ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

The Terminological Analysis Method SemAn and its Implementation

Peter Bernard Ladkin[1], Lou Xinxin[2], Dieter Schnäpp[3]

1. Causalis Ingenieurgesellschaft mbH, Bielefeld, Germany.
2. Causalis Ing.-GmbH. Currently at TÜV Süd, München, Germany.
3. Technische Universität Braunschweig, Institut ITL. Currently at DKE, Offenbach.

Abstract

We present the method "SemAn" for the semantic analysis of electrotechnological definitions appearing in IEC standards. SemAn is accompanied by a software tool, the SemAn Analyser, which outputs partial SemAn results in a pretty-printed and annotated format retaining the symbol-for-symbol syntax of the original definiens text. We discuss the purpose and use of this method and tool.

1 Introduction

1.1 Intellectual Background

Gottlob Frege published his *Begriffschrift* (literally, "concept-writing") in 1879 (Frege 1879); see also Wikipedia (Begriffschrift 2023). It was by no means the first attempt to render natural language into a form in which logical reasoning could be formulated and used (Aristostle's Syllogistic is perhaps the first such writing), but it has become the most successful, resulting almost immediately in what we know today as Predicate Logic, or First-Order Logic (Goldrei 2005). The use of such formal languages and logic is widespread in digital-computer science, not only in building circuits which exemplify calculations based on the "logical constants" AND, OR and NOT, but in formal languages for specifying and describing computations, as well as systems which check whether such descriptions (including high-level-language "source code") fulfil their expectations.

The ability to render natural language into formal language is taught to most university freshman philosophy students in introductory logic courses. However, rendering the semantics of most of any natural language (such as English) in a modern-logical system is far more problematic, quite apart from the doubts concerning whether such an enterprise can be at all successful (Wittgenstein 1953/1967); see also (Kripke 1982). A series of sophisticated attempts at a formal semantics for English were made by Richard Montague from 1955 to around 1970 (Montague 1974), using Higher-Order Modal Logic. Montague Semantics has subsequently been quite successfully pursued in linguistics (Janssen 2011). There are other formal semantics such as Situation Semantics (Kratzer 2007). Almost all these formal (logical) renderings refer to objects, their properties and relations between them. There is a discipline which looks at what objects the use of a natural language presumes; known as natural language ontology (Moltmann 2022). The study of ontology (rather, ontologies) is now pursued in terminological definition in computer science, and

increasingly in related engineering disciplines, e.g. the SCSC Ontology Working Group (Safety-Critical Systems Club 2023).

Ontologies speak to what objects there are. Besides objects, Fregean *Begriffschrift* and its formal-logical successors speak to properties of those objects and their relations; at time of writing, properties and relations are not as well-developed interests in computer science as objects are, although they are essential for a rendering of natural language into such formal languages.

Functional requirements specifications for digital-computer-based systems may often be rendered in formal languages specially developed for the purpose, as may, rather more easily, specifications for algorithms; see, for example Lamport (2003). The purposes of this move to formality include avoiding ambiguity, as well as enabling mathematically-rigorous checking that, say, a computer program actually fulfils its functional requirements. However, in broader engineering disciplines, it is often required that functional specifications are written in natural language — indeed, that the natural-language specification is the legally-valid specification of requirements. There are thus two main reasons why it is desirable that engineering concepts in natural language be rendered more formally:

1. It ensures that engineers are using a term to refer to one and the same concept in various working environments, in particular when they are discussing technical matters; and
2. It allows legal requirements to be formulated in such a way that enables mathematically-rigorous checking that, say, a computer program written by a supplier fulfils those requirements.

Both of these are major undertakings. The first is good practice, but only the second is (recently) recognised as an engineering discipline in its own right. The importance of the former is, however, understated. Concepts such as "risk" are formally defined in electrotechnical standards — and there are many of them, some of them very different from others. Risk is a central concept for safety engineering, and there is at time of writing an Advisory Group of the International Electrotechnical Commission (IEC) attempting to arrive at a "harmonised" definition of the concept, because of the engineering problems caused by the plethora of existing definitions (IEC 2023).

More importantly, people have been jailed in England based on arguments about the meaning of electrotechnical terminology and what this implies for software-based system behaviour. The transcript of the trial of Ms. Seema Misra for fraud in the use of the Post Office Horizon system is available (Mason 2015). There is a commentary on the use of technical terminology in this and related cases (Ladkin 2020). We are happy to report that Ms. Misra was acquitted on appeal in April 2021.

We conclude it is important to get electrotechnical terminology "right". Whatever "right" may be, considering what happened to Ms. Misra, it should reflect the reality of systems and their behaviour; other desirable properties may be clarity, and non-ambiguity (absence of homonyms).

It is not our purpose here to discuss general properties of terminology further, but rather to present a technique and a software implementation of that technique that has had some encouraging application to the analysis of electrotechnical terminology defined in standards of the International Electrotechnical Commission to enhance clarity and highlight ambiguity and point, in some cases, towards resolution.

The technique is called "SemAn", and the software tool the "SemAn Analyser". SemAn is conceptually a translation of (actual) terminology definitions into a language of Sorted

First-Order Quantifier-Free Logic. Illustrations are given below of how this helps to analyse the concepts involved. The SemAn Analyser annotates the natural-language definitions through the devices of pretty-printing and annotation with the logical constants AND and OR (quite literally, "annotates" — all symbols of the original definition are retained in the exact order in which they occur); again, examples are given below.

In contrast to philosophical or (most) linguistic purposes, the point of SemAn and the SemAn Analyser is not to render the exact meaning of a natural language phrase, but to exhibit a (*not* "the") logical structure, which will show engineers more clearly what is or seems to be meant, and highlight various possibilities for improvement. Terminology work is ongoing at the IEC and the SemAn Analyser annotations have been (cautiously, in preliminary viewing) welcomed.

SemAn and the SemAn Analyser were developed on the terminology introduced in the IEC standards and standards-like documents on functional safety and cybersecurity[1]. We can confidently state that for this specific terminology corpus, which includes over 450 terms with between 60 and 70 of them multiply/variantly defined, SemAn and the SemAn Analyser render a service known to be needed and indeed "required" by the ISO/IEC Directives but (we would suggest) often absent.

1.2 Conventions Used

In this paper, we give and discuss SemAn in two ways: as a principled method, and as the output to a tool partially implementing the method, known as the SemAn Analyser. We write manual SemAn, in Sub-sections 4.3 and 4.3, in a language of sorted predicate logic. The output of the SemAn Analyser is given pretty-printed in `Courier` font. We need to distinguish the two analyses, for example a manual SemAn introduces Meaning Postulates (MPs), and the SemAn Analyser has no facility to do this. We find that distinguishing the analyses typographically is the easiest way to do so.

2 Semantic Analysis by Means of SemAn: Preliminaries

2.1 The Scope of SemAn

The term "semantic analysis" is used here as a technical term which refers to a specific way in which definitions in technical terminology may be analysed. The SemAn method has been developed specifically for electrotechnical terminology occurring in Clause 3, "Terms and Definitions", of IEC standards. Manual examples of SemAn are given first, below, to show the method. Output of the SemAn Analyser is formatted ("pretty-printed") text with annotations illustrating logical structure.

SemAn is particularly geared towards comparative analysis, in which one has syntactically-varying definitions of the same term (homonyms), or syntactically-similar definitions of different terms (quasi-synonyms). SemAn allows the similarities and divergences between the terms to be illustrated in a canonical and intuitive way. SemAn

[1] The original list of definitions was compiled in Project Harbsafe by Sven Müller, at the time with VDE and at time of writing with DB Systel GmbH, from IEC-61508-4 2010, IEC-62443-2-1 2010, IEC-62443-2-4 2015, IEC-62443-3-1 2009, IEC-62443-3-2 2020, IEC-62443-3-3 2013, IEC-63069 2019, ISO/IEC-51 2014, and IEC-120 2018 (IEC various dates) (ISO/IEC2014).

exhibits the logico-semantic structure of individual natural-language definitions, so it also enables individual definitions to be improved to enhance understanding.

There is no one unique resulting analysis of a definition in SemAn. One may choose different primitives (unanalysed words or phrases): in one analysis, a syntactic unit may be taken to be primitive; in another analysis, a slight divergence of that syntactic unit from another item in a related definition may require the unit be further analysed (as a compound of further primitives) so that the divergence can be exactly specified[2].

The software tool SemAn Analyser gives one output per conformant definition, illustrating the logical form of the definition while taking the individual syntactic units to be primitive. It annotates the *definiens*[3] with logical constants and punctuation and pretty-prints it, as for example in Sub-section 2.4. Further examples of SemAn Analyser output are given in Section 3.

2.2 The Formal Language of SemAn

Formal semantic analysis in the linguistics of natural language, as it is practiced today, uses formal annotation into which a target definition is parsed. So does SemAn. The language used is isomorphic to the language of first-order logic (FOL). An introduction to the language of propositional logic and FOL is to be found in Goldrei (2005). Nearly a century and a half of experience with FOL has established its pre-eminence as a system in which assertions may be made with precision, and formal inferences may be precisely codified (there are other logics, often known as higher-order or non-classical logics, depending on their type, which are useful for similar purposes in domains in which FOL is limited). The language of FOL (LFOL) consists of

- predicate symbols;
- object symbols (divided into constants, which SemAn uses, and variables, which SemAn does not use);
- functional symbols (largely not used in SemAn);
- the logical constants AND, OR (used widely in SemAn and SemAn Analyser);
- the logical constant NOT (largely not used in SemAn and SemAn Analyser, because negations are often incorporated into the terms themselves); and
- quantifiers, largely incorporated into the syntactic items themselves (as negation often is).

The meaningful syntactic units of LFOL are sentences. There are no meaningful parts of sentences, such as phrases, which are not themselves sentences. This entails that translating natural language expressions into LFOL requires expanding the expressions to conform with the phraseology of LFOL.

2.3 Translating Natural Language Phrases into the Language of SemAn

As far as is yet known, there is no generally-accepted algorithm for translating natural language sentences into LFOL in a way that preserves their meaning. However, there are some more or less standard translation rules, partly illustrated below.

[2] An example is given in the manual SemAn of "harm" in Sub-section 4.2 below, in which "physical injury" and "damage to the health of a person" are discussed.

[3] In linguistics and analytical philosophy, a term being defined is known as the "*definiendum*" and the definition the "*definiens*". IEC uses the words "term" and "definition", but these have wider general use than just in Clause 3 of standards. We thus prefer to use technical terms for the linguistic items appearing in such Clauses 3.

(English) *John or Joan opened the front door*

First, the phrase in subject position, *John or Joan*, has no equivalent in LFOL. In LFOL, OR may only be used to conjoin sentences. Second, there are no syntactic elements corresponding to phrases in LFOL, only sentences and their component symbols. Third, the sentence intuitively speaks to one of two situations; one in which John opened the front door, and another in which Joan opened the front door (as well as a third in which they both did, but presumably not simultaneously). These observations may be used to convert the English sentence into one conforming to LFOL with the same intuitive meaning, namely:

(LFOL) *John opened the front door OR Joan opened the front door*

In English, phrases in subject position or object position can also be lists, with one constant (usually separating the last two list words) and separated by commas, as in

(English) *John, Joan or Jeremiah opened the front door*

Similar principles apply here as above, and we obtain the translation

(LFOL) *John opened the front door OR Joan opened the front door OR Jeremiah opened the front door*

A further step is that of constructing synonyms for predicates. In this example, three different people seem to have engaged in the same action, "*opened the front door*". In LFOL, the following action can be performed. A simpler symbol may be used to stand for the verb phrase "*opened the front door*". Second, whereas in English the subject (the person who opened the door) is typically written first and the predicate (the action) follows, with no punctuation, as in *John opened the front door*, in LFOL the assertion is expressed in a symbolic form akin to that of the elementary mathematics of functions: the argument (whoever did the opening) is expressed in parentheses after the predicate, as in *opened-the-front-door(John)* (here, hyphens are used to indicate that the predicate is denoted by a string of words rather than a single word). When symbol P is chosen to represent *opened the front door*, then this becomes syntactically easier to read.

