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

Principles of Conceptual Analysis for Electrotechnical Terminology (ConcAn)

Peter Bernard Ladkin

Causalis Ingenieurgesellschaft mbH, Bielefeld, Germany

Abstract

The term Conceptual Analysis has a storied history in philosophy, in particular in the 20th Century. I argue here for a specific application to electrotechnical terminology, ConcAn. I suggest the necessity for ConcAn by considering a contemporary example from the IEC. I then elucidate some principles of, and illustrate, ConcAn by means of a running example, the notion of reliability. *There are likely important principles still to discover.*

1 Introduction

1.1 Background

In October 2023, a proposal was circulated by the IEC[1] to revise the entries in the International Electrotechnical Vocabulary (IEV n. d.) for the terms "electric" and "electrical". The key entries are 151-11-03 electric: "*containing, producing, arising from, or actuated by electricity*", and 151-11-05 electrical: "*pertaining to electricity, but not having its properties or characteristics*" [2].

I had not thought about these terms before. They are surely basic adjectives in the engineering science of electrotechnology. That suggests to me that we ought to have them clearly and accurately defined for such use.

A non-native-English-speaking colleague suggested that he was not at all clear on any difference. If that were to be so, surely, we could dispense with one of them? Indeed, IEC rules say we should — synonyms are not to be assigned separate entries in the IEV, but just one entry with the synonyms listed there as such.

A look in the Oxford English Dictionary[3] reveals that they register 175 meanings for the English word *electric* and *"[t]he usual current sense*" (no pun intended) is *"[p]owered by electricity, operating by means of electricity; (also) used for measuring or producing electricity*". It also hints that it can be a synonym for "*electrica*l". The OED registers — attempts to register — all uses of the term in the language. Terms used in science and engineering may well have more circumscribed meanings that are appropriate for science and engineering use. We shall see that this may well be so for "*electric*".

[1] The International Electrotechnical Commission, an international standards organization.

[2] The International Electrotechnical Vocabulary is available at www.electropedia.org and entries may be found by searching for the term, or by giving the reference number.

[3] Available at www.oed.com

© Peter Bernard Ladkin 2024.

The OED "*usual current sense*" does not include "*actuated by electricity*", which the IEV definition includes. Let us consider "*actuated by electricity*". My building heating is usually described as "*gas heating*" and it includes a "*gas boiler*", which heats water by burning gas piped in from the street gas supply (heat exchange), and this water is circulated in the building radiators. It is actuated by electrical equipment and thus by electricity: if there is no electricity, my gas boiler does not work. According to the IEV definition, my gas heating is electric.

The IEV definition does not include "*operating by means of electricity*". But that is how my brain works (according to neurophysiologists); indeed, how my nervous system works. My nervous system is "*actuated by electricity*". When Walt Whitman wrote "*I Sing the Body Electric*", he was not writing an ode to neurophysiology[4]; he was trying to say something new.

Furthermore, it turns out all the cars we now have on the roads are really *electric cars* after all, for they are *actuated by electricity*, and *operated by means of electricity*, as anyone knows who has had the misfortune to deal with a faulty generator on a journey, or who has had to call the emergency road service to help with a dead battery. All those diesel locomotives we have on our railroads worldwide are also *electric*, for the traction is provided by motors which are *powered by electricity*. (In GB, they are indeed called diesel-electric, but this moniker is not common in other European countries, or in the US.)

If we take these definitions/explanations of the term as literally meaning what they say, we can thus quickly get into confusion concerning their appropriate use in English. Current usage says: my body is not electric; its source of power is predominantly electromagnetic (EM) (heat ultimately from the sun) and biochemical. My gas heating is not electric; it is gas (that is why we call it "gas heating"). Those internal combustion engine (ICE) cars are not electric, their source of power is chemical, from liquid petrol or diesel fuel. Those diesel locomotives burn diesel fuel as a chemical source of energy. All of this technical material about power and sources and conversions is readily apparent to, say, a bright Chinese-native-speaking engineer. If that engineer is trying to learn English electrotechnical vocabulary, in order to converse with other engineers in other countries, she will be misled by the IEV and OED definitions.

