div class="prop" property="riskman:hasResidualRiskLevel">RISK_LEVEL</div>
        </div>
        ...

      </div>
```

9.2.7 EXF_REQ_ANALYZED

For each *AnalyzedRisk* to be represented in the *Exchange Format* , the manufacturer shall generate – a row like given below, with – identifiers DSH_ID for the *DomainSpecificHazard*, ARI_ID for the *AnalyzedRisk*, – identifiers COMP_ID, FUNC_ID, HAZ_ID, HARM_ID, for respective terms in properties of

the *DomainSpecificHazard*, – the identifier HASI_ID for the HazardousSituation being analyzed, – term names COMPONENT_NAME, FUNC_NAME, HAZ_NAME, HAZ_SIT_NAME, HARM_NAME, (names should be character strings, see note below) – an optional element TARGET_TABLE for the list of harm targets, – an element RISK_VALUE for the list of components of an unmitigated risk value (severity, probability),

```
<div class="cell aris" typeof="riskman:AnalyzedRisk">
             <div class="value" property="riskman:id" title="id">ARI_ID
                <div class="value" property="riskman:hasDomainSpecificHazard">

           ... for each DomainSpecificHazard
                   <div class="value dosh" typeof="riskman:DomainSpecificHazard" id="DSH_ID">
                      <div class="prop" property="riskman:id" title="id">DSH_ID</div>
                      <div class="prop" property="riskman:hasDeviceComponent" ref="COMP_ID">COMPONENT_N
AME</div>
                      <div class="prop" property="riskman:hasDeviceFunction" ref="FUNC_ID">FUNC_NAME</d
iv>
                      <div class="prop" property="riskman:hasHazard" ref="HAZ_ID">HAZ_NAME</div>
                   </div>
                   ...

                </div>
                <div class="prop" property="riskman:hasTarget">TARGET_TABLE</div>
                <div class="prop" property="riskman:hasHazardousSituation" ref="HASI_ID">HAZ_SIT_NAME</
div>
                <div class="prop" property="riskman:hasHarm">HARM_NAME</div>
                <div class="clos" property="riskman:hasInitialRiskLevel">RISK_VALUE</div>
             </div>
          </div>
```

9.2.8 EXF_INF_DOSH_IDENT

The manufacturer should create the identifier DSH_ID of each *DomainSpecificHazard* with the corresponding identifier RIT_ID of the enclosing *ControlledRisk* being a prefix.

Note: DSH_ID having their RIT_ID as a prefix may be easier to generate and process.

9.2.9 EXF_INF_NAME

Instead of character strings for values in element values of the *Exchange Format*, the manufacturer may also use a tabular format using HTML markup like this:

```
    <div class="object">

       ...multiple entries...
       <div class="value">
    CHARACTER STRING
       </div>

    </div>
```

Note: The device header (DEVICE_HEADER) or the list of targets (TAGET_TABLE) are examples for such a structured representation.

9.2.10 EXF_INF_TARGET

For each *TARGET_TABLE*, the manufacturer should generate the *Exchange Format* as an HTML table containing a row for each *Target* (where TARGET is the string name for a harm subject)

```
    <div class="object" typeof="riskman:Target">
    ... (for each target subject)
        <div class="value"><div class="prop">TARGET</div></div>
    </div>
```

Note: *Target* is a property of *AnalyzedRisk*, with a list of names describing the potential subjects of *Harm*.

9.2.11 EXF_REQ_RISK_LEVEL

For each *RISK_LEVEL* the manufacturer shall generate the *Exchange Format* as an HTML table

```
    <div class="object" typeOf="riskman:RiskLevel">
       <div class="value" property="riskman:hasSeverity"><div class="prop">SEVERITY</div></
div>
       <div class="value" property="riskman:hasProbability"><div class="prop">PROBABILITY</
div></div>
    </div>
```

For each additional attribute (e.g. the risk region), the manufacturer should add an additional row:

```
       <div class="value" title="Risk Region"><div class="prop">RISK REGION</div></div>
```

9.2.12 EXF_REQ_SDAVALUE

For each *RiskSDA* in a *ControlledRisk*, the manufacturer shall generate SDA_VALUE in the *Exchange Format* as an HTML row (with SDA_ID being the identifier of that *Risk SDA* and SUB_SDA_ID being the identifier of any nested *RiskSDAs*)

```
    <div class="value" typeof="riskman:RiskSDA" id="SDA_ID">
       [optional _Assurance_ represented as ASSURANCE]
       <div class="clos" property="riskman:hasSubSDA">

    ... (for each nested SDA)
          <div class="object rsda" typeof="riskman:SDA" id="SUB_SDA_ID">
             <div class="prop" property="riskman:id" title="id">SUB_SDA_ID</div>
             <div class="prop" title="measureId">MEASURE_ID</div>

             <div class="prop" title="sdaName">SDA_NAME</div>
             <div class="prop" title="sdaText">SDA_TEXT</div>
             <div class="prop" title="requirementCode">REQUIREMENT_CODE</div>
          </div>
    ...
       </div>
       <div class="object" property="riskman:hasImplementationManifest" title="Implementati
on">
          <div class="value" typeof="riskman:ImplementationManifest">
             <div class="prop" property="riskman:external" title="external">EXTERNAL</div>
             <div class="prop" property="riskman:proof" title="solution">PROOF</div>
          </div>
       </div>
    </div>
```

9.2.13 EXF_INF_ASSURANCE

For each *Risk SDA* in a *ControlledRisk*, the manufacturer should generate SDA_VALUE in the *Exchange Format* elements with data of an *Assurance Case* as follows.