(LFOL) Let the symbol *P* stand for the predicate "*opened the front door*". Then the assertion becomes:

P(John) OR P(Joan) OR P(Jeremiah)

SemAn uses such a natural-language version of LFOL as has been illustrated above. By experience, the illustrated translations seem to cover the routine majority of the task of translation. This language will become clearer when examples are discussed below.

3 The SemAn Analyser

3.1 *Modus Operandi*

The SemAn Analyser, in contrast to (manual) SemAn, does not use LFOL at all. It parses, annotates and pretty-prints the words and punctuation in the definition itself, in the order in which they occur. A manual translation from SemAn Analyser output into LFOL is intended to be straightforward. If a translation is not straightforward, this serves as an indication that the original definition proposed may be deficient; unclear, say. The recommended remedy is to modify the source definition so that the translation of SemAn Analyser output into LFOL becomes straightforward.

The SemAn Analyser:

- Takes all English words as primitive formal symbols
- Exhibits the logical structure of phrases by means of annotations using the logical constants (AND, OR, more rarely NOT) and marked indents

3.2 Implementation

The SemAn Analyser uses Dependency Parsing (Jurafsky and Martin 2020). It is programmed using the Dependency-Parsing suite spaCy (ExplosionAI n.d.). The programming is largely due to the second author, with help from the third author. All authors were continually involved in the evolution of the output specification.

3.3 A Simple Example

Consider the two following definitions of "signal". These are not original IEC terminology, but are "cleaned up" from existing definitions. The *definiendum* is given in bold-face font on a line by itself. The *definiens* follows on the next line, optionally prefixed by an "area of application" given in angle brackets. Here, the areas of application are "electrical", respectively "information".

signal
<electrical> electrical impulse controlled or observed by a test resource

signal
<information> visual, audible, or other indication used to convey information

The annotated versions would ideally be[4]:

```
signal:
<electrical> electrical impulse controlled or observed by a test
resource
\\
electrical impulse
                      > [OR] controlled
                      > [OR] or observed
                                > by a test resource
signal:
<information> visual, audible, or other indication used to convey
information
\\
     > [OR] visual
     > [OR] , audible
     > [OR] , or other indication
                           > used to convey information
```

SemAn Analyser thus exhibits the first as a sort, *electrical impulse*, with one of two relations to a *test resource*, that of being *controlled* or that of being *observed*. The second definition is a disjunction: the qualifier of all three disjuncts is that they are *used to convey information*, and the information conveyer may be *visual* or *audible* or an *other indication*.

[4] It has been suggested that there might be an alternative reading. This may well be. One of the purposes of SemAn Analyser output is to make clear such possibilities. SemAn Analyser output is dependent upon a non-deterministic parser, so such possibilities can be expected to arise simply from the parsing operation itself.

In this case, with simple and short definitions which have no key terms in common, a comparison of the two *definiens* shows that they are clearly distinct concepts.

Note: the above SemAn renderings are manual. The current implementation of the SemAn Analyser does not in fact output these annotations, although we wish it did — it renders both definitions without the annotations shown here. However, the examples of *application*, *harm* and *asset*, following, are indeed output by the current implementation of SemAn Analyser.

3.4 "Application"

An example which intuitively illustrates the benefits of logical annotation in more complex definitions is that of *application*, defined as

```
software program that performs specific functions initiated
by a user command or a process event and that can be
executed without access to system control, monitoring, or
administrative privileges
```

Parsed, this becomes:

```
\\
     software program
          > [AND] that performs specific functions
                       > initiated by a | [OR] user command
                                        | [OR] or a process event
          > [AND] and that can be executed without access
                       > to | [OR] system control
                            | [OR] , monitoring
                            | [OR] , or administrative privileges
```

This shows the clear logical structure that:

- this is a software program (defines the *sort*, the type of object which is being talked about);
- that this program has two properties:
  - of performing specific functions …
  - of executing without access to …
- and that these properties have further logical details.

3.5 "Harm"

The annotated/pretty-printed output of the SemAn Analyser invoked on the term *harm* is as follows::

```
67.
harm:
physical injury or damage to the health of people or damage to
property or the environment
\\
     [OR] physical injury
     [OR] or damage
               > [OR] to the health
                            > of people
               > [OR] to property
               > [OR] or the environment
[Source: IEC 61508-4:2010]
```

It can be seen that the SemAn Analyser takes the definiens as syntactically given and marks it up. It treats *physical injury* as a primitive. Below (Sub-section 4.2), a manual SemAn does not take this phrase as primitive, but invokes *Meaning Postulates*, which allow *physical injury* to be compared with *damage to the health of people* in order to determine if the definition can be expressed more succinctly and clearly (answer: yes).

It follows that the output of the SemAn Analyser is not a full SemAn, but a preliminary processing of the definition that exhibits certain formal features of the definition, enabling improvements to be made where they are appropriate, and which enables a human analyst to continue the SemAn if desired; for example by considering the meaning of *physical injury* and relating it to *damage to the health of people*. It is also clear from the example of *signal* that the current implementation of the SemAn Analyser does not quite yet do all we wish to expect of it.

4 Examples of SemAn Analyser Output and of SemAn

4.1 Output of SemAn Analyser on *asset*

There are two non-identical definitions of *asset* in the IEC 62443 series of standards. Both are considered below, in order to illustrate the harmonisation task, and to show how much easier it is made by using the SemAn Analyser.

SemAn Analyser output on the two definitions of asset is:

```
10.
asset:
physical or logical object owned by or under the custodial duties
of an organization, having either a perceived or actual value to
the organization
\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]

11.
asset:
physical or logical object having either a perceived or actual
value to the IACS
\\
     physical or logical object
          > having either a perceived or actual value
                 > to the IACS
[Source: IEC 62443-3-3:2013]
```

This annotated parsing/pretty-printing immediately shows a number of similarities and differences in the two definitions. First, an *asset* is a *physical or logical object*[5]. Second, it *[has] a perceived or actual value*. To whom the value accrues is different in the two cases (some implicit *organisation* in the first, presumably a human organisation such as a company; in the second, a system, namely the *IACS* (Industrial Automation and Control System)). Similarly, the first definition mentions custodial duties associated with the asset; the second mentions no such duties.

This comparison gives clear indications of difference, and therefore the scope of discussion, to domain experts attempted to harmonise the two definitions. The harmonisation task here is twofold:

- To whom/what does the *value* of the *asset* accrue?
- Is the ownership/custody of the asset a key property? Is it implicit, or does it need to be explicit?

4.2 Example: A Manual SemAn of *harm*

1. harm IEC 61508-4 subclause 3.2.1 and IEC Guide 120 subclause 3.7 :

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

SemAn goes further than the SemAn Analyser, using domain knowledge about the concepts (words and phrases) occurring in the definition (recall that the SemAn Analyser takes these as primitive). Invoking domain knowledge results in a meaning postulate. Because the result analysis has used the meaning postulates, they are restated along with the result of the SemAn.

First is to fill this definition out by "expanding conflations", as follows.

- Expand syntactic conflation: "OR" is used to conjoin two noun phrases. The SemAn Analyser has identified two "levels" of conjoined phrase:
  - associated with *physical injury*
  - associated with *damage*

  A first step is thus to expand. The *damage* is associated with the same qualifying phrase, namely

  to the health of people OR to property OR to the environment

  There are two ways this qualifying phrase can be treated:
  - Parentheses can be used to make a unit out of this phrase:
    (to the health of people OR to property OR to the environment)
  - An auxiliary definition can be used:
    Let *P* stand for *to the health of people OR to property OR to the environment*

- The resulting phrase is:

  physical injury (to the health of people OR to property OR to the environment)
  OR
  damage (to the health of people OR to property OR to the environment)

[5] An "or" occurring in an input phrase, as here, is simply a syntactic token. The "OR" outputted as annotation by the SemAn Analyser is intended to be the logical constant OR. The SemAn Analyser at present has no mechanism for recognising syntactic tokens representing logical constants in the input and manipulating its output accordingly.

Alternatively

P(physical injury) OR P(damage)

The second alternative is obviously of no help whatever in further analysis. The first alternative is used to proceed.

- Consider next the first conjunct:

  physical injury (to the health of people OR to property OR to the environment)

  The ORs can be expanded further:

  physical injury to the health of people
  OR
  physical injury to property
  OR
  physical injury to the environment

  Semantic domain knowledge is invoked: (Meaning Postulate MP1) only people or sentient beings can be physically injured, not property or the environment. According to (MP1), then, this may be further reduced:

  physical injury to the health of people

  Using further domain knowledge, we note that physical injury to the health is redundant:

  physical injury to people

- Consider the second conjunct:

  damage (to the health of people OR to property OR to the environment)

  Again, this expands to:

  damage to the health of people
  OR
  damage to property
  OR
  damage to the environment

- Conjoining the two expanded/reduced phrases gives

  physical injury to people
  OR
  (damage to the health of people
  OR
  damage to property
  OR
  damage to the environment)

  Note that logical OR is associative: *A OR (B OR C)* is the same as *(A OR B) OR C*, and thus either may be written unambiguously without parentheses: *A OR B OR C* (Goldrei 2005). So this can be written:

  physical injury to people
  OR
  damage to the health of people
  OR
  damage to property

OR
damage to the environment

- *Physical injury* is a term which contains *injury*, and (Meaning Postulate MP2, obviously related to MP1) injury can only occur to sentient beings. The term *people* is used; (domain knowledge) *people* is a plural of *person*, as is *persons*. The question arises if *harm* can be caused to one *person*, or must it always be more than one (plural)? Singular or plural? (Meaning Postulate from domain knowledge MP3) Harm to one person is still harm. The issue could be clarified by rewriting *people* as *one or more persons*

  physical injury to one or more persons
  OR
  damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

- The first two conjoined clauses have as part *one or more persons*. Furthermore, they are semantically related: (MP4) *Physical injury* is *damage to the health* of (a person or persons). But is all *damage to the health* also *physical injury*? No, there can be damage to health that is predominantly psychiatric: post-traumatic stress syndrome for example. So (MP5) *damage to the health* includes *physical injury* but not vice versa. Put in terms of logic,

  physical injury to one or more persons
  IMPLIES
  damage to the health of one or more persons

  but not vice versa. It follows that the first clause can be omitted without semantic loss. However, an analyst might wish to retain it as a means of emphasis[6].

- Result:

  damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

  Alternatively,

  physical injury to one or more persons
  OR
  other damage to the health of one or more persons
  OR
  damage to property
  OR
  damage to the environment

[6] There are circumstances in which additional words are logically unnecessary, but help to ensure understanding, and that it is ideally part of an analyst's skillset to recognise such cases.

- Finally, these could be consolidated, by regrouping according to English conventions, for example:

  physical injury or other damage to the health of one or more persons
  OR
  damage to property or to the environment

  Alternatively,

  damage to the health of one or more persons, or to property, or to the environment

- The second definition can now be considered.