I think we can take it that it is no purpose, either of the IEV or of the OED, to sow confusion about the appropriate use of terms in the English language. It is a purpose of the OED to register all usage; it should not surprise us that some meanings are inconsistent with others. However, for the IEV, we can surely see a purpose for precision and clarity in the meanings given for terms which it takes to be technical. But we have just seen how confusion can easily happen.

What is the remedy? The remedy is, surely, to get it right.

How do we get it right? The proposal of this paper is: conceptual analysis.

Yes, bodily functions such as thinking and moving are actuated by electricity, but the body is not in common parlance electric. Why not? Well, to get our energy, we eat and drink, and we wear clothes to keep warm (37° C is recommended). Eating and drinking provides energy (both warmth and electrical energy) through biochemical processes; the sun and other EM sources provide warmth (and clothing helps us to preserve it). My gas heating is not in common parlance electric. Why not? Because most of the energy which goes to warm my building comes from burning gas and heat exchanging (first to water circulation, then to aerial convection and conduction and EM heat radiation). Similarly, when our IEC

[4] As one might clearly read at https://www.poetryfoundation.org/poems/45472/i-sing-the-body-electric

cars run out of energy, we fill them with burnable, i.e. chemically transformable, liquid petroleum or diesel fuel. When our diesel locomotive needs to run another 500km, it is filled with burnable liquid diesel fuel.

In all of these cases, energy is transformed amongst different types. I would suggest: we tend to label the operation with the *source* of its used energy. "Source" here means "from outside the entity itself". The electricity in the human body, in the diesel locomotive, in my building's heating, in the ICE car, is an intermediary store at best. The source is elsewhere. In the case of my body, there are two: basic environmental heat (we may take it: radiative and conductive) and biochemical. In the case of my heating and ICE and diesel vehicles, chemical.

1.2 Being More Precise About "Electric"

Let me propose: something is *electric* if electricity is the *main source of power for its function*. (In such a definition, *electric* is the definiendum; *main source of power for its function* is the definiens.)[5]

The terms in this definition which are not purely syntactic are *main*, *source*, *power*, *function*. The terms which are "purely syntactic" are *of*, *for*, *its*; their semantic roles are to be explained in terms of how they are used to combine the other terms. Let me call these conjunctive words. We have addressed the roles of conjunctive words in definitions using a technique we called "SemAn" (Ladkin et al. 2023). What I am here calling conceptual analysis considers what the other terms *main*, *source*, *power*, *function* in the definiens — let me call them *conceptual terms* — contribute to the meaning of the term *electric*.

I deal now with the conceptual terms in turn, but in the order *power*, *source*, *main*, *function*.

The main substantive in the definiens is *power*. Such power could be electric, chemical, physico-chemical, e.g. internal-combustive, biochemical, nuclear, laser, heat, light, magnetic. It is surely, and clearly, important engineering-scientific information that the power enabling the function of an entity is, for example, electric.

The definiens says, not that electricity is the *power*, but that it is the *source of power*. Why this? I will take the answer to have been given in the discussion above. Distinguishing between electricity as the *power* and electricity as the *source of power* is thus important to conform with current technical usage.

The term *main* in *main source* is important. For, consider the case of the human body. I take it that it is possible to argue that the source of power for most human functions is electric — the operation of neurons and the complicated nervous-system interactions that give us our human characteristics are predominantly electrical. But the amount of electrical energy involved is small. The main source of bodily power is chemical (food) and heat, as noted above.

Can we speak of everything as having a function? A word for this is teleological (which I have used in systems engineering for nearly thirty years; it hasn't caught on). All engineering-devised systems are teleological; someone put them together for a purpose. The classic von Bertalanffy systems are not teleological — predator-prey systems for example (unless one adheres to a religion which says they are divinely purposed).

[5] Note that this definiendum/definiens pair does not satisfy the substitutability condition: that the definiens be substitutable for the definiendum *salva veritate* in all contexts. A suitable definiens which better satisfies the substitutability condition would be "using electricity as the main source of power for its function".