```
    <div class="prop">
       <div class="object case">
          <div class="value">
             <div class="clos" property="riskman:problem" title="problem">PROBLEM</div>
             <div class="clos" property="riskman:goal" title="goal">GOAL</div>
             <div class="clos" property="riskman:cause" title="cause">CAUSE</div>
          </div>
       </div>
    </div>
```

9.2.14 EXF_INF_TABLES

The manufacturer should generate in the *Exchange Format* a table for all *DeviceComponents*, with COMPONENT_ID being the respective identifier of the *DeviceComponent*.

```
    <div class="object" property="riskman:DeviceComponent" id="regDeviceComponent"><div cla
ss="value">
        ...
    <div class="prop">COMPONENT_ID</div>
        ...
    </div></div>
```

The manufacturer should generate in the *Exchange Format* a table for all *DeviceFunctions*, with FUNCTION_ID being the respective identifier of the *DeviceFunction*.

```
    <div class="object" property="riskman:DeviceFunction" id="regDeviceFunction"><div class
="value">
        ...
    <div class="prop">FUNCTION_ID</div>
        ...
    </div></div>
```

The manufacturer should generate in the *Exchange Format* a table for all *Harms*, with HARM_ID being the respective identifier of the *Harm*.

```
    <div class="object" property="riskman:Harm" id="regHarm"><div class="value">
       ...
       <div class="prop">HARM_ID</div>
       ...
    </div></div>
```

Note: Each table entry can be enhanced with cross-references into related *DomainSpecificHazards*, *AnalyzedRisks* or *ControlledRisks*.

Figure 12 – HTML Toplevel Structure

9.2.15 EXF_INF_TABLE

The manufacturer should generate the *head* element of the *Exchange Format* with a *style* supporting tabular rendering:

```
<style>
.object {
  display: table;
  border: 1px solid black;
  border-collapse: collapse;
}

.value {
  display: table-row;
  overflow:auto;
}

.hedr {
  display: table-cell;
  min-width: 45px;
  border-top: 1px solid black;
  padding: 0px;
}
```

```
.prop {
   display: table-cell;
   min-width: 45px;
   border: 1px solid black;
   border-collapse: collapse;
   padding: 4px;
   overflow:auto;
}

.cell { display: table-cell; border: none; overflow:auto; }
.dsh { min-width: 430px; max-width: 430px; }

.aris { min-width: 740px; max-width: 740px; }

.case { min-width: 340px; max-width: 340px; }

.rsda { min-width: 490px; max-width: 490px; }

.miti { min-width:1140px; max-width:1140px; }

.fill {
  display: table-cell;
  width: 100%;
  border-top: 1px solid black;
  border-bottom: 1px solid black;
}

.clos {
  display: table-cell;
  width: 100%;
  border-top: 1px solid black;
  border-right: 1px solid black;
  border-bottom: 1px solid black;
}