  2. harm IEC Guide 51 subclause 3.1:

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

- Comparing with the analysis of IEC 61508-4 subclause 3.2.1 above, it is clear that
  - the analysis can proceed largely as before;
  - (MP6) *damage to the health* can be considered equivalent to *injury*

- Result:

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

  Equivalently

  injury to people, or damage to property or the environment

Given that people and one or more persons are synonyms, as are injury to and damage to the health of, it follows that, under MP1 … MP6, the two definitions are synonymous. The results may be expressed as follows:

- Under meaning postulates[7]

  (MP1) only people or sentient beings can be *physically injured*, not property or the environment;

  (MP2) *injury* can only occur to sentient beings;

  (MP3) *harm* to one *person* is still *harm*;

  (MP4) *Physical injury* is *damage to the health* of (a person or persons);

  (MP5) *damage to the health* includes *physical injury* but not vice versa; and

  (MP6) *damage to the health* can be considered equivalent to *injury*,

  the two definitions are synonymous and equivalent to:
  physical injury or other damage to the health of one or more persons, or
  damage to property or to the environment
  damage to the health of one or more persons, or to property, or to the environment
  injury to people, or damage to property or the environment

- It follows that there is a harmonisation task, but one which is in this case purely syntactic: an analyst must choose between the three example definitions above (or ones

[7] Note these MPs are specific to the SemAn of "*harm*". This article does not address the appropriate formulation of MPs across multiple definitions and resolution of possible conflicts. We are not so far along.

in which synonymic phrases are used, such as *people* instead of *one or more persons* or vice versa).

This analysis is laborious, and the result relatively easily foreseeable from the start, but the purpose is to illustrate the principles and steps involved in a manual SemAn, including the formulation of MPs and this is shown more easily on such straightforward examples[8].

4.3 SemAn Example: *asset*

1. asset, IEC 62443-1-1 subclause 3.2.6 and IEC 62443-2-1 subclause 3.1.3

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

The SemAn proceeds with similar steps to that of *harm* in Sub-section 4.2. The steps are not elaborated here in as much detail. However, the SemAn itself is more complex.

- Expand: An *asset* is a *physical object OR a logical object <with additional properties>*. The adjectives here are (Meaning Postulate MP1) applicative, so an *asset* is an object. It is left unexplained exactly what a logical object is. (One might speculate that a *metaphysical object* is meant, but most engineers do not use that term.) Introduce the primitive *Ob* to denote the thing of sort Obj which is being talked about. The mathematics-type notation typical of formal logic is used: *P(Ob)* says *Ob is physical*, whereas *L(Ob)* says *Ob is logical*. For objecthood, then, the term *Ob* of sort Obj has been introduced and yields the assertion *P(Ob) OR L(Ob)*.
- Fill out *<additional properties>*: another OR syntactic conflation is expanded.

  owned by an organisation OR under the custodial duties of an organisation.

  There is another sort here, *organisation*. Whereas for *Ob*, a specific *asset* is meant, the organisation is unspecified: (MP2) *some organisation* is meant. The term *some* is a quantifier and in logic, one would be tempted to quantify: "*there is an organisation Org such that …*". But, for a given *asset*, it can be assumed that (Meaning Postulate MP3) there is just one organisation that owns it or just one organisation that has custody of it. Note that this meaning postulate is not like the ones involved in the analysis of *harm*; it involves rather an assumption about the way of the world; that if there are multiple owners or custodians, just one can be singled out to be *Org* for the purposes of the definition. So, for *Ob*, there is a single *Org* of sort *Organisation* (let us say *Orgn*) which either *Owns* it or *HasCustody* of it:

  Owns(Ob,Org) OR HasCustody(Ob,Org).

- Fill out ",": there is a list of properties here, starting with *owned by … OR under the custodial duties of …* and then *having … .* It is clear that *AND* is meant by the comma.
- Fill out further. Result: *(Ob has a perceived value to Org) OR (Ob has an actual value to Org)*. Choose primitives *PV* and *AV* for the predicates *has a perceived value to* and *has an actual value to*. The result is *PV(Ob,Org) OR AV (Ob,Org).*
- Result: it seems the analysis has arrived at the following, in formal form:

  P(Ob) OR L(Ob) AND Owns(Ob,Org) OR HasCustody(Ob,Org) AND PV(Ob,Org) OR AV (Ob,Org)

[8] There might be disputes concerning the MPs, and such disputes could be problematic in, say, courts of law. The result given here follows from the MPs given. We construe the SemAn task here as identifying the need for, and formulating, MPs. The validity of MPs so formulated may indeed be doubted, but resolution of such doubts we see as a task more appropriate for the accompanying, more philosophic-analytic, technique ConcAn (Ladkin 2022).

However, there is an AND..OR ambiguity which needs to be disambiguated. AND..OR ambiguities arise because *A AND (B OR C)* does not have the same meaning *as (A AND B) OR C* and when there are no parentheses, as in *A AND B OR C*, one cannot tell which is meant. To disambiguate, parentheses are used:

(P(Ob) OR L(Ob)) AND (Owns(Ob,Org) OR HasCustody(Ob,Org)) AND (PV(Ob,Org) OR AV (Ob,Org))

- Rewriting the result: This formula looks "formal" and is typical for the indication of the logical structure of phrases and sentences/assertions. But it is hard to read. There are some ways to make such formulas easier to read, for example the vertical stacking of clauses, as in TLA$^+$ (Lamport 2003)[9]. In the TLA$^+$ "pretty-printing" style, all clauses in a conjunction are preceded by the conjunction sign and stacked vertically, *mutatis mutandi*s for disjunction. Indentation allows the elimination of the parentheses used for disambiguation:

  && P(Ob) OR L(Ob)
  && Owns(Ob,Org) OR HasCustody(Ob,Org)
  && PV(Ob,Org) OR AV (Ob,Org)

  The OR clauses within the conjuncts can be similarly formatted if so wished (the symbol ⋁ is used to denote OR), to yield:

  && ⋁ P(Ob)
  ⋁ L(Ob)
  && ⋁ Owns(Ob,Org)
  ⋁ HasCustody(Ob,Org)
  && ⋁ PV(Ob,Org)
  ⋁ AV (Ob,Org)

  but there seems to be little point to doing so here. It is up to the analyst to decide which is most helpful. The sorts of *O*b and *Org* have been so far left implicit, but there might be circumstances in which one needs to reason with them taken into account (see below). When introduced, the formal sentence in the language of sorted logic looks like:

  && Obj(Ob)
  && Orgn(Org)
  && P(Ob) OR L(Ob)
  && Owns(Ob,Org) OR HasCustody(Ob,Org)
  && PV(Ob,Org) OR AV(Ob,Org)

Consider now the second definition of asset.

2. asset IEC 62443-3-3 subclause 3.1.1
physical or logical object having either a perceived or actual value to the IACS

- Fill it out: The first observation is that too much was done with the first definition. The predicate *physical* need not have been separated from the predicate *logical*: instead of *P(Ob) OR L(Ob)* we could have used one predicate *PorL(Ob)*. But no matter; it was done, and will be left so.
- Fill it out: again, *perceived value OR actual value*, but the subject of the valuation has changed. Now, it is not an *organisation* (a group of people) but is an engineering object, a system, namely the Industrial Automation and Control System — IACS — to

[9] TLA = Temporal Logic of Actions

which the IEC 62443 series is specifically targeted. Here, (Meaning Postulate MP3) there is no possible ambiguity as to which IACS is meant: it is the one to which this standard is currently being applied. A sort *IACS* is introduced along with a primitive *theIACS* for an object of this sort.

- Result:

  && Obj(Ob)
  && IACS(theIACS)
  && P(Ob) OR L(Ob)
  && PV(Ob,theIACS) OR AV(Ob,theIACS)

There are now two analysed definitions of *asset*, which are not identical. The term *asset* is thus a homonym. The task of harmonisation is to select one of these as the primary definition. There are most often two ways in which this may be done. First, definitions may be specialised to domains of application, as illustrated in Sub-section 3.3. So, for example, *signal* means one thing in railway control, and another thing in wire-transmitted telecommunications, leading to two definitions, one for *signal (railways)* and a different one for *signal (telecommunications)*. The specialisations in electrotechnical terminology usually follow the designations of the IEC Technical Committees (TC 9 is Electrical equipment and systems for railways); there are many Technical Committees which could (and do) use a telecommunications notion (in fact, signal has many definitions; see Sub-section 3.3). The second way is by reconciling the two different definitions into one. Considerations towards the second path are illustrated here.

- Much of both definitions is the same, but some of it is definitively different. The IACS in question is uniquely determined: it is whichever system the IEC 62443 series of standard is applied to in the instance of its application. The organisation involved (according to the first definition) might also be unique, but it could be that many organisations are involved in the joint ownership or custodianship of an asset. Is an IACS, as a nonsentient physical object, an object of which it might make any sense at all to speak of as having values? Or is the valuer an implicit organisation which is considering *Ob* and *theIACS* together, to determine whether there is a perceived or actual "value" (causal influence?) of the one on the other? Say, *PV(Ob,theIACS,Org) OR AV(Ob,theIACS,Org)*. The SemAn analyst cannot decide such matters; the domain specialists writing the standard must do so.

4.4 Output of SemAn Analyser on *asset*

There are two non-identical definitions of asset in the IEC 62443 series of standards. Here is the output of the SemAn Analyser on both:

```
10.
asset:

physical or logical object owned by or under the custodial duties of
an organization, having either a perceived or actual value to the
organization

\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
```

```
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]

11.
asset:

physical or logical object having either a perceived or actual value
to the IACS

\\
     physical or logical object
          > having either a perceived or actual value
                > to the IACS
[Source: IEC 62443-3-3:2013]
```

This annotated parsing/pretty-printing shows immediately and clearly the similarities and differences immediately which we have recognised in the more laborious manual SemAn. Namely, first, an *asset* is a *physical or logical object*; and, second, this object *[has] a perceived or actual value*. To whom the value accrues is clearly different in the two cases. Further, one definition mentions custodial duties associated with the asset; the other does not. This comparison gives clear indications of the differences seen during the manual SemAn, and leads to the same scope of discussion for domain experts attempting to harmonise the two definitions as did the manual analysis.

5 Conclusions

We have argued, briefly, that getting electrotechnical terminology "right" is an important task, for many reasons (not least, that using it properly may help keep some innocent people out of jail!). Logical annotation seems to us to be a helpful method of doing so, and we have explicated here a method of logical analysis, SemAn, and an annotator, the SemAn Analyser, which annotates according to SemAn but without (as yet) using Meaning Postulates.

We have endeavoured to show by example that such analyses are useful in identifying similarities and distinctions in definitions which are ripe for clarification. Meaning Postulates can help, but skill is involved in the formulation of the Meaning Postulates and we don't see at present how this process may be automated.

Experience has shown that use of the SemAn Analyser eases the task of performing a SemAn, as it clearly did in the case of *asse*t in Sub-sections 4.3 and 4.4. In the case of *harm*, Sub-section 4.2 showed that there were many Meaning Postulates that played a role in eliminating/reducing some of the terms occurring in the definition, which the SemAn Analyser treats as primitive. So here the manual SemAn achieved results which the SemAn Analyser could not obtain. (Also, we observed in Sub-section 3.3 that the current implementation of the SemAn Analyser does not quite do all we wish it to do.) Third parties involved in terminology work have indicated to us that they find it helpful.

Correspondence Address

The Corresponding Author is Peter Bernard Ladkin, Causalis Ing.-GmbH, Bielefeld, Germany; e-mail: Ladkin@causalis.com.

Acknowledgments

The SemAn method was developed by the first author in the project Harbsafe, financed by (as it then was) the German Federal Ministry for Economic Affairs and Energy, No. 03TNG006A-B in the Wipano programme, awarded to the Technical University of Braunschweig (TU-BS), Institut IVA, and DKE (the Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE), which is a German electrotechnical standardisation organisation, in 2017—2019.

The SemAn Analyser was developed by Causalis Ingenieurgesellschaft mbH as subcontractor to TU-BS, Institut IVA (then to become Institut IITL) in the project Harbsafe II, Nos. 03TN0018A-C, granted to TU-BS, DKE and INOSOFT AG, financed by the German Federal Ministry for Economic Affairs and Climate Action, in 2020—2022, also in the Wipano programme.