The term function is also used informally when explaining how a living creature or parts of it fits into its environment; e.g., what is the function of the eye? A strict evolutionary theorist would say that no evolved living creature or its parts has literally a function in this sense; it merely has parts which have had survival advantages over others. But, we can ask, what are these advantages? And, if we like, understanding that proposed mechanism, we can call them by analogy functions, which is what indeed many biologists do.

Consider an art installation that relies upon neon light tubes to provide bright colours. It is art; it is also static; however, it does have behaviour (behaviour is a change of state; it can go from off to on and from on to off). Does it have a function? One may say that it was conceived and built by the artist for some reason — say, as with much art, to induce the viewer to engage. Then it is teleological. Is electricity part of that function? Yes; if it is turned on at some point and that is part of what the artist intended. If it is never turned on and the artist did not intend for it ever to be turned on, the answer could well be no. According to the proposed definition, it is an electric art installation in the first case; not in the second.

I am concerned here, as are most readers of this journal I take it, with electrotechnology — electrical engineering — and its vocabulary. I would propose that all engineering is teleological, and it makes sense for any engineering artifact to inquire what its function is (or is intended to be).

1.3 Conceptual Analysis and ConcAn

The reader may or may not agree with all the considerations adduced above. The important aspects for this article are:

- We distinguish in a terminological definition between definiendum and definiens
- The definiens includes conceptual terms and conjunctive words
- The role of conjunctive words has been (partially) addressed by SemAn (Ladkin et al. 2023)
- The conceptual terms may be considered both individually and in conjunction to determine, along with SemAn, what the definiendum means in electrotechnological use
- The analytical consideration of the conceptual terms is what I am calling conceptual analysis
- The specific form of conceptual analysis advocated in this paper is called ConcAn

There are some things to be said about electrical*, and how this term differs from* electric*, but I would suggest that is for terminologists improving the IEV and not for this paper. In this paper I propose a way to go about analysing concepts, as I did electric, above, and thereby improving the terminological definitions available to us in electrotechnology. I call this* "ConcAn".

2 Some Philosophical History

2.1 Conceptual Analysis

The term conceptual analysis has a history in philosophy, which can be argued to originate with Immanuel Kant (although the techniques are as old as philosophy itself). This section gives a brief survey. The point of such a survey is that the history of conceptual analysis

in philosophy includes major contributions by major intellects, and the reasons why those contributions arose is important to understand what they offer. Much of it will not necessarily be relevant for electrotechnology, but some of it I would argue is not only relevant but very important.

2.2 A Very Brief Summary of Conceptual Analysis in Analytical Philosophy

It is fairly clear to most people what a physical object is. They are encountered every minute of our waking life, and indeed our sleeping life also, although we are less aware of them. We can designate them and communicate about them when they are not ostensively present. But those same communicative actions can also be used to communicate about things which may not exist in the same way, or at all. I can talk about a ghost the same way I can talk about my next-door neighbour. I can identify patterns of objects: there is an orange and another orange; there is an apple and another apple; there is something similar, we think, about those two situations. We call that similarity the number of designated objects, in this case two. But I cannot point to a number itself, such as *two* or *three*, or throw it to you, or eat it, in the same way in which I can an orange; the mode of designation, we might call it, is different.

British "empiricists" in the 17th and into the 18th Centuries (well exemplified by John Locke, Bishop George Berkeley, and David Hume) were concerned to explain "the world", i.e. the world of physical objects plus whatever, through considering how our mental activity connected to the world of objects independently of our bodily capabilities. Features — patterns — in the world of objects were "perceived" by us. According to Locke, there were supposed to be mental correlates of these features somehow "in the mind" of the perceiver (when perceiving veridically); these mental correlates were called "ideas". We have immediate cognitive access to the ideas occurring in our minds; according to Locke's philosophical psychology that is *exactly* what we had cognitive access to. But then the problem became to explain veridicality: if our ideas are all we have access to, how could we determine they were veridical representations of the world? For we had, by hypothesis, no access to "the world" in itself to compare, just to our ideas. This came to be called the "veil of perception", behind which we could, by hypothesis, not peek.