.sep {
  display: table-cell;
  border-top: 1px solid black;
  border-left: 1px solid black;
  border-bottom: 1px solid black;
  padding: 4px;
}
</style>
```

Annex A

Considerations
(informative)

A.1 General

This document specifies a file format for representing, storing and communication of risk control information for a medical device according to ISO 14971. For that purpose, the concept of the Digital Risk Management File (DRMF) is introduced as a structured, electronic container that resembles the “analog” tables that have, up to now, been state of the art for keeping and exchanging risk control information.

The main application of Digital Risk Management Files (DRMF) is for communicating the results of risk management, for inspection and European market approval under the EU MDR. Files using this format can be created and maintained by medical device manufacturers and then be sent to inspectors, authorities and Notified Bodies.

This document explains the underlying *concepts* for the elements in the Digital Risk Management File (DRMF) and a *format* for representing the file as a text string. It does not specify the use or processing of such files; however, the format is intended to support all stages of risk management as indicated by ISO/TR 24971, which are risk analysis, risk evaluation, risk control, evaluation of overall residual risk, risk management review and even (post-) production activities.

A.2 Concepts

For the purpose of capturing the results of risk analysis and risk evaluation, the conceptual model formalizes *harm*, *hazard*, *hazardous situation* and the *risk* (value as a combination of severity and probability). Since ISO 14971 confuses the level of risk (here: *Risk*) with a domain-specific scenario potentially leading to harm, the concept of *DomainSpecificHazard* is introduced as a new concept to capture typical scenarios.

In the context of an identified medical device, the evaluation of the risk scenario specified by a single *DomainSpecificHazard* is captured as one or multiple instances of *AnalyzedRisk*, which focuses on one *Harm* and documents the *risk level prior to mitigation*.

An instance of *ControlledRisk* combines some *AnalyzedRisk* with any measures (zero, one or multiple *RiskSDAs*) that had been chosen as the mitigation, together with the *residual risk level* after that documented mitigation.

Risk control information is captured by instances of *Safe-Design Argument* (*SDA*), which formalizes an aspect of a device-related risk scenario for which the hazardous situation is reduced and/or harm is alleviated. An *SDA* also captures the information how that scenario is being mitigated, i.e. a *reasoning* how a group of measures reduces the risk level related to the risk scenario.

In the current version of this document, little or no ranges, restrictions or code sets for the attributes of *SDA* are specified.

A.3 Format

The format specified as *Exchange Format* combines human-readability with machine-readability. The main goals for selecting a format were: full human visibility for all content of risk control information - what had been stored as tables up to now, and -out-of-the-box use of common, wide-spread browsers when rendering the full view of each element of the digital risk file, and machine-readability based on well-defined mark-up which separates and identifies all values and instances of concepts and relationships as defined the conceptual model.

For that purpose, HTML with additional mark-up has been chosen. That mark-up relates single HTML elements with concepts defined in an ontology that had been established for the purpose of modelling device-related risk control.

A.4 Benefits

A.4.1 General

The main benefits can be seen in the practical support of a consistent Technical File.

A.4.2 Visual Representation

All common browsers in their default mode can be used to view the full content of the Digital Risk Management File (DRMF).

For custom layouts, implementers can add *class* attributes when generating a file conforming to the *Exchange Format*, since no *class* attributes are specified in this document. As a result, the *Exchange Format* allows a high degree of visual layout flexibility.

Furthermore, recipients may adapt the rendering with defining or modifying *styles* (or, CSS) for arbitrary classes when rending such files.

Since no *id* attributes nor *anchor* elements are specified in this document, implementers are free to introduce hyperlinks.

A.4.3 Model-defined content structure

Implementers of generators producing the *Exchange Format* can add scripts to generate tables of defined terms, giving an overview to elements like *Harm*, *Hazard*, *Component*, *Function*, *HazardousSituation* etc. Hyperlinks from the *ControlledRisks* can be added to such term overview tables. This can be used to examine and display coverage of measures over *HazardousSituations*.

A.4.4 Workflow integration

The detailed structure of the *AnalyzedRisks* allows for reuse of either elements of the analysis, for example from a list of pre-defined *DomainSpecificHazards*, or reuse of mitigations from a list of measures represented as *ControlledRisk* in a kind of library. Without any further details on embedding such elements from a library, the degree of reuse seems to be quite high for a new medical device that resembles the intended use and the use environment as other predecessor devices of which risk elements are managed by such a library.

The format separates the device-related *Content* of the digital risk file from an *Envelope* container that keeps a checksum plus a script to redo the checksum at the recipient side. Together with a separate means of authentication, this allows to verify the integrity of the digital risk file: In a simple scenario, the manufacturer sends the checksum via separate eMail to the recipient who then can reproduce this checksum and thus confirm the file integrity.

The integrity checksum feature can furthermore be used as a safe indicator for the need to update or even re-submit: The format does not define *versions* or *stages of editing* (like e.g. *unfinished* elements). However, implementers may add attributes and (inline) script-based functionality to add, evaluate and update such version information. In that case, the checksum is broken, i.e. a new checksum value indicates an update to the file.

An additional attribute to *ControlledRisk* may capture one of these proposed maturity levels:

- “DomainSpecificHazard assigned”,
- “Harm documented”,
- “Pre-Risk evaluated”,
- “SDA implemented”,
- “Residual risk documented”

Such info could be a single attribute with one of six easy-to-remember values like e.g. 0, A, D, E, I, R for empty/assigned/documented/evaluated/implemented/residual risk. Depending on the value of the other attributes - null values or missing attributes - some assessment generator could automatically assign an appropriate maturity value, indicating gaps and open work-items.

A.4.5 References into external databases

Despite the wish of recipients to avoid any references to external IT systems the *requirementCode* in *SDA*, and the *solution* in *Assurance* capture values that are not resolved within the Digital Risk Management File itself.

This document specifies a device header to which additional elements can be added in order to define access to external repositories.

Certain attributes in the device header specify database root URLs or access prefixes can be combined with *requirementCode* and *solution*, such that a globally usable absolute URL can be derived.

Through more attributes (or just the *id*) generated by implementers, identifiers for elements in the *Exchange Format* can be used to refer to external databases and services - notably software development repositories, databases and ALM tools.