References

Begriffschrift. (2023). In *Wikipedia*. https://en.wikipedia.org/wiki/Begriffsschrift. Accessed 13th January 2023.

ExplosionAI. (n.d.). spaCy DependencyParser. https://spacy.io/api/dependencyparser. Accessed 13th January 2023.

Frege G. (1879). *Begriffsschrift: eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. Halle an der Saale: Verlag von Louis Nebert.

Goldrei D. (2005). *Proposition and Predicate Calculus: A Model of Argument*. Springer-Verlag, London.

IEC. (2023). *Standards Management Board – Joint Task Force on the Concept of Risk and Associated Terms*. International Electrotechnical Commission. Overview available from https://www.iec.ch/dyn/www/f?p=103:85:702664603091386::::FSP_ORG_ID,FSP_LANG_ID:28611,25. Accessed 13th January 2023.

IEC 61508-4:2010. *Functional Safety of Electrical/electronic/programmable electronic Safety-related Systems– Part 4: Definitions and abbreviations*. IEC 61508-4, Edition 2. International Electrotechnical Commission. Geneva. 2010.

IEC TS 62443-1-1:2009. *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. IEC TS 62443-1-1, Edition 1. International Electrotechnical Commission. Geneva. 2009.

IEC 62443-2-1:2010. *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*. IEC 62443-2-1, Edition 1. International Electrotechnical Commission. Geneva. 2010

IEC 62443-2-4:2015+AMD1:2017. *Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*. IEC 62443-2-4, Edition 1.1. International Electrotechnical Commission. Geneva. 2017.

IEC 62443-3-1:2009. *Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*. IEC 62443-3-1, Edition 1. International Electrotechnical Commission. Geneva. 2009.

IEC 62443-3-2:2020. *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*. IEC 62443-3-2, Edition 1. International Electrotechnical Commission. Geneva. 2020.

IEC 62443-3-3:2013. *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*. IEC 62443-3-3, Edition 1.0. International Electrotechnical Commission. Geneva. 2013.

IEC TR 63069:2019. *Industrial-process measurement, control and automation - Framework for functional safety and security*. IEC TR 63069, Edition 1. International Electrotechnical Commission. Geneva. 2019.

IEC Guide 120. *Security aspects - Guidelines for their inclusion in publications*. IEC Guide 120, Edition 1. International Electrotechnical Commission. Geneva. 2018

ISO/IEC Guide 51. *Safety aspects – Guidelines for their inclusion in standards*. ISO/IEC Guide 51, Edition 3. International Organization for Standardization and International Electrotechnical Commission. Geneva. 2014.

Janssen T. M. V. (2011). *Montague Semantics*. In Stanford Encyclopedia of Philosophy. 2011, revised 2021. Available from https://plato.stanford.edu/entries/montague-semantics/. Accessed 13th January 2023.

Jurafsky D, and Martin J. H. (2023). *Speech and Natural Language Processing, Chapter 14: Dependency Parsing*. Preprint draft of January 7, 2023. Available from https://web.stanford.edu/~jurafsky/slp3/14.pdf. Accessed 13th January 2023.

Ladkin P. B. (2020). *Robustness of Software*. In Digital Evidence and Electronic Signature Law Review, Vol. 17. Available from https://journals.sas.ac.uk/deeslr/article/view/5171. Accessed 13th January 2023.

Ladkin P. B. (2022). *Some Principles of Conceptual Analysis for Electrotechnical Terminology (ConcAn)*. Submitted for publication, 2022. {**Editor's Note:** It is hoped that this paper can be published in Volume 2, Issue 2, of this Journal}

Lamport L. (2003). *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*. Addison-Wesley

Kratzer A. (2007). *Situations in Natural Language Semantics*. In Stanford Encyclopedia of Philosophy. 2007, revised 2021. Available from https://plato.stanford.edu/entries/situations-semantics/. Accessed 13th January 2023.

Kripke S. A. (1982). *Wittgenstein on Rules and Private Language: An Elementary Exposition*. Wiley Blackwell

Mason S. (2015). *Case Transcript: England & Wales - Regina v Seema Misra, T20090070 - Commentary and Index to the transcript by Stephen Mason*. In Digital Evidence and Electronic Signature Law Review, Vol. 12. Available from https://journals.sas.ac.uk/deeslr/issue/view/328. . Accessed 13th January 2023.

Moltmann F. (2022). *Natural Language Ontology*. In Stanford Encyclopedia of Philosophy. Available from https://plato.stanford.edu/entries/natural-language-ontology/. Accessed 13th January 2023.

Montague R. (1974). *Formal Philosophy: Selected Papers of Richard Montague* (Ed. H. Richmond H. Thomason). Yale University Press 1974.

Safety-Critical Systems Club. (2023). *SCSC — Group: Ontology Working Group*. https://scsc.uk/go. Accessed 13th January 2023.

Wittgenstein L. (1967). *Philosophical Investigations* (G. E. M. Anscombe, Trans.). Basil Blackwell, Third Edition. (Original work written 1953).

This collation page left blank intentionally.

Appendix A. Multiply-Defined Concepts: Diff. Notes

A.1 Introduction

This document presents a list of concepts in the IEC functional safety and cybersecurity standards listed in the main body of the paper. Amongst the 450+ concepts defined in those documents; these are the concepts which have multiple definitions.

The list of multiply-defined concepts was developed in 2018 in Project Harbsafe (see the Acknowledgments section above), and has been reformatted for this paper.

A.2 Summary

Identical definitions	22
Minor difference (including syntactic)	11
Moderate difference	7
Substantial difference	21
Unknown (one is reference)	2
Total	63

Notes to Summary

- where there are different classes of difference within the definitions of one term, the highest difference category is assigned to the term
- "*availability*" occurs in two syntactic variants, counted here as one
- "*authenticate/authentication*" occurs as verb and noun, counted as one
- "*configuration baseline*" only occurs once — an error in the MultDefConcepts list
- there are five different versions of "*integrity*", counted as one
- "*non-repudiation*" is spelled multiple ways, counted as one
- "*risk tolerance*" and "*risk tolerance level*" are counted as one…

A.3 List of Multiply-defined Concepts

Table 1 ~ List of Multiply-defined Concepts

Concept	Sources	Remarks
access control	IEC 62443-1-1 IEC 62443-3-1	minor difference labelled enumeration (-3-1), or not

Concept	Sources	Remarks
accountability	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1	identical
application	IEC 61508-4 IEC 62443-1-1	substantial difference IEC 61508-4: referring to system: EUC IEC 62443-1-1: specialist meaning for SW
asset	IEC 62443-1-1 IEC 62443-2-1 IEC 62443-3-3	Identical includes ownership/custody and subject (organisation) moderate difference no ownership; subject IACS
asset owner	IEC 62443-2-4+AMD IEC 62443-3-3	moderate difference IEC 62443-2-4+AMD: subject: organization IEC 62443-3-3: subject: company
attack	IEC 62443-1-1 IEC Guide 120 IEC 62443-3-3	identical definition + paraphrase (in “i.e.” clause) minor difference definition only, no paraphrase
authenticate	IEC 62443-1-1	difference from noun verb: concrete action: verify
authentication	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1 IEC 62443-3-3	identical noun: measure designed to verify (different objects) substantial difference noun: abstractly formulated action: assurance
authorization	IEC Guide 120 IEC 62443-1-1 IEC 62443-3-1	identical
availability availability (performance)	IEC Guide 120 IEC62443-3-3 IEC 62443-3-1 IEC 62443-1-1	moderate difference no subject of property substantial difference probability, circumscribed in time, qualified substantial difference that of which the probability (above) is assessed

Concept	Sources	Remarks
channel	IEC 61508-4 IEC 62443-1-1	substantial difference IEC 61508-4: independent implementation of safety function IEC 62443-1-1: link in a conduit
ciphertext	IEC 62443-1-1 IEC 62443-3-1	minor (syntactic) difference
client	IEC 62443-1-1 IEC 62443-3-1	identical
conduit	IEC 62443-1-1 IEC 62443-3-3	moderate difference IEC 62443-1-1: for channels, common secreqs IEC 62443-3-3: for assets, protection
confidentiality	IEC 62443-1-1 IEC 62443-3-1 IEC Guide 120 IEC 62443-3-3	identical moderate difference essentially semantically equivalent, negative formulation substantial difference positive formulation as restrictions
configuration baseline	IEC 61508-4	only defined once
consequence	IEC 62443-2-1 IEC 62443-3-3	substantial difference IEC 62443-2-1: abstract, subject “incident” IEC 62443-3-3: condition or state, subject “event”
control system	IEC 62443-2-4+AMD IEC 62443-3-3	substantial difference IEC 62443-2-4+AMD: also that “used in design” IEC 62443-3-3: HW & SW of an IACS
countermeasure	IEC 62443-1-1 IEC 62443-3-3	identical
decryption	IEC 62443-1-1 IEC 62443-3-1	identical
defence in depth	IEC 62443-1-1 IEC 62443-3-1	substantial difference IEC 62443-1-1: usual: layers IEC 62443-3-1: architecture, abstract

Concept	Sources	Remarks
demilitarized zone	IEC 62443-1-1 IEC 62443-3-3	substantial difference IEC 62443-1-1: usual internal vs. external IEC 62433-3-3: generalised: between zones (ambiguity “zone”)
denial of service	IEC 62443-1-1 IEC 62443-3-1	identical
digital signature	IEC 62443-1-1 IEC 62443-3-1	identical
encryption	IEC 62443-1-1 IEC 62443-3-1	identical
environment	IEC 61508-4 IEC 62443-3-3	substantial difference IEC 61508-4: abstract: parameters IEC 62443-3-3: surrounding entities & circumstances
equipment under control	IEC 61508-4 IEC 62443-1-1	identical
harm	IEC Guide 120 ISO/IEC Guide 51 IEC 61508-4	identical minor difference
hazard	IEC 61508-4 ISO/IEC Guide 51	identical
hazardous event	IEC 61508-4 ISO/IEC Guide 51	minor difference semantically equivalent
hazardous situation	IEC 61508-4 ISO/IEC Guide 51	identical
incident	IEC 62443-2-1 IEC 62443-3-3	minor difference punctuation
industrial automation and control system	IEC 62443-1-1 IEC 62443-2-4+AMD IEC 62443-3-3	moderate differences all collections … that … IEC62443-1-1: of personnel, HW, SW IEC 62443-3-3: of personnel, HW, SW, policies IEC 62443-2-4+AMD: of personnel, HW, SW, policies, procedures

Concept	Sources	Remarks
integrity	IEC 62443-1-1 IEC 62443-3-1	identical
	IEC 62443-3-3 IEC Guide 120	moderate differences (changed to substantial) various concepts of “integrity” dealt with elsewhere
– software safety integrity	IEC 61508-4	substantial differences
– software safety integrity level	IEC 61508-4	substantial differences
– safety integrity	IEC 61508-4	substantial differences
– safety integrity level	IEC 61508-4 IEC 62443-1-1	moderate differences, also different from above
interception	IEC 62443-1-1 IEC 62443-3-1	minor difference IEC 62443-1-1: synonym also given — otherwise identical
interface	IEC 62443-1-1 IEC 62443-3-1	identical
local area network	IEC 62443-1-1 IEC 62443-3-1	identical
non-repudiation	IEC 62443-3-3 IEC Guide 120	identical
	IEC 62443-1-1 IEC 62443-3-1	identical, but substantially different from above heterographs IEC 62443-3-3/Guide 120: positive formulation: prove IEC 62443-1-1/3-1: service providing protection against...
plaintext	IEC 62443-1-1 IEC 62443-3-1	identical
product supplier	IEC 62443-2-4+AMD IEC 62443-3-3	identical
reasonably foreseeable misuse	IEC 61508-4 ISO/IEC Guide 51	identical