Bishop Berkeley bit the bullet and said, actually, "the world" consists of ideas in the mind of God, and the way we know our ideas (perceptions) are veridical is because the good God ensures that it is so in various ways; he doesn't try to deceive us, nor does he let us be deceived about them, as Descartes worried. Berkeley's is an answer of a sort, but just pushes the problem a bit further: how do we know that God is like that? One answer, "faith", is Christian-religiously but no longer philosophically respectable — the question proved to be almost impossible to answer for those not disposed to Christian-theological precepts. Berkeley's position came to be seen as a version of "assume the answer".

David Hume worried (amongst other things) about how "the world" exhibited its regularities. How and why do things happen? What are the origins of such happenings — the causes, as they came to be called — of things which happen? We can see causes and their effects as "constant conjunction": when phenomenon A causes phenomenon B, A is always temporally accompanied by or followed by B. Hume noted that we can observe constant conjunction, but what we cannot do is perceive causation happening directly. But if we cannot observe causation directly, how can we be sure that the next iteration of A will be followed by B? We can, if it is indeed the case that A causes B, but we cannot be sure of that from observation — we only observed the constant conjunction; maybe what we observed was just happenstance, and not an instance of causation? The sun has risen

each and every day of the world's existence; elaborate theories of the causes of that phenomenon, from Ptolemy through Copernicus and Kepler to Newton, were/are available. But what if tomorrow it didn't happen? How do I know that I have been seeing an instance of causation? How can I reason from what has happened to what will happen?

Kant attempted to shoehorn all this into structural constraints on perception and cognition, and to derive from them, along with veridical perception, concrete manifestations of causality. These structural constraints could be called concepts, and thinking according to these constraints is conceptualisation. These concepts were to be independent of people, in so far as they were still to be present even if there were no people around to engage in perception. One might say, the structure is valid even if not realised. Our perceptions are, and experience is, veridical in so far as it conforms with these constraints. When it does, causality is manifested as such-and-such. It is facile, one might think, to summarise Kant's philosophy in a few such sentences as these. I would agree, but Kant's philosophy is not the subject of this paper. Rather, his notion of concept and the kinds of analysis in which he indulged can be considered the modern origins of the topic of this paper.

Kant considered in detail what it meant for a *concept* to have a definition. For example, one could define a bachelor to be an unmarried man. How does such a definition work? Kant suggested such assertions are *analytic*, meaning for him that the "concept" of bachelor "contains" the "concept" of "unmarried" as well as the concept of "man". The notion of "contains" needs elaboration (and will not get it in this document). A statement/assertion for Kant is a statement P(A), where A denotes the subject and P the predicate. The idea would be that the predicate "contains" the concept under which the subject is presented. So this means that, in P(A), which is analytic, A is not a proper name, but a presentation of a kind of thing: "a bachelor", for example, which is a count noun; or a mass term — "water", for example. Thus, "Peter is an unmarried man" could not be analytic because of its form ("Peter" is a name, not a count noun or mass term); "a bachelor is an unmarried man" is analytic[6].

Kant claimed all assertions had such subject-predicate form. This view changed with the introduction of the language of first-order logic (FOL) by Frege, and its subsequent uses, for example in Russell and Whitehead's *Principia Mathematica*, and Russell's *Theory of Descriptions*, in which an assertion can have the general forms known in FOL[7]. So, for example, "all bachelors are unmarried men" could be analytic, even though it is not nowadays seen to have subject-predicate form; c.f. "all positive integers are either even or odd". Conceptual analysis thus could come to mean the study of analytic statements and what makes them analytic, and how to tell if a statement is analytic.