Such extra prefix can be represented via additional attributes of the device info header.

A.4.6 References from external services

Vice versa, references managed by external services can “point into” the Digital Risk Management File (DRMF), by using those identifiers stored as element values. This feature needs additional markup (e.g. HTML anchors) which then can be used as targets for simple URL references from repositories or ALM tools into the Digital Risk Management File (DRMF).

Generators of the *ExchangeFormat* can add ‘id’ attributes to elements that will allow to reference not only from within the file but also from some outside IT actor, provided that the path of the file is used as a prefix to the identifier in the ‘id’ attribute.

External services can process *ExternalFiles* with such “id”s and use the “maturity” attribute in order determine “incomplete work” or “next point to update” the DRMF.

A.4.7 Machine-Processing

The parsing of HTML and the ontology-driven extraction of information in the HTML elements is easy and has been demonstrated by simple (script) functions.

It should be noted that a reference to the (external) ontology is specified as an attribute to the top-level table element in HTML. This reference can be used to refer to defined elements (concepts, relationships, properties) of the ontology.

A.5 Basic Considerations

This section is about foundations in resolving digital aggregates (like e.g. the internal representation of risk control according to the conceptual model of clause 5) into some serial (“string”) representation.

In general, the definition of a serial representation consists of defining representations for all the entities in the static model and then determining a walkthrough-*procedure* along all the relationships of the static model that ensures that each entity is being visited – with the idea that this walkthrough describes the overall structure of the serial representation.

As the relationship information of the static model is addressed via the walkthrough, each entity is represented by its attribute values – and in the case of *instances* of *classes* – with an additional primary key.

However, for the purposes of capturing semantic aspects and also for cross-referencing and coverage checks, it is useful to collect all values of each entity type (not only objects) in a registry and assign a concept identifier for referencing each known value, which acts as a primary key, so that independent of whether some entity models a scalar record or an instance of a class, there is always a unique key, which for simplicity, will be called primary key.

Now with having a defined representation for each entity of the model, one can choose a more or less arbitrary walkthrough procedure across the model. However, in the case of an entity type being visited twice during the selected walkthrough, there are two problems: repeating the object representation once more risks running into consistency issues when later filling a file with objects of that entity. In addition – in the “evil” case of cyclic relationships – the walkthrough would turn into an infinite loop.

Both problems justify substituting the full representation of a – repeatedly “visited” – entity with its respective key (concept or primary). Therefore, representations of relationships between entity representations more or less rely on some kind of unique key in order to identify the entities in the internal file. As shown above, such keys are available not only for referencing *instances* of *classes* but also for referencing other entities.

A.6 Serializing the conceptual model for risk control

The device Digital Risk Management File (DRMF) according to this document is assumed to be internally represented in some computer-based application (like a modelling tool or a spreadsheet) as a composed entity modelling a single medical device. This composed entity contains entities which are instances of the classes *Component*, *DeviceContext*, *Function*, *Harm*, *Hazard*, *HazardousSituation*, *DomainSpecificHazard*, *AnalyzedRisk ControlledRisk* and, *RiskSDA* as specified in the preceding clauses of this document.

Per conceptual model (clause 5) we assume that a single medical device is the scope for any Digital Risk Management File (DRMF). Within the scope of an identified device, we can consider *Device Context*, *Component*, *Function*, *Harm*, *Hazard* as “registered terms” (from a limited, known set as it would be from some previous risk table), which are identified by their concept key, and which have an invariant name but no attributes.

In contrast to that, the “larger” objects (*HazardousSituation*, *DomainSpecificHazard*, *AnalyzedRisk ControlledRisk* and, *RiskSDA*) are objects because they model some artifacts of the device life-cycle, and therefore are considered as activities – subject to “authorship”, “modification”, “review”, “release”, and so on, which is why they depend on a primary key to implement the necessary technical identification used for distinguishing any pair of objects that happen to be “equal” (by value) but are still not “the same”.

So when defining the external representation (e.g. file format) of some relationship to an entity type X, there are the following implementation choices:

“X” – the entity X is fully represented by the plain value of all its attributes, or

“refX” – the entity X is being referenced by just replacing it with its key value, leaving it to the referring object to resolve the type and value of this entity (“post-specified”), or

“regX” – the entity X is specified by inserting a suitable structured combination of a registry key, a short textual description plus – optionally – type and further categorization info (“pre-specified”), or

“extX” – the external entity X is referenced with additional data supporting a fully qualified URL to its external repository. This alternative is like “refX” but also includes the base URL for resolving that key, base type of resolving IT system, and proves to be useful when splitting an aggregate into separate partitions or messages that refer to each other.

Annex B

Controlled Vocabulary
(informative)

B.1 Vocabulary

This clause specifies recommendations towards structured encoding of the risk analysis. For automated generation and processing of risk management files, encoding several terms used by ISO 14971 can be supported by controlled vocabularies. The result of a device risk file following the recommendations of this clause is called an *Encoded File*.

B.2 Harm

This sub-section specifies a basis for identifying the instances of *Harm* towards a controlled vocabulary.

It has to be said that each harm instance relevant for device risk analysis usually is a placeholder for a variety of detrimental outcomes unintended by the foreseen user, where such outcomes could be intended by some attacker or malevolent user.

In general, this clause does not specify a *terminology* in the sense of absolute vocabulary terms. Instead for each concept, elements of a combined term are recommended to avoid overly restricting the needs of the device risk analysis. As an example, in the context of a single *AnalyzedRisk*, the specific code for a defined harm related to burns would be “HEAL.1T30.0” as taken from ICD10.

Harm includes physical injury or damage to the health of people, or damage to property or the environment. As a first dimension of harm classification this clause distinguishes the main protection goals essentially being affected (i.e. lost or reduced).

B.2.1 VOC_INF_DEF_IMPACT

The manufacturer should generate an *Encoded File* by identifying for each *Harm* the kind of impact using one of the following elements:

```
HEAL = damage to health including loss of life
CONF = violation of confidentiality of data
DAMG = material damage to the environment
INTG = device damage, device errors or any reduction of the general integrity of documented functions o
r data
AVAI = reduction of the general availability of the documented data or function
```

B.2.2 VOC_INF_DEF_VOCAB

For a refined specification of health effects, terms from SNOMED CT, IMDRF Adverse Event Terminology, Annex E or Annex F or the NCI Thesaurus (“findings”) or other publicly available code sets can be appended. Since terms from both IMDRF AET E/F and NCIT Findings use different prefix letters (‘E’,F’ or ‘C’ respectively), these codes can be immediately appended to the HEAL prefix.

The manufacturer should generate an *Encoded File* by identifying for each *Harm*, any health impact using one of the following terminologies:

```
HEAL.Sccccc where ccccc is a SNOMED CT code, or
HEAL.Eeeeee where eeeee is an IMDRF Adverse Event Term from the E section, or
HEAL.Ffffff where fffff is an IMDRF Adverse Event Term from the F section, or
HEAL.Iiiiii where iiiii is an ICD-9 term, or
HEAL.0iiiii where iiiii is an ICD-10 term, or
HEAL.1iiiii where iiiii is an ICD-11 term.
```

Note: Examples are HEAL.C50536 (NCIThesaurus: ‘Finding by Cause/Permanent Deformation’) or HEAL.F1204 (IMDRF AET Health Effects: ‘Irreversible deterioration’).

B.3 Hazard

B.3.1 General

This section introduces defined terms for hazards that can be related to medical devices based on Annex C.1 in ISO 14971.

B.3.2 Terms

Hazard is defined as the *potential* to cause harm, i.e. the hazard is not an event but a general setting that makes certain events “harmful”.

Cause: In complex settings, *the* single cause of a hazardous situation is hard to determine and often is a “combination of unlikely events”. For the purpose of this section, the concept of hazard as a “potential cause” therefore can be seen as any unexpected technical circumstance that can contribute to a hazardous chain of events.

Event: A specific hazard is based on a device-related technical solution (i.e. one or multiple elements of the device’s implementation) that can contribute to hazardous situations related to that device. It is important to note that hazards are independent of an event or other instances of time.

B.3.3 Agents in Information Security and Physical Scenarios

As a first classification within this “agent dimension” which describes which agent (rather than event) has the potential to lead to the hazardous situation.

Typical physical hazard agents are technical properties of a device that is exposed to or controls physical energies. Therefore one might classify physical hazards by the different types of physical energies or interactions controlled by or expected during the foreseeable ways of handling or using the device.

The agent is categorized according to ISO 14971 Annex C section 1.

It has to be noted that the “Cause” terminology in IMDRF AET is rather addressing the manufacturing cause of reported events than the hazards themselves.

Since data protection is included in the concept of harm, the device’s capability (intended or not) to affect confidentiality, integrity or availability of computing resources -notably data- regularly makes it necessary to consider hazards related to information security.

B.3.4 VOC_INF_HAZ_AGENT

The manufacturer should generate an *Encoded File* by identifying for each *Hazard*, the agent that can cause a hazardous situation:

```
ENRY - energy-related hazard
BIOC - biological/chemical hazard
PERF - performance-related hazard
```

Instead of the term ENRY for an energy-related hazard, the manufacturer should use a more detailed term, as applicable:

```
ACOU - acoustic hazard
ELCT - electric hazard
MECH - mechanical hazard
POTE - stored-energy hazard (e.g. masses in height, charged batteries)
RADI - radiation
THER - thermal
```

Instead of the term MECH for a mechanical hazard, the manufacturer should use a more detailed term, as applicable:

```
MOVE - motoric forces which can move or rotate masses
SUSP - or suspending parts, which might break or bend
EDGE - sharp edges or holes at the device/component surface
PRES - low pressure (suction) or high pressure of liquids or gases
VIBR - mechanical vibrations of any kind
```

Instead of the term ELCT for an electrical hazard, the manufacturer should use a more detailed term, as applicable:

```
MICR - microwaves
LITE - light
IRAD - ionizing radiation
MAGN - magnetic hazards
```

```
CURR - hazards resulting from electrical current
VOLT - hazards resulting from static voltage
```

Instead of the term BIOC for a biochemical hazard, the manufacturer should use a more detailed term, as applicable:

```
BIOL - biological interactions including infection with viruses or bacteria
TOXI - toxic substances or other substances adversely affecting the metabolism or general health
CHEM - chemical interaction including floods, humidity, vapours, dust, gases, corrosive/radioactive/con
taminating substances
IMUN - immunological interactions that are related to the body's response to external agents
```

Instead of the term PERF for a performance-related hazard, the manufacturer should use a more detailed term, as applicable:

```
DATA - data loss or errors
DELV - interfacing, input, output errors
DIAG - diagnostic function/data absence or errors
FUNC - other lack or errors of functionality
```

B.4 Hazardous Situation and Causes

B.4.1 General

A hazardous situation is a circumstance which is influenced by one or multiple hazards. In this specification, the model construct of *AnalyzedRisk* combines one *Harm* and one *Hazard* (obtained from the higher-level *DomainSpecificHazard*) and relates both to a *HazardousSituation*.

For the purposes of constructing an *AnalyzedRisk*, the *Harm* to be modelled can specifiy the most severe outcome covered by the *Hazardous Situation* specified.

Causes can be internal or external to the device, with internal events simply being the result of device malfunction which can be refined into unexpected (UNEX) or undocumented (UDOC) or unspecified (USPC) behaviour, depending on where in the life-cycle the deviation occurred.

External causes can be distinguished by their origin in causes from environment (ENVI), operators (OPTR), (which in turn might be administrators, service staff, medical users, lay persons) or even patients (PATI) themselves.

Again we have to point out that the Cause terminology in IMDRF AET also lists processual and manufacturing causes which play a rather indirect role in a sequence of events. Rather it seems beneficial to document the ‘real-time’ sequence of events and then determine the manufacturing cause.

B.4.2 Usage Scenarios

B.4.3 VOC_INF_DEF_USAGE

The manufacturer should generate an *EncodedFile* by identifying for each *Hazard* the kind of using the medical device that contributes to the situation:

```
SHIP - during device shipping and handling
STOR - during device storage
INST - during device installation and configuration
INTD - during the specified intended use
CLEN - during cleaning the device
SERV - during service to, or maintenance of the device
MISU - during misuse of the device
DUMP - during decommissioning / undocumented handling / undocumented storage
```

In this scheme, hazards related to the device in general (i.e. while the device is not necessarily being operated, e.g. static decomposition while the device is off or idle) should be classified as being in hazards related to its intended use and without any suffix = ‘INTD’.

Note: As a more precise classification of the intended use (INTD), the manufacturer can further refine this class INTD by a self-defined suffix describing the specific device function; example: INTD.PatientRegistration.

B.4.4 VOC_INF_DEF_CAUSE

The manufacturer should generate an *Encoded File* by identifying for each *HazardousSituation*, its cause as:

```
UNEX - unexpected state of the device
UDOC - undocumented state of the device
```

```
USPC - unknown or non-specified state of the device's design
ENVI - unexpected state of the environment (includes interfaces)
OPTR - unexpected action of the operator
PATI - unexpected action of the patient
```

B.5 Summary

In the practical world of device manufacturing, most devices have a technical ‘ancestor’ or ‘sibling’, from which the term lists may be taken as a starting point, such that the classes along the above dimensions can then help to determine additional terms and to also rule out some non-applicable hazards.

A database of *DomainSpecificHazards* can represent, provide and check relevant *Harm* and *Hazard* combinations.

Annex C

Internal Storage Format
(informative)

C.1 Introduction

This clause specifies general requirements for representations suitable for storing device risk assessment and control information as specified in the clauses on the underlying conceptual model and on the vocabulary and terms. The file for which the risk control information format is specified in this clause is called the *internal file*. The intention of this clause is to ensure that the *internal file* contains a text string describing all relevant content of the internal device risk assessment and control information, such that all logical risk control information can be reconstructed from information in the *internal file*.

One application of the *internal file* can be the temporary, local storage (e.g. by the manufacturer) for subsequent electronic editing, storing or processing by the same organisation.

The formatting requirements for the purposes of archive and export are specified in subsequent clauses and further restrict the specifications in this clause. Therefore, the requirements in this clause are a prerequisite for archive and export. Note that, prior to archive or export, the omission of some attributes or references (due to missing information) is not an obstacle to constructing a device risk file.

The entity who is responsible for creating the *internal file* is called the *manufacturer*.

For creation of Digital Risk Management Files (DRMF) (i.e. for communication, export or archive) application of this clause is not required.

Note 1: An *internal file* can be used for internal storage while editing the risk control information with tools. An *internal file* supports generation of files according to the *exchange format*.

Note 2: Throughout this clause, the tag…