Concept	Sources	Remarks
remote access	IEC 62443-1-1 IEC 62443-2-1 IEC 62443-2-4+AMD IEC 62443-3-3	substantial differences IEC 62443-1-1: zone + “different geog. location” + rights IEC 62443-2-1: “perimeter” rather than “zone” IEC 62443-2-4+AMD: access through external interface (usual) IEC 62443-3-3: zone + “perimeter”
repudiation	IEC 62443-1-1 IEC 62443-3-1	identical
residual risk	IEC 61508-4 ISO/IEC /Guide 51 IEC 62443-1-1	minor differences IEC 61508-4: “protective measures” Guide 51: “risk reduction measures (protective measures)” IEC 62443-1-1: “security controls or countermeasures: specific to sec. risk
risk	IEC 61508-4 ISO/IEC Guide 51 IEC Guide 120 IEC 62443-1-1/3-1	identical identical, but substantial difference from above IEC 61508-4, etc.: combination of probability with severity IEC 62443-1-1, etc: expectation of loss, restricted to “vulnerability”
risk assessment	ISO/IEC Guide 51 IEC 62443-1-1 IEC 62443-2-1	substantial differences IEC Guide 51: risk analysis + risk evaluation IEC 62443-1-1: description of process, restricted to “vulnerabilities” IEC 62443-2-1: description of process, no restriction
risk tolerance /level	IEC 62443-1-1 IEC 62443-2-1	substantial difference (change 2018-12-27: minor difference) IEC 62443-1-1: term “level”, else semantically equivalent

Concept	Sources	Remarks
safety	IEC 61508-4 IEC 62443-1-1 ISO/IEC Guide 51 IEC Guide 120	identical identical but minor difference from above semantically equivalent if "unacceptable" = "not tolerable
safety instrumented system	IEC 62443-2-4+AMD IEC 62443-3-3	substantial difference IEC 62443-2-4+AMD: system used to implement FS IEC 62443-3-3: system used to implement SFs
security	IEC Guide 120 IEC 62443-1-1	substantial difference IEC Guide 120: protection ensuring inviolability IEC 62443-1-1: enumerated listing of features
security incident	IEC 62443-1-1 IEC 62443-2-4+AMD	substantial difference IEC 62443-1-1: "adverse" event or a threat of occurrence IEC 62443-2-4+AMD: compromise or attempt of significance to asset owner
security level	IEC 62443-1-1 IEC 62443-3-3	substantial difference IEC 62443-1-1: required effectiveness of countermeasures and properties IEC 62443-3-3: measure of confidence of vulnerability-freeness
security program	IEC 62443-1-1 IEC 62443-2-4+AMD	substantial difference IEC 62443-1-1: combination of all aspects of secmanagement IEC 62443-2-4+AMD: portfolio of secservices applicable to IACS
security services	IEC 62443-1-1 IEC 62443-3-1 IEC Guide 120	identical
server	IEC 62443-1-1 IEC 62443-3-1	identical
service provider	IEC 62443-2-4+AMD IEC 62443-3-3	moderate difference IEC 62443-2-4+AMD: organisation that has agreed to provide service IEC 62443-3-3: individual or organisation providing support

Concept	Sources	Remarks
sniffing	IEC 62443-1-1 IEC 62443-3-1	minor difference IEC 62443-1-1: a reference to another entry
spoof	IEC 62443-1-1 IEC 62443-3-1	identical
system	IEC 62443-1-1 IEC 62443-2-4+AMD	identical
system software	IEC 62443-1-1 IEC 62443-3-1 IEC 61508-4	Identical SW to facilitate ops and maintenance moderate difference from above SW relates to functioning of device itself or its services
threat	IEC 62443-1-1 IEC Guide 120 IEC 62443-3-1 IEC 62443-3-3	identical potential for violation of security moderate difference, also to above IEC 62443-3-1: potentially damaging action or capability IEC 62443-3-3: potentially circumstance/event adversely affecting operations
tolerable risk	IEC 61508-4 ISO/IEC Guide 51	minor difference IEC Guide 51: “level of ...”
vulnerability	IEC 62443-1-1 IEC 62443-2-4+AMD IEC 62443-3-1 IEC Guide 120	identical
wide area network	IEC 62443-1-1 IEC 62443-3-1	minor differences IEC 62443-1-1: “to connect computers, networks or other devices...” IEC 62443-3-1: “to connect computers...”
zone	IEC 62443-1-1 IEC 62443-3-3	minor difference? IEC 62443-1-1: a reference to another subclause

Appendix B. SemAn Analyser Output on Multiply-Defined Concepts

B.1 Introduction

The SemAn Analyser results below were developed in 2021-2 by TU-BS and Causalis Ing.-GmbH in Project Harbsafe II (see the Acknowledgments section above).