In the mid-20th Century, W. V. O. Quine wrote an influential paper, *Two Dogmas of Empiricism*, in which he cast doubt that the Kantian notion of analyticity had a well-defined meaning (Quine 1951). This is not quite the way he put it, for he cast doubt on the coherence of the notion of unambiguous "meanings" in general. In his later book, *Word and Object*, he illustrates in detail through the notion of "radical translation" (Quine 1960). He considers in detail an attempt by an individual to learn an unknown language from scratch. Watching a speaker use so-called "observation sentences" is helpful: observation sentences are assertions about things in the present environment to which one can point with a hand or a finger. A speaker points at a rabbit and says "*gavagai*". Quine argues

[6] There is a question whether "a bachelor is a married man" should be considered analytic in Kant's sense, for the subject is not "contained in" the predicate, but rather explicitly excluded by it. Modern discussions which accept the notion of "analytic" would deem the sentence to be *analytically false*; in this case the relevant predicates of sentences are "analytically true" and "analytically false" and the term "analytic" can be taken to mean "either … or …" .

[7] This view has since widened further to include more complex formal-logical languages than FOL.

that a "radical translator" is fundamentally unable to distinguish whether "gavagai" is a rabbit, and the assertions about "gavagai" assertions about rabbits, or whether "gavagai" refers rather to a coherent collection of mutually cooperating rabbit-parts, and assertions about gavagai are assertions about mutually-cooperating rabbit-parts. He further observes that these two kinds of discourse in our language are logically different: one assertion is about a singular (rabbit); the other about a plurality (lots of rabbit parts). This is the thesis of the "indeterminacy of translation": gavagai is a rabbit, or equivalently many cohering rabbit-parts, and according to Quine a translator fundamentally has no means of telling which ontology is being used.

It follows that this must be so even when you and I are talking to each other in the "same" language: you cannot fix my "set of concepts" just by experiencing how I use them, and there is no way of eliminating this indeterminacy. It follows further that, if there is no way of telling what concepts are being used and how, there is no reasonable way in which we can talk to each other about concepts, except in so far as we make "working assumptions": when you say "*rabbit*", I presume your concept is identical to my concept of rabbit. That makes it easier to work with you, but it by no means entails that you have my concept of rabbit. So that sets the whole idea of "concepts" in question. Quine held that this even extends to logic and mathematics: he further suggests that, if even these are indeterminate, we might just as well use first-order logic (FOL) and mathematics based on it (and Peano Arithmetic, and…).

If there are no concepts as construed in broadly Kantian terms, then there is clearly no conceptual analysis based on broadly Kantian notions. The "standard story" (one version of it) is then that Saul Kripke got the notion of "concept" back on track. He became known in the mid-1950's for a piece of logic performed when he was a teenager. He gave a Tarskian semantics for so-called modal logics; formal logics that, besides the sentential logical operators AND, OR, NOT and IF...THEN, and quantifiers if first-order, have additional unary sentential operators NECESSARILY and POSSIBLY (which are "dual" in a technical sense: an assertion is necessary if and only if its negation is not possible, and something is possible if and only if its negation is not necessary). Quine had rubbished modal logic, by connecting it with the notion of "analytic", which notion he had argued could not be coherently sustained. Kripke gave a "possible world" semantics, a Tarskian model-theoretic semantics in which the models of a theory in modal logic were a class of "possible worlds". Some of those worlds were "accessible" from others, and some not. Those sentences (NECESSARILY A) were true in a world W just in case A is true in every world accessible from W.

So, for example, a world W.1 in which I am driving a car, swerve to avoid an obstacle and narrowly miss crashing into a wall at 60 kph is accessible from a world W.2 in which I am driving that car, and the same things happen, except that I hit the wall head-on (and all which follows from that) at time T. The world W.3 in which I am alive at T+100 seconds is accessible from W.1 (indeed, W.1 itself might be such a world), but it is implausible to claim that it is accessible from W.2; as we say, "*no one could survive that*", or as we might say using the terminology of modal logic, "*it is not possible to survive that event*".

Kripke extended his analysis in an article (and then a book), *Naming and Necessity*, in which he explained how names came to be used for objects, and how from these processes it could be argued that some objects (referred to by using their names) had some properties necessarily (that is, had those properties in all possible worlds), and these properties could be then taken to define the object that the term named (Kripke 1980). Such terms were called "rigid designators". Concepts and their definitions, according to this telling of the story, were rehabilitated through this account.