```
"X" denotes a value representation of one X, and
"regX" denotes a (comprehensive) list of values of one or many X, and
"refX" the primary key value -- without any markup or so -- to one instance of X, and
"relX" a list of references to one or many X.
```

C.2 Recommendations

C.2.1 IFF_INF_ABS_FILE

The manufacturer should generate the *internal file* as an *abstract file* as specified in this document.

C.2.2 IFF_INF_FILE_STRUCTURE

The manufacturer should include as part of the *internal file* at least

- a tag “device”, listing one *Device* header, and
- a tag “regComponent”, listing each *Component* value, and
- a tag “regContext”, listing each *Context* value, and
- a tag “regFunction”, listing each *Function* value, and
- a tag “regHazard”, listing each *Hazard* value, and
- a tag “regHarm”, listing each *Harm* value, and
- a tag “regHazardousSituation”, listing each *HazardousSituation* value, and
- a tag “regControlledRisk”, listing each *ControlledRisk* value, and
- a tag “relSDA” with a list of values of *RiskSDA*.

C.2.3 IFF_INF_HEADER

The manufacturer should generate the *internal file* with a device header information like this:

- a tag “entity” describing the manufacturer of the device,
- a tag “project” describing the internal, administrative name of the product or product family,
- a tag “version” that at least distinguishes changes in risk-related information of the device master data, and
- an optional tag “udi” capturing an identification used for submission / approval purposes, and
- an optional tag “urlRequirement” with a URL prefix into an external “requirements” database, and
- an optional tag “urlSolution” with a URL prefix into an external “test-case” database,

The manufacturer should assign a new version at least in case any risk-related changes in requirements, design or implementation occur.

C.2.4 IFF_INF_CORI_VALUE (Controlled-Risk Value)

The manufacturer should represent each instance of *ControlledRisk* in the *internal file* like this:

- a tag “id” with a key unique within the *internal file* , and
- a tag “title” with the name “ControlledRisk”, and
- a tag “refComponent” with a reference to the component considered, and
- a tag “refFunction” with a reference to the function considered, and
- a tag “harm” with a full name of the harm addressed, and
- a tag “refHazard” with a reference to the hazard list considered, and
- a tag “regHazard” with the values of the hazards considered, and
- an optional tag “regEncodedHazard” with the encoded values of the hazard terms considered, and
- a tag “regAnalyzedRisk” with a list of values of *AnalyzedRisk*, which themselves can contain the respective *ControlledRisk* attributes, in case that exists.

Note: Some *DomainSpecificHazard* instance is uniquely determined by the combination of references to one *Component*, and to one *Function*, and to one *Hazard*.

C.2.5 IFF_INF_ARI_VALUE (Analyzed-Risk Value)

The manufacturer should represent each instance of *AnalyzedRisk* in the *internal file* like this:

- a tag “id” with a key unique within the *internal file*, and
- a tag “title” with the name “AnalyzedRisk”, and
- a tag “refCOR” with a reference to the related *ControlledRisk*, and
- a tag “refHS” with a reference to the hazardous situation addressed, and
- a tag “refHarm” with a reference to the harm addressed, and
- an optional tag “regTarget” with a list of the subjects protected by the *AnalyzedRisk*, and
- a tag “risk” with the value of the *RiskLevel* before mitigation.

C.2.6 IFF_INF_RISK_CONTROL (Controlled-Risk Value)

The manufacturer should represent each instance of *ControlledRisk* in the *internal file* like this:

- all tags of the associated *AnalyzedRisk*, and
- a tag “refRiskSDA” with a reference to the top-level *RiskSDA*, and
- a tag “residualRisk” with the value of the *RiskLevel* after mitigation.

Note: In the *internal file*, any *ControlledRisk* appears as an instance of *AnalyzedRisk*, plus these two extra tags.

C.2.7 IFF_INF_RISK_LEVEL (Risk-level Value)

In the *internal file*, the manufacturer should represent instances of the class *RiskLevel* like this:

- a tag “severity” with a text describing the severity level as one dimension of a product-specific risk matrix
- a tag “probability” with a text describing the probability level as one dimension of a product-specific risk matrix
- an optional tag “riskRegion” with a text describing the risk region within a product-specific risk matrix

C.2.8 IFF_INF_SDA_VALUE (Safe Design Argument Value)

In the *internal file* the manufacturer should represent instances of *RiskSDA* like this:

- a tag “id” and a key unique within the *internal file*, and
- a tag “goal” and the harm text addressed by the SDA claim, and
- a tag “cause” and the hazardous situation text addressed by the SDA claim, and
- a tag “problem” and the hazard text addressed by the SDA claim, and
- a tag “argument” and the argument text (at least one of the values “PREVENT” or “ALLEVIATE”), and
- an optional tag “regAssurance” with a list of all supporting (nested) *SDAs* beneath this *RiskSDA*, and
- an optional tag “solution” specifying the corresponding *ImplementationManifest* data. (that can be qualified using the “urlSolution” attribute of the *Device* header).

The manufacturer should specify in the *regAssurance* list all (nested) *SDAs* values, that support the argument.

The manufacturer should specify either the corresponding *ImplementationManifest* as a character string in the *solution* attribute.

Note 1: Because of their tree-like composition in exactly one *RiskSDA* instance, all representations of nested *SDAs* can be textually nested within their “parent” *RiskSDA*.

Note 2: With some *urlSolution* attribute in the device header, the *solution* attribute can be qualified, in order to form a URL into some software application life-cycle tool. In the simplest fashion, the solution text is just a traceable key into the test specification list.

C.2.9 IFF_INF_ASU_VALUE (Assurance Value)

In the *internal file*, the manufacturer should represent the respective *Assurance* instance x via

- a tag “id” and a key unique within the *internal file*, and
- a tag “sdaAssurance” which itself has a tag “text” with a description of the control measure and an optional character string “requirementCode” with a reference (that can be qualified using the “urlRequirement” attribute of the *Device* header).

Note: With some *urlRequirement* attribute in the device header, the *requirementCode* can be qualified, in order to form a URL into some software application life-cycle tool. In the simplest fashion, the value of *requirementCode* is just a traceable key into the requirements specification list.

C.2.10 IFF_INF_NO_EXT_REF (No External References Allowed)

The manufacturer should create the *internal file* without dependencies on external tools nor making any assumptions about the external IT environment.

Note: There are a few exceptions:

- the optional *solution* attribute of *RiskSDA*, and
- the optional *requirementCode* attribute of *Assurance*.

Such references are qualified by the information in the *Device* header of the file, which acts as a prefix to the attribute information in order to build an external reference (URI) into some device repository or device master record.

Annex D

List of Links

D.1 Links to: Terms

Analyzed risk

Assurance SDA

Assurance SDAI

Controlled risk

Device component

Device context

Device function

Domain-specific hazard

Event

Harm

Hazard

Hazardous situation

Implementation manifest

Instructions for use

Intended environment of use

Intended purpose

Intended use, intended purpose

Objective evidence

P1

P2

Residual risk

Risk

Risk analysis

Risk control

Risk level

Risk matrix

Risk SDA

Risk SDAI

SDA (Safe design argument)

SDAI (SDA implementation)

Safety

Safety assurance

Severity

State of the art

Use-Context

D.2 Links to: Conceptual Model

MOD_DEF_ARI

MOD_DEF_ASSURANCE

MOD_DEF_COMP

MOD_DEF_COR

MOD_DEF_FUNCTION

MOD_DEF_SDA

MOD_DEF_SITUATION

MOD_DEF_STRATEGY

MOD_REQ_DSH

MOD_REQ_HARM

MOD_REQ_HAZARD

D.3 Links to: Abstract Storage Format

ASF_INF_REG_KEY (Registry Key)

ASF_REQ_DEVICE_HEADER

ASF_REQ_DEVICE_VERSION

ASF_REQ_PRIM_KEY (Primary Key)

D.4 Links to: Requirements for Export

RFE_INF_ENCODE_UTF

RFE_REQ_ENCODING

RFE_REQ_ENVELOPE

RFE_REQ_HUMAN

RFE_REQ_MACHINE

RFE_REQ_NO_EXT_KEYS

RFE_REQ_SEE_ALL

D.5 Links to: Using HTML with RDFa (informative)

INT_INF_ANALYZEDRISK

INT_INF_COMP

INT_INF_COMPLETE

INT_INF_CONTROL

INT_INF_ENC_COMP (Encoded Component)

INT_INF_FUNC

INT_INF_HARM

INT_INF_HASI

INT_INF_HAZ

INT_INF_IMDRF_CAUSE (IMDRF AET Cause)

INT_INF_IMDRF_HEALTH (IMDRF AET Health Effects)

INT_INF_IMDRF_PROBLEM (IMDRF AET Device Problem)

INT_INF_POST_EVAL

INT_INF_PRE_EVAL

INT_INF_MITIGATED

D.6 Links to: HTML & RDFa Exchange Format

EXF_INF_ASSURANCE

EXF_INF_NAME

EXF_INF_TABLE

EXF_INF_TABLES

EXF_INF_TARGET

EXF_INF_VOCAB

EXF_REQ_ANALYZED

EXF_REQ_CORI

EXF_REQ_FILE

EXF_REQ_HTML

EXF_REQ_RDFA_PROP

EXF_REQ_RDFA_TYPE

EXF_REQ_RISK_LEVEL

EXF_REQ_SDAVALUE

D.7 Links to: Controlled Vocabulary (informative)

VOC_INF_DEF_CAUSE

VOC_INF_HAZ_AGENT

VOC_INF_DEF_IMPACT

VOC_INF_DEF_USAGE

VOC_INF_DEF_VOCAB

D.8 Links to: Internal Storage Format (informative)

IFF_INF_ABS_FILE

IFF_INF_ARI_VALUE (Analyzed-Risk Value)

IFF_INF_ASU_VALUE (Assurance Value)

IFF_INF_CORI_VALUE (Controlled-Risk Value)

IFF_INF_FILE_STRUCTURE

IFF_INF_HEADER

IFF_INF_NO_EXT_REF (No External References Allowed)

IFF_INF_RISK_CONTROL (Controlled-Risk Value)

IFF_INF_RISK_LEVEL (Risk-level Value)

IFF_INF_SDA_VALUE (Safe Design Argument Value)

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.

Merianstraße 28
63069 Offenbach am Main
Tel. +49 69 6308-0
service@vde.com
www.vde.com

VDE