B.2 SemAn Analyser Results

```
1. (no definition)

2.
access control(a):

a) protection of system resources against unauthorized access

\\
     a) protection
          > of system resources
                 > against unauthorized access
[Source: IEC TR 62443-3-1:2009]

3.
access control(b):

b) process by which use of system resources is regulated according to a security
policy and is permitted only by authorized entities according to that policy

\\
     b) process
          > by which use
                 > of system resources
                 > [AND] is regulated according to a security policy
                 > [AND] and is permitted only by authorized entities
                           > according to that policy
[Source: IEC TR 62443-3-1:2009]

4.
access control:

protection of system resources against unauthorized access;

a process by which use of system resources is regulated according to a security
policy and is permitted by only authorized entities according to that policy

\\
     protection
          > of system resources
                > against unauthorized access
     ;

     a process
          > by which use
                 > of system resources
```

```
                > [AND] is regulated according to a security policy
                > [AND] and is permitted only by authorized entities
                                    > according to that policy
[Source: IEC TS 62443-1-1:2009]

5.
accountability:

property of a system that ensures that the actions of a system entity may be
traced uniquely to that entity, which can be held responsible for its actions

\\
     property
          > [AND] of a system
          > [AND] that ensures that the actions
                       > [AND] of a system entity
                       > [AND] may be traced uniquely to that entity
                                    > , which can be held responsible for its
actions
[Source: IEC Draft Guide 120]
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

8.
application:

task related to the EUC rather than to the E/E/PE system

\\
     task
          > [AND] related to the EUC
          > [AND] rather than to the E/E/PE system
[Source: IEC 61508-4:2010]

9.
application:

software program that performs specific functions initiated by a user command or
a process event and that can be executed without access to system control,
monitoring, or administrative privileges

\\
      software program
          > [AND] that performs specific functions
                       > initiated by a |[OR] user command
                                       |[OR] or a process event

          > [AND] and that can be executed without access
                       > to | [OR] system control
                            | [OR] , monitoring
                            | [OR] , or administrative privileges
[Source: IEC TS 62443-1-1:2009]

10.
asset:

physical or logical object owned by or under the custodial duties of an
organization, having either a perceived or actual value to the organization

\\
     physical or logical object
          > [AND] owned by or under the custodial duties
                       > of an organization
          > [AND] , having either a perceived or actual value
                       > to the organization
[Source: IEC 62443-2-1:2010]
[Source: IEC TS 62443-1-1:2009]
```

```
11.
asset:

physical or logical object having either a perceived or actual value to the IACS

\\
     physical or logical object
          > having either a perceived or actual value
                > to the IACS
[Source: IEC 62443-3-3:2013]

13.
asset owner:

individual or company responsible for one or more IACS

\\
     [OR] individual
     [OR] or company
               > responsible for
                     > one or more IACS
[Source: IEC 62443-3-3:2013]

14.
asset owner:

individual or organization responsible for one or more IACSs

\\
     [OR] individual
     [OR] or organization
               > responsible for
                     > one or more IACS
[Source: IEC 62443-2-4:2015+AMD1:2017]

15.
attack:

assault on a system that derives from an intelligent threat

\\
     assault
          > [AND] on a system
          > [AND] that derives from an intelligent threat
[Source: IEC 62443-3-3:2013]

16.
attack:

assault on a system that derives from an intelligent threat – i.e., an
intelligent act that is a deliberate attempt (especially in the sense of a method
or technique) to evade security services and violate the security policy of a
system

\\
     assault
          > [AND] on a system
          > [AND] that derives from an intelligent threat
     – i.e.
     , an intelligent act
          > that is a deliberate attempt
                > [AND] to evade security services
                > [AND] and violate the security policy
                           > of a system
[Source: IEC Draft Guide 120]
[Source: IEC TS 62443-1-1:2009]
```

```
18.
Authenticate

verify the identity of a user, user device, or other entity, or the integrity of
data stored, transmitted, or otherwise exposed to unauthorized modification in an
information system, or to establish the validity of a transmission

\\
     [OR] verify the identity
               > of | [OR] a user
                    | [OR] , user device
                    | [OR] , or other entity
     [OR] , or the integrity
               > of data
                     > stored, transmitted, or otherwise exposed to unauthorized
modification
                               > in an information system
     [OR] , or to establish the validity
               > of a transmission
[Source: IEC TS 62443-1-1:2009]

19.
authentication:

security measure designed to establish the validity of a transmission, message or
originator or a means of verifying an individual’s authorization to receive
specific categories of information

\\
     security measure
          > designed to establish the | [OR] validity
                                      |           > of a | [OR] transmission
                                      |                  | [OR] , message
                                      |                  | [OR] , or originator
                                      | [OR] or a means
                                      |           > of verifying an individual’s
authorization
                                      |                  > to receive specific
categories
                                      |                        > of information
[Source: IEC 62443-2-1:2010]

20.
authentication:

provision of assurance that a claimed characteristic of an identity is correct

\\
     provision
          > of assurance
                 > that a claimed characteristic
                        > [AND] of an identity
                        > [AND] is correct

[Source: IEC 62443-3-3:2013]

21.
authentication:

security measure designed to establish the validity of a transmission, message,
or originator, or a means of verifying an individual's authorization to receive
specific categories of information

\\
     security measure
          > designed to establish the | [OR] validity
                                      |           > of a | [OR] transmission
                                      |                  | [OR] , message
```

```
                                        |                  | [OR] , or originator
                                        | [OR] , or a means
                                        |           > of verifying an individuals
authorization
                                        |                  > to receive specific
categories
                                        |                        > of information
[Source: IEC Draft Guide 120]
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

24.
authorization:

right or permission that is granted to a system entity to access a system
resource

\\
      [OR] right
      [OR] or permission
                > [AND] that is granted to a system entity
                > [AND] to access a system resource
[Source: IEC Draft Guide 120]
[Source: IEC TS 62443-1-1:2009]

25.
authorization:

right or a permission that is granted to a system entity to access a system
resource

\\
      [OR] right
      [OR] or a permission
                > [AND] that is granted to a system entity
                > [AND] to access a system resource
[Source: IEC TR 62443-3-1:2009]

27.
availability:

property of ensuring timely and reliable access to and use of control system
information and functionality

\\
     property
          > of ensuring timely and reliable | [AND] access to
                                            | [AND] and use
                                            |            > of control system |
[AND] information
                                            |                               |
[AND] and functionality
[Source: IEC 62443-3-3:2013]

28.
availability:

property of being accessible and usable upon demand by an authorized entity

\\
     property
          > of being accessible and usable upon demand
                 > by an authorized entity
[Source: IEC Draft Guide 120]

29.
availability:
```

```
probability that an asset, under the combined influence of its reliability,
maintainability and security will be able to fulfil its required function over a
stated period of time or at a given point in time

\\
     probability
          > that an asset
                 > [AND] , under the combined influence
                             > of its | [AND] reliability
                                      | [AND] , maintainability
                                      | [AND] and security
                 > [AND] will be able to fulfil its required function
                             > [OR] over a stated period
                                         > of time
                             > [OR] or at a given point
                                         > in time
[Source: IEC TR 62443-3-1:2009]

30.
availability:

ability of an item to be in a state to perform a required function under given
conditions at a given instant or over a given time interval, assuming that the
required external resources are provided

\\
     ability
          > [AND] of an item
                        > to be in a state
          > [AND] to perform a required function
                        > under given conditions
                               > [OR] at a given instant
                               > [OR] or over a given time interval
                               > [AND] , assuming that the required external
resources
                                                  > are provided
[Source: IEC TS 62443-1-1:2009]

31.
channel:

element or group of elements that independently implement an element safety
function

\\
     [OR] element
     [OR] or group
               > [AND] of elements
               > [AND] that independently implement
                           > an element safety function
[Source: IEC 61508-4:2010]

32.
channel:

specific communication link established within a communication conduit

\\
     specific communication link
          > established within a communication conduit
[Source: IEC TS 62443-1-1:2009]

33.
ciphertext:

data that have been transformed by encryption so that the semantic information
content is no longer intelligible or directly available
\\
```

```
     data
          > that have been transformed by encryption
                 > so that the semantic information content
                        > [OR] is no longer intelligible
                        > [OR] or directly available
[Source: IEC TR 62443-3-1:2009]

34.

ciphertext:

data that has been transformed by encryption so that its semantic information
content (i.e., its meaning) is no longer intelligible or directly available

\\
     data
          > that has been transformed by encryption
                 > so that the semantic information content
                        > [OR] is no longer intelligible
                        > [OR] or directly available

[Source: IEC TS 62443-1-1:2009]

35.
client:

device or application receiving or requesting services or information from a
server application

\\
     [OR] device
     [OR] or application
               > [OR] receiving or requesting services
               > [OR] or information
                           > from a server application
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

37.
conduit:

logical grouping of communication channels, connecting two or more zones, that
share common security requirements

\\
     logical grouping
          > of communication channels
                 > , connecting | [OR] two
                                | [OR] or more zones
                                |           > , that share common security
requirements
[Source: IEC 62443-3-3:2013]

38.
conduit:

logical grouping of communication assets that protects the security of the
channels it contains

\\
     logical grouping
          > [AND] of communication assets
          > [AND] that protects the security
                        > of the channels
                              > it contains
[Source: IEC TS 62443-1-1:2009]
```

```
39.
confidentiality:

preserving authorized restrictions on information access and disclosure,
including means for protecting personal privacy and proprietary information

\\
     preserving authorized restrictions
          > on | [AND] information access
               | [AND] and disclosure
               |            > , including means
               |                  > for protecting | [AND] personal privacy
               |                                  | [AND] and proprietary
information
[Source: IEC 62443-3-3:2013]

40.
confidentiality:

property that information is not made available or disclosed to unauthorized
individuals, entities, or processes

\\
     property
          > [AND] that information
          > [AND] is not | [OR] made available
                         | [OR] or disclosed to unauthorized | [OR] individuals
                         |                                   | [OR] , entities
                         |                                   | [OR] , or
processes
[Source: IEC Draft Guide 120]

41.
confidentiality:

assurance that information is not disclosed to unauthorized individuals,
processes or devices
\\
     assurance
          > that information
                 > is not disclosed to unauthorized | [OR] individuals
                                                    | [OR] , processes
                                                    | [OR] or devices
[Source: IEC TR 62443-3-1:2009]

42.
confidentiality:

assurance that information is not disclosed to unauthorized individuals,
processes or devices
\\
     assurance
          > that information
                 > is not disclosed to unauthorized | [OR] individuals
                                                    | [OR] , processes
                                                    | [OR] ,or devices
[Source: IEC TS 62443-1-1:2009]

43.

configuration baseline:

information that allows the software release to be recreated in an auditable and
systematic way, including: all source code, data, run time files, documentation,
configuration files, and installation scripts that comprise a software release;

information about compilers, operating systems, and development tools used to
create the software release
```

```
\\
     information
          > that allows the software release
                 > [AND] to be recreated in an auditable and systematic way
                 > [AND] , including: all | [AND] source code
                                          | [AND] data
                                          | [AND] run time files
                                          | [AND] , documentation
                                          | [AND] , configuration files
                                          | [AND] , and installation scripts
                                          |           > that comprise a software
release
; information about compilers
     > [AND], operating systems
     > [AND], and development tools
                    > used to create the software release
[Source: IEC 61508-4:2010]

44.
consequence:

result that occurs from a particular incident

\\
     result
          > that occurs from a particular incident
[Source: IEC 62443-2-1:2010]

45.
consequence:

condition or state that logically or naturally follows from an event

\\
     [OR] condition
     [OR] or state
               > that logically or naturally follows from an event
[Source: IEC 62443-3-3:2013]

46.
control system:

hardware and software components of an IACS

\\
     hardware and software components
          > of an IACS
[Source: IEC 62443-3-3:2013]

47.
control system:

hardware and software components used in the design and implementation of an IACS

\\
     hardware and software components
          > used in the | [AND] design
                        | [AND] and implementation
                        |            > of an IACS
[Source: IEC 62443-2-4:2015 + AMD1:2017]

48.
countermeasure:

action, device, procedure, or technique that reduces a threat, a vulnerability,
or an attack by eliminating or preventing it, by minimizing the harm it can
cause, or by discovering and reporting it so that corrective action can be taken
```

```
\\
     [OR] action
     [OR] , device
     [OR] , procedure
     [OR] , or technique
               > [AND] that reduces | [OR] a threat
                                    | [OR] , a vulnerability
                                    | [OR] , or an attack
                                > [OR] by eliminating
                                > [OR] or preventing it
                                > [OR] , by minimizing the harm
                                                > it can cause,
                                > [OR] or by | [AND] discovering
                                             | [AND] and reporting it
               > [AND] so that corrective action
                                > can be taken
[Source: IEC 62443-3-3:2013]
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TS 62443-1-1:2009]
```

```
51.
decryption:

process of changing ciphertext into plaintext using a cryptographic algorithm and
key (see 3.1.24 “encryption”)

\\
     process
          > of changing ciphertext
                 > [AND] into plaintext
                 > [AND] using a | [AND] cryptographic algorithm
                                 | [AND] and key
[Source: IEC TR 62443-3-1:2009]
```

```
52.
decryption:

process of changing cipher text into plaintext using a cryptographic algorithm
and key

\\
     process
          > of changing cipher text
                 > [AND] into plaintext
                 > [AND] using a | [AND] cryptographic algorithm
                                 | [AND] and key
[Source: IEC TS 62443-1-1:2009]
```

```
53.
defense in depth:

security architecture based on the idea that any one point of protection may, and
probably will, be defeated

\\
     security architecture
          > based on the idea
                 > that any one point
                        > of protection
                              > may, and probably will, be defeated
[Source: IEC TR 62443-3-1:2009]
```

```
54.
defense in depth:

provision of multiple security protections, especially in layers, with the intent
to delay if not prevent an attack

\\
     provision
          > [AND] of multiple security protections
                    > ,especially in layers
          > [AND] , with the intent
                              > to delay if not prevent an attack
[Source: IEC TS 62443-1-1:2009]

55.
demilitarized zone:

common, limited network of servers joining two or more zones for the purpose of
controlling data flow between zones

\\
     common, limited network
          > [AND] of servers
          > [AND] joining two or more zones
                       > for the purpose
                              > of controlling data flow
                                     > between zones
[Source: IEC 62443-3-3:2013]

56.
demilitarized zone:

perimeter network segment that is logically inserted between internal and
external networks

\\
     perimeter network segment
          > that is logically inserted
                 > between | [AND] internal
                           | [AND] and external networks
[Source: IEC TS 62443-1-1:2009]

57.
denial of service:

prevention or interruption of authorized access to a system resource or the
delaying of system operations and functions

\\
     [OR] prevention
     [OR] or interruption
               > of authorized access
                      > to a system resource
     [OR] or the delaying
               > of system | [AND] operations
                           | [AND] and functions
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TR 62443-3-1:2009]

59.
digital signature:

result of a cryptographic transformation of data which, when properly
implemented, provides the services of origin authentication, data integrity, and
signer non-repudiation

\\
     result
```

```
          > of a cryptographic transformation
                > [AND] of data
                > [AND] which, when properly implemented, provides the services
                              > of | [AND] origin authentication
                                   | [AND] , data integrity
                                   | [AND] and signer non-repudiation
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

61.
encryption:

cryptographic transformation of plaintext into ciphertext that conceals the
data’s original meaning to prevent it from being known or used

\\
     cryptographic transformation
          > [AND] of plaintext
          > [AND] into ciphertext
          > [AND] that conceals the data’s original meaning
                        > to prevent it
                              > from being known or used
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

63.
environment:

all relevant parameters that can affect the achievement of functional safety in
the specific application under consideration and in any safety lifecycle phase

\\
     all relevant parameters
          > that can affect the achievement
                > of functional safety
                      > in the specific | [AND] application
                                        |            > under consideration
                                        | [AND] and in any safety lifecycle
phase
[Source: IEC 61508-4:2010]

64.
environment:

surrounding objects, region or circumstances which may influence the behavior of
the IACS and/or may be influenced by the IACS

\\
     surrounding | [OR] objects
                 | [OR] , region
                 | [OR] or circumstances
          > [OR] which may influence the behavior
                     > of the IACS
          > [OR] and/or may be influenced by the IACS
[Source: IEC 62443-3-3:2013]

65.
equipment under control:

equipment, machinery, apparatus or plant used for manufacturing, process,
transportation, medical or other activities

\\
     [OR] equipment
     [OR] , machinery
     [OR] , apparatus
     [OR] or plant
               > used for | [OR] manufacturing
```

```
                          | [OR] , process
                          | [OR] , transportation
                          | [OR] , medical or other activities
[Source: IEC TS 62443-1-1:2009]
[Source: IEC 61508-4:2010]

67.
harm:

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

\\
     [OR] physical injury
     [OR] or damage
               > [OR] to the health
                           > of people
     [OR] or damage
               > [OR] to property
               > [OR] or the environment
[Source: IEC 61508-4:2010]

68.
harm:

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

\\
     [OR] injury
     [OR] or damage
               > to the health
                      > of people
     [OR] , or damage
               > to | [OR] property
                    | [OR] or the environment
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]



70.
hazard:

potential source of harm

\\
     potential source
          > of harm
[Source: IEC 61508-4:2010]
[Source: IEC Guide 51:2014]

72.
hazardous event:

event that may result in harm

\\
     event
          > that may result in harm
[Source: IEC 61508-4:2010]

73.
hazardous event

event that can cause harm

\\
```

```
     event
          > that can cause harm
```

[Source: IEC Guide 51:2014]

74.
hazardous situation:

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

```
\\
     circumstance
          > in which | [OR] people
                     | [OR] , property
                     | [OR] or the environment
                     |           > are exposed to one or more hazards
```

[Source: IEC 61508-4:2010]
[Source: IEC Guide 51:2014]

76.
incident: correct except for the splitting

event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

```
\\
     event
          > [AND] that is not part
                       > of the expected operation
                              > of a | [OR] system
                                     | [OR] or service
          > [AND] that causes or may cause,
                       > [OR] an interruption to,
                       > [OR] or a reduction in,
                                   > the quality
                                          > of the service
                                                 > provided by the system
```

[Source: IEC 62443-2-1:2010]

77.
incident:

event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

```
\\
     event
          > [AND] that is not part
                       > of the expected operation
                              > of a | [OR] system
                                     | [OR] or service
          > [AND] that causes, or may cause,
                       > [OR] an interruption to,
                       > [OR] or a reduction in,
                                   > the quality
                                          > of the service
                                                 > provided by the control system
```

[Source: IEC 62443-3-3:2013]