This story is well-summarised by Jerry Fodor (2004). Some more matter on Conceptual Analysis in philosophy may be found in Beaney (2003) and in Margolis & Laurence (2005).

2.3 The Importance of This History for Electrotechnology

2.3.1 Preamble

The importance of this story for electrotechnological conceptual analysis is threefold. First, *pace* Quine, conceptual analysis can be performed (Kripke). Second, there are people working in electrotechnology who think that truth is relative (to one's interests — see below for a fairy tale). That truth is relative to one's interests, rather than a measure of an objective condition of the world, is a thesis associated with philosophical pragmatism, an approach to which Quine is commonly held to conform. That truth is relative is a common accompaniment of the Quinean argument, but more often associated with Richard Rorty, and far more prevalent in the academic humanities, and thereby amongst far more people than there are philosophers, let alone philosophers with the academic inclination to refute it.

2.3.2 Contra Analytics: The Relativity of Truth and Its Use in Business

People who hold that truth is relative set little store by careful definition, because there is, according to them, no such thing. To those of us who believe that conceptual analysis is helpful, even necessary, it can be a hindrance to have people propose what we take to be poor or deviant definitions of technical terms and insist it does not matter. A fairy tale suffices to illustrate[8].

The fairy tale: If truth is relative, then it can be deemed by a company's engineers to be relative to the business model of their company. Say the business model says "*As the solution to issue Y, we do X; we do X particularly well; everybody should do X, and they should engage us to do X for them*." The question for a conceptual analyst would be *inter alia* if X makes sense as a solution to issue Y. To a non-relativist, the answer would be maybe it does, or partially does; or maybe it doesn't. To a relativist company engineer, it suffices that the company advocates X as the solution to Y for X to be the solution to Y. To that engineer, there need be no "yes, but …." to which she has to accede. There need be no discussion of whether X is a satisfactory solution to Y in which she has to participate. She has only to align customers with the company's point of view.

2.3.3 Notions in Cybersecurity

An example of such analytics and/or their lack may be seen in the way in which cybersecurity and functional safety is currently handled in IEC standards. There is an IEC Technical Report (TR, which gives recommendations, but does not contain normative injunctions) that recommends how cybersecurity considerations should be integrated into the development of safety-critical E/E/PE systems. This TR, IEC TR 63069:2019, uses centrally the notion of "security environment", which is defined as "*area of consideration where all relevant security countermeasures are in place and effective*". Setting aside

[8] A reviewer wished for examples of relativity. To elucidate concrete instances would likely contravene a number of my professional commitments (including codes of conduct); hence the fairy tale.

what the first four words may mean, and using instead the term in the definiendum, a reasonable interpretation of this is "a system environment in which all relevant security countermeasures are in place and effective". It was discussed in Ladkin (2020) whether (and how) such a notion can make any sense. Reading books for practitioners by some eminent authors could lead one to the conclusion that such an environment cannot exist in the current state of the art (Spafford et al. 2023).

IEC TR 63069 advocates establishing a "security environment" (in its sense) for the development of safety-critical systems. The TR is in process of becoming a Technical Specification (TS), a document which has normative import. That means that those developing or integrating systems with safety-critical components conformant with the document will be required to establish a "security environment", which is an impossible task if one cannot exist. One can imagine, though, companies promoting their expertise in establishing such "security environments" according to IEC TR 63069:2019 and its successor TS and gaining business by so doing. A conceptual analyst conversant with Spafford, Metcalf & Dykstra (2023), and other literature from cybersecurity experts, may well object to such marketing. The company can claim that an IEC standard says do it, and they do it, so you should buy their expertise. The analyst says no one can do it, in particular the company, so no one should believe the misleading claims. The company has "its truth"; the analyst has "her truth". "So what?", says the truth-relativist (amongst them, the company).

End of fairy tale: The reader may conclude that this situation is satisfactory, or that it is unsatisfactory. If this situation is unsatisfactory, part of the goal of this paper is to demonstrate what can be done about it conceptually-analytically.

2.3.4 An Example of Fruitful Application

It turns out that possible-worlds thinking, of the sort introduced by Kripke as part of his rehabilitation of concepts, is amenable to practicing engineers. I introduced a causal-analysis method, Why-Because Analysis (WBA), starting in 1995, to analyse accidents causally (Ladkin 2001) (Ladkin 2017). WBA is based on the counterfactual notion of causality expounded by David Lewis (1973a) and others (Collins et al. 2004) (Paul and Hall 2013), and counterfactual assertions were given a possible-worlds semantics (also by Lewis (1973b)). Our early experience with WBA showed that engineers were able to reason counterfactually in a more or less uniform manner (their judgements on the counterfactuals which occur when trying to analyse engineered-system causality counterfactually were generally uniform, modulo independent sources of error). Because of this, we could base our fault analysis method, Causal Fault Analysis (CFA), as well as our hazard analysis technique, Ontological Hazard Analysis (OHA), also on this approach (Ladkin 2017).

3 Goals of Conceptual Analysis in Electrotechnology

3.1 System Science

Electrotechnologists (and others) nowadays concern themselves with complex conjunctions of equipment, each of which can be individually quite complex, either with notionally complex behaviour, or with complex conditions under which the desired behaviour is to be guaranteed as far as possible. These conjunctions of equipment are

called systems. There is an emerging branch of technology called systems engineering, which is concerned with how systems are built, how they acquire and maintain the properties desired of them by their creators, what their desired and undesired behaviour may consist of, and so forth. Much of this work is nowadays very conceptual, for example the documentation of moderately complex dependable software includes specifications, as well as arguments providing reasons why the software satisfies its requirements, and also lower-level specifications, because such systems are often designed hierarchically (or "recursively" as some system engineers like to say (Ricque 2019)). Such software is mostly built hierarchically unless it is very simple indeed, and most assured-dependable software is not simple, in the sense that even a few lines of code may have complex behaviour when compiled, linked and loaded onto hardware which executes it. The documentation of how all this fits together is equally complex. And then there are test designs and documentation of the results of tests and assessments of test coverage. Even here, testing is known to be scientifically inadequate to assure properties of software that is required to be highly dependable (Littlewood and Strigini 1993).

Such a complex process as critical-software development, assessment and operation, then, is driven by intermediate items ("documentation" in the phrase of David Parnas[9]) which are primarily conceptual. A collection of concepts demonstrably adequate to this task is key to its accomplishment.

System science is not the only phenomenon in modern electrotechnology, but it is currently one of the least developed. The technical terminology for the physics and mechanics used in electrotechnology is in contrast pretty well established (in some cases for a century or longer). The conceptual analysis required is a matter of going back to visit physics courses to refresh it.

Engineers make statements about systems in discussion with other engineers and others, and it is currently hard to tell how many of these statements connect with the real world of a plethora of engineered and other objects engaging in joint behaviour. So, while systems science is not the whole story, we can maybe use it to illustrate how a useful conceptual apparatus may be built up, and what the adverse consequences can be if it is not.

3.2 The Vocabulary of Systems Science

First, systems have parts. It makes sense to call some of those parts systems in their own right (in this case, subsystems[10]) and there are other parts which may be taken to be unitary[11]. Subsystems may overlap — some unitary part may belong to more than one subsystem. So terms are needed for unitary parts, as well as sets of such parts engaging in more complex coordinated behaviour within the system.

1. *A vocabulary of architectural terms (for systems and parts of systems)*

[9] "Documentation" consists at least of descriptions of an engineered system and its intended behaviour, usually on multiple levels from very general ("functional requirements") through intermediate levels (e.g., "functional architecture/specification") down to implementation (the actual system itself). The "levels" are intended to be related to each other through "refinement" and conversely "abstraction". There is not yet agreement on what levels there are or what they are called; whereas refinement is pretty well defined; abstraction is its relational converse.

[10] Although system engineers adhering to the INCOSE terminology use a different term.

[11] "Atomic" is a word philosophers