78.
industrial automation and control system:

collection of personnel, hardware, software and policies involved in the

```
operation of the industrial process and that can affect or influence its safe,
secure and reliable operation

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , software
                     | [AND] and policies
          > [AND] involved in the operation
                       > of the industrial process
          > [AND] and that can | [OR] affect
                               | [OR] or influence its | [AND] safe,
                               |                       | [AND] secure
                               |                       | [AND] and reliable
operation
[Source: IEC 62443-3-3:2013]

79.
industrial automation and control system:

collection of personnel, hardware, software, procedures and policies involved in
the operation of the industrial process and that can affect or influence its
safe, secure and reliable operation

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , software
                     | [AND] , procedures
                     | [AND] and policies
          > [AND] involved in the operation
                       > of the industrial process
          > [AND] and that can | [OR] affect
                               | [OR] or influence its | [AND] safe,
                               |                       | [AND] secure
                               |                       | [AND] and reliable
operation
[Source: IEC 62443-2-4:2015 + AMD1:2017]

80.
industrial automation and control system:

collection of personnel, hardware, and software that can affect or influence the
safe, secure, and reliable operation of an industrial process

\\
     collection
          > [AND] of | [AND] personnel
                     | [AND] , hardware
                     | [AND] , and software
          > [AND] that can | [OR] affect
                           | [OR] or influence the | [AND] safe,
                           |                       | [AND] secure,
                           |                       | [AND] and reliable operation
                           |                       |           > of an
industrial process
[Source: IEC TS 62443-1-1:2009]


81.
integrity:

property of protecting the accuracy and completeness of assets

\\
     property
```

```
          > of protecting the | [AND] accuracy
                              | [AND] and completeness
                              |           > of assets
```

[Source: IEC 62443-3-3:2013]

82.
integrity:

property of accuracy and completeness

```
\\
     property
          > of | [AND] accuracy
               | [AND] and completeness
```

[Source: IEC Draft Guide 120]

83.
integrity:

quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

```
\\
     quality
          > [AND] of a system
          > [AND] reflecting the | [AND] logical correctness
                                 | [AND] and reliability
                                 |            > of the operating system
                                 | [AND] , the logical completeness
                                 |              > of the | [AND] hardware
                                 |                       | [AND] and software
                                 |                       |           >
implementing the protection mechanisms
                                 | [AND] , and the consistency
                                 |            > of the | [AND] data structures
                                 |                     | [AND] and occurrence
                                 |                     |            > of the
stored data
```

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

85.
interception:

capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission and other communication attributes

```
\\
     [OR] [AND] capture
          [AND] and disclosure
                     > of message contents
     [OR] or use
               > of traffic analysis
                     > [AND] to compromise the confidentiality
                                  > of a communication system
                     > [AND] based on | [OR] message destination
                                      | [OR] or origin
                                      | [OR] , frequency
                                      | [OR] or length
                                      |           > of transmission
                                      | [OR] and other communication attributes
```

[Source: IEC TR 62443-3-1:2009]

86.

interception:

sniffing, capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes

\\
[AND] sniffing
[AND] capture
[AND] and disclosure
> of message contents
[OR] or use
> of traffic analysis
> [AND] to compromise the confidentiality
> of a communication system
> [AND] based on | [OR] message destination
| [OR] or origin
| [OR] , frequency
| [OR] , and other communication attributes
| [OR] or length
| > of transmission
[Source: IEC TS 62443-1-1:2009]

87.
interface:

logical entry or exit point that provides access to the module for logical information flows

\\
[OR] logical entry
[OR] or exit point
> that provides access
> [AND] to the module
> [AND] for logical information flows
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

89.
local area network:

communications network designed to connect computers and other intelligent devices in a limited geographic area

\\
communications network
> designed to connect | [AND] computers
| [AND] and other intelligent devices
> in a limited geographic area
[Source: IEC TS 62443-1-1:2009]
[Source: IEC TR 62443-3-1:2009]

91.
non repudiation:

ability to prove the occurrence of a claimed event or action and its originating entities

\\
ability
> to prove the | [AND] occurrence
| > of a claimed | [OR] event
| | [OR] or action
| [AND] and its originating entities
[Source: IEC Draft Guide 120]

```
[Source: IEC 62443-3-3:2013]


93.
non repudiation:

security service that provides protection against false denial of involvement in
a communication

\\
     security service
          > that provides protection
                 > against false denial
                        > of involvement
                               > in a communication
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

95.
plaintext:

unencoded data that is input to and transformed by an encryption process or that
is output by a decryption process

\\
     unencoded data
          > [OR] that is input to and transformed
                        > by an encryption process
          > [OR] or that is output
                        > by a decryption process
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

97.
product supplier:

manufacturer of hardware and/or software product

\\
     manufacturer
          > of | [OR] hardware
               | [OR] and/or software product

[Source: IEC 62443-3-3:2013]
[Source: IEC 62443-2-4:2015 + AMD1:2017]

99.
reasonably foreseeable misuse:

use of a product, process or service in a way not intended by the supplier, but
which may result from readily predictable human behaviour

\\
     use
          > [AND] of a | [OR] product
                       | [OR] , process
                       | [OR] or service
          > [AND] in a way
                       > [AND] not intended by the supplier
                       > [AND] , but which may result from readily predictable
human behaviour
[Source: IEC 61508-4:2010]


100.
reasonably foreseeable misuse:

use of a product or system in a way not intended by the supplier, but which can
```

```
result from readily predictable human behaviour

\\
     use
          > [AND] of a | [OR] product
                       | [OR] or service
          > [AND] in a way
                       > [AND] not intended by the supplier
                       > [AND] , but which may result from readily predictable
human behaviour
[Source: IEC Guide 51:2014]

101.
remote access:

communication with, or use of, assets or systems within a defined perimeter from
any location outside that perimeter

\\
     [OR] communication with,
     [OR] or use of, | [OR] assets
                     | [OR] or systems
                     |           > [AND] within a defined perimeter
                     |           > [AND] from any location
                     |                       > outside that perimeter
[Source: IEC 62443-2-1:2010]

102.
remote access:

access to a control system by any user communicating from outside the perimeter
of the zone being addressed

\\
     access
          > to a control system
                 > by any user
                        > communicating from
                               > outside the perimeter
                                      > of the zone
                                             > being addressed
[Source: IEC 62443-3-3:2013]

103.
remote access:

access to a control system through an external interface of the control system

\\
     access
          > to a control system
                 > through an external interface
                        > of the control system
[Source: IEC 62443-2-4:2015 + AMD1:2017]

104.
remote access:

use of systems that are inside the perimeter of the security zone being addressed
from a different geographical location with the same rights as when physically
present at the location

\\
     use
          > of systems
                 > [AND] that are inside the perimeter
                              > of the security zone
                 > [AND] being addressed from a different geographical location
```

```
                              > with the same rights
                                    > as when physically present at the location
[Source: IEC TS 62443-1-1:2009]

105.
repudiation:

denial by one of the entities involved in a communication of having participated
in all or part of the communication

\\
     denial
          > [AND] by one of the entities
                       > involved in a communication
          > [AND] of having participated in | [OR] all
                                           | [OR] or part
                                           |           > of the communication
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

107.
residual risk:

risk remaining after protective measures have been taken

\\
     risk
          > remaining after protective measures
                 > have been taken
[Source: IEC 61508-4:2010]

108.
residual risk:

risk remaining after risk reduction measures have been implemented

\\
     risk
          > remaining after risk reduction measures
                 > have been implemented
[Source: IEC Guide 51:2014]

109.
residual risk

remaining risk after the security controls or countermeasures have been applied

\\
     remaining risk
          > after the | [OR] security controls
                      | [OR] or countermeasures
                      |           > have been applied
[Source: IEC TS 62443-1-1:2009]


110.
risk:

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

\\
     combination
          > of the | [AND] probability
                   |            > of occurrence
                   |                   > of harm
                   | [AND] and the severity
                   |            > of that harm
```

```
[Source: IEC 61508-4:2010]
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]


113.
risk:

expectation of loss expressed as the probability that a particular threat will
exploit a particular vulnerability with a particular consequence

\\
     expectation
          > of loss
                 > expressed as the probability
                        > that a particular threat
                               > will exploit a particular vulnerability
                                      > with a particular consequence
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

115.
risk assessment:

process of identifying and evaluating risks to the organization’s operations, the
organization’s assets or individuals by determining the likelihood of occurrence,
the resulting impact, and additional countermeasures that would mitigate this
impact

\\
     process
          > of identifying and evaluating risks
                 > [AND] to the | [OR] organization’s operations
                                | [OR] , the organization’s assets
                                | [OR] or individuals
                 > [AND] by determining | [AND] the likelihood
                                        |            > of occurrence
                                        | [AND] , the resulting impact
                                        | [AND] , and additional countermeasures
                                        |            > that would mitigate this
impact
[Source: IEC 62443-2-1:2010]

116.
risk assessment:

overall process comprising a risk analysis and a risk evaluation

\\
     overall process
          > comprising a | [AND] risk analysis
                         | [AND] and a risk evaluation
[Source: IEC Guide 51:2014]

117.
risk assessment:

process that systematically identifies potential vulnerabilities to valuable
system resources and threats to those resources, quantifies loss exposures and
consequences based on probability of occurrence, and recommends how to allocate
resources to countermeasures to minimize total exposure

\\
     process
          > that systematically identifies potential | [AND] vulnerabilities
                                                     |            > to valuable
system resources
                                                     | [AND] and threats
```

```
                                                        |            > to those
resources
                                                        | [AND] , quantifies loss
exposures
                                                        | [AND] and consequences
                                                                   > based on
probability
                                                                        > of
occurrence
                                                        | [AND] , and recommends how
to allocate resources
                                                        |            > to
countermeasures
                                                        |            > to minimize
total exposure
[Source: IEC TS 62443-1-1:2009]


118.
risk tolerance:

risk the organization is willing to accept

\\
     risk
          > the organization
                > is willing to accept
[Source: IEC 62443-2-1:2010]



119.
risk tolerance level:

level of residual risk that is acceptable to an organization

\\
     level
          > of residual risk
                > that is acceptable to an organization
[Source: IEC TS 62443-1-1:2009]

120.
safety:

freedom from unacceptable risk

\\
     freedom
          > from unacceptable risk
[Source: IEC 61508-4:2010]
[Source: IEC TS 62443-1-1:2009]

121.
safety:

freedom from risk which is not tolerable

\\
     freedom
          > from risk
                > which is not tolerable
[Source: IEC Draft Guide 120]
[Source: IEC Guide 51:2014]

124.
safety instrumented system:
```

system used to implement one or more safety-related functions

\\
     system
          > used to implement one or more safety-related functions
[Source: IEC 62443-3-3:2013]

125.
safety instrumented system:

system used to implement functional safety

\\
     system
          > used to implement functional safety
[Source: IEC 62443-2-4:2015 + AMD1:2017]

126.
safety integrity:

probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

\\
     probability of
          > an E/E/PE safety-related system
                 > satisfactorily performing the specified safety functions
                        > [AND] under all the stated conditions
                        > [AND] within a stated period
                                    > of time
[Source: IEC 61508-4:2010]

127.
safety integrity level:

discrete level for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems

\\
     discrete level
          > for specifying the safety integrity requirements
                 > of the safety-instrumented functions
                        > to be allocated to the safety-instrumented systems
[Source: IEC TS 62443-1-1:2009]

128.
safety integrity level:

discrete level, corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

\\
     discrete level
          > corresponding to a range
                 > of safety integrity values
                        > , where | [AND] safety integrity level 4
                                  | > has the highest level
                                  | > of safety integrity
                                  | [AND] and safety integrity level 1
                                  | > has the lowest
[Source: IEC 61508-4:2010]

129.
security:

a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

\\
     a condition
          > that results from the | [AND] establishment
                                  | [AND] and maintenance
                                  | > of protective measures
                                  | > that ensure a state
                                  | > of inviolability
                                  | > from | [OR] hostile acts
                                  | | [OR] or influences
[Source: IEC Draft Guide 120]

130.
security:

a) measures taken to protect a system

\\
     a) measures
          > taken to protect a system
[Source: IEC TS 62443-1-1:2009]

131.
security:

b) condition of a system that results from the establishment and maintenance of measures to protect the system

\\
     b) condition
          > [AND] of a system
          > [AND] that results from the | [AND] establishment
                                        | [AND] and maintenance
                                        | > of measures
                                        | > to protect the system
[Source: IEC TS 62443-1-1:2009]

132.
security:

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

\\
     c) condition
          > of system resources
                > being free from | [AND] unauthorized access
                                  | [AND] and from | [OR] unauthorized
                                  | | [OR] or accidental change
                                  | | [OR] , destruction
                                  | | [OR] , or loss
[Source: IEC TS 62443-1-1:2009]

133.
security:

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

\\
d) capability
> of a computer-based system
> [AND] to provide adequate confidence
> that unauthorized | [AND] persons
| [AND] and systems
| > can neither | [OR] modify the software
| | [OR] nor gain access
| | > to the | [AND] system functions
| | | [AND] and its data
> [AND] , and yet to ensure that this is not denied to authorized persons
[Source: IEC TS 62443-1-1:2009]

134.
security:

prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

\\
prevention
> [OR] of illegal or unwanted penetration of
> [OR] , or interference
> with the | [AND] proper
| [AND] and intended operation
| > of an industrial automation and control system
[Source: IEC TS 62443-1-1:2009]

135.
security incident:

security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

\\
[OR] security compromise
> that is of some significance
> to the asset owner
[OR] or failed attempt
> [AND] to compromise the system
> [AND] whose result
> could have been of some significance
> to the asset owner
[Source: IEC 62443-2-4:2015 + AMD1:2017]

136.
security incident:

adverse event in a system or network, or the threat of the occurrence of such an event

\\
[OR] adverse event
> in a | [OR] system
| [OR] or network

```
     [OR] , or the threat
               > of the occurrence
                     > of such an event
[Source: IEC TS 62443-1-1:2009]
```

```
137.
security level:

measure of confidence that the IACS is free from vulnerabilities and functions in
the intended manner

\\
     measure
          > of confidence
                 > that the IACS
                       > [AND] is free from vulnerabilities
                       > [AND] and functions in the intended manner
[Source: IEC 62443-3-3:2013]
```

```
138.
security level:

level corresponding to the required effectiveness of countermeasures and inherent
security properties of devices and systems for a zone or conduit based on
assessment of risk for the zone or conduit

\\
     level
          > [AND] corresponding to the | [AND] required effectiveness
                                       |            > of countermeasures
                                       | [AND] and inherent security properties
                                       |            > [AND] of devices
                                       |            > [AND] and systems
                                       |                        > for a | [OR]
zone
                                       |                                | [OR] or
conduit
          > [AND] based on assessment
                      > of risk
                           > for the zone
[Source: IEC TS 62443-1-1:2009]

139.
security program:

portfolio of security services, including integration services and maintenance
services, and their associated policies, procedures, and products that are
applicable to the IACS

\\
     portfolio
          > [AND] of security services
          > [AND], including | [AND] integration services
                             | [AND] and maintenance services
                             | [AND] , and their associated | [AND] policies
                             |                              | [AND] , procedures
                             |                              | [AND] , and
products
                             |                              |           > that
are applicable to the IACS
[Source: IEC 62443-2-4:2015 + AMD1:2017]


140.
security program:
```

```
combination of all aspects of managing security, ranging from the definition and
communication of policies through implementation of best industry practices,
ongoing operation and auditing

\\
     combination
          > of all aspects
                 > [AND] of managing security
                 > [AND], ranging from the | [AND] definition
                                           | [AND] and communication
                                           |           > of policies
                 > [AND] through | [AND] implementation
                                 |           > of best industry practices
                                 | [AND] , ongoing operation
                                 | [AND] and auditing
[Source: IEC TS 62443-1-1:2009]

141.
security services:

mechanisms used to provide confidentiality, data integrity, authentication, or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] , or no repudiation
                            |           > of information
[Source: IEC Draft Guide 120]



142.
security services:

mechanisms used to provide confidentiality, data integrity, authentication or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] or no repudiation
                            |           > of information
[Source: IEC TR 62443-3-1:2009]

143.
security services:

mechanisms used to provide confidentiality, data integrity, authentication or no
repudiation of information

\\
     mechanisms
          > used to provide | [OR] confidentiality
                            | [OR] , data integrity
                            | [OR] , authentication
                            | [OR] , or no repudiation
                            |             > of information
[Source: IEC TS 62443-1-1:2009]

144.
server:
```

```
device or application that provides information or services to client
applications and devices

\\
     [OR] device
     [OR] or application
               > that provides | [OR] information
                               | [OR] or services
                               |           > to | [OR] client applications
                               |                | [OR] and devices
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

146.
service provider:

organization that has agreed to undertake responsibility for providing a given
support service and obtaining, when specified, supplies in accordance with an
agreement

\\
     organization
          > that has agreed to undertake responsibility
                 | [AND] for providing a given support service
                 | [AND] and obtaining, when specified, supplies
                 |            > in accordance
                 |                  > with an agreement
[Source: IEC 62443-3-3:2013]


147.
service provider:

individual or organization that provides a specific support service and
associated supplies in accordance with an agreement with the asset owner

\\
     [OR] individual
     [OR] or organization
               > that provides a | [AND] specific support service
                                 | [AND] and associated supplies
                                 |            > in accordance
                                 |                  > with an agreement
                                 |                        > with the asset
owner
[Source: IEC 62443-2-4:2015 + AMD1:2017]


148.(omitted since it has only one word)
149.(omitted since it has only one word)

150.
software safety integrity:

part of the safety integrity of a safety-related system relating to systematic
failures in a dangerous mode of failure that are attributable to software

\\
     part
          > of the safety integrity
                 > [AND] of a safety-related system
                 > [AND] relating to systematic failures
                            > [AND] in a dangerous mode
                                      > of failure
                            > [AND] that are attributable to software
[Source: IEC 61508-4:2010]
```

```
151.
software safety integrity level:

systematic capability of a software element that forms part of a subsystem of a
safety-related system

\\
     systematic capability
          > of a software element
                 > that forms part
                        > of a subsystem
                               > of a safety-related system
[Source: IEC 61508-4:2010]

152.
spoof:

pretending to be an authorized user and performing an unauthorized action

\\
      [AND] pretending to be authorized user
      [AND] and performing an unauthorized action
[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

154.
system:

interacting, interrelated, or interdependent elements forming a complex whole

\\
     [OR] interacting,
     [OR] interrelated,
     [OR] or interdependent elements
               > forming a complex whole
[Source: IEC 62443-2-4:2015 + AMD1:2017]
[Source: IEC TS 62443-1-1:2009]

156.
system software:

part of the software of a PE system that relates to the functioning of, and
services provided by, the programmable device itself, as opposed to the
application software that specifies the functions that perform a task related to
the safety of the EUC

\\
     part
          > [AND] of the software
                        > of a PE system
          > [AND] that relates to the | [AND] functioning of, and services
                                      |            > provided by, the
programmable device itself
                                      | [AND] , as opposed to the application
software
                                      |            > that specifies the functions
                                      |                   > that perform a task
                                      |                          > related to the
safety
                                      |                                 > of the
EUC
[Source: IEC 61508-4:2010]

157.
system software:

special software designed for a specific computer system or family of computer
```

systems to facilitate the operation and maintenance of the computer system and associated programs and data

\\
special software
| [AND] designed for a specific | [OR] computer system
| | [OR] or family
| | > of computer systems
| [AND] to facilitate the operation
| [AND] and maintenance
| > of the | [AND] computer system
| | [AND] and associated | [AND] programs
| | | [AND] and data

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

159.
threat:

circumstance or event with the potential to adversely affect operations, assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

\\
[OR] circumstance
[OR] or event
> with the potential
> to adversely affect | [OR] operations
| [OR] , assets
| [OR] , control systems
| [OR] or individuals
> via | [OR] unauthorized access
| [OR] , destruction
| [OR] , disclosure
| [OR] , modification
| > of data
| [OR] and/or denial
| > of service

[Source: IEC 62443-3-3:2013]

160.
threat:

potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

\\
potential
> [AND] for violation
> of security
> [AND], which exists when there is a | [OR] circumstance
| [OR] , capability
| [OR] , action
| [OR] , or event
| > that could | [AND] breach security
| | [AND] and cause harm

[Source: IEC Draft Guide 120]

161.
threat:

potentially damaging action or capability to adversely impact through a vulnerability

\\
potentially | [OR] damaging action
| [OR] or capability
| > to adversely impact
| > through a vulnerability
[Source: IEC TR 62443-3-1:2009]

162.
threat:
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

\\
potential
> [AND] for violation
> of security
> [AND] , which exists when there is a | [OR] circumstance
| [OR] , capability
| [OR] , action
| [OR] , or event
| > that could | [AND] breach security
| | [AND] and cause harm
[Source: IEC TS 62443-1-1:2009]

163.
tolerable risk:

risk which is accepted in a given context based on the current values of society

\\
risk
> which is accepted in a given context
> based on the current values
> of society
[Source: IEC 61508-4:2010]

164.
tolerable risk:

level of risk which is accepted in a given context based on the current values of society

\\
level
> of risk
> which is accepted in a given context
> based on the current values
> of society
[Source: IEC Guide 51:2014]

165.
vulnerability:

flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise

\\
[OR] flaw
[OR] or weakness
> [AND] in the | [OR] design
| [OR] , implementation

```
                                | [OR] , or operation
                                | [OR] and management
                                |           > of a component
                > [AND] that can be exploited to cause a security compromise
[Source: IEC 62443-2-4:2015 + AMD1:2017]


166.
vulnerability:


flaw or weakness in a system’s design, implementation, or operation and
management that could be exploited to violate the system’s security policy

\\
     [OR] flaw
     [OR] or weakness
               > [AND] in a system’s | [OR] design
                                     | [OR] , implementation
                                     | [OR] , or operation
                                     | [OR] and management
               > [AND] that could be exploited to violate the system’s security
policy
[Source: IEC Draft Guide 120]

167.
vulnerability:

flaw or weakness in a system's design, implementation, or operation and
management that could be exploited to violate the system's integrity or security
policy

\\
     [OR] flaw
     [OR] or weakness
               > [AND] in a system’s | [OR] design
                                     | [OR] , implementation
                                     | [OR] , or operation
                                     | [OR] and management
               > [AND] that could be exploited to violate the system’s | [OR]
integrity
                                                                       | [OR] or
security policy

[Source: IEC TR 62443-3-1:2009]
[Source: IEC TS 62443-1-1:2009]

169.
wide area network:

communications network designed to connect computers, networks and other devices
over a large distance, such as across a country or the world

\\
     communications network
          > designed to connect | [AND] computers
                                | [AND] , networks
                                | [AND] and other devices
                                |            > over a large distance
                                |                  > , such as across a | [OR]
country
                                |                                       | [OR]
or the world
[Source: IEC TS 62443-1-1:2009]

170.
wide area network:
```

communications network designed to connect computers over a large distance, such as across a country or the world

\\
     communications network
          > designed to connect computers
                 > over a large distance
                        >, such as across a | [OR] country
                                            | [OR] or the world
[Source: IEC TR 62443-3-1:2009]

171.
zone:

grouping of logical or physical assets that share common security requirements

\\
     grouping
          > of logical or physical assets
                 > that share common security requirements

[Source: IEC 62443-3-3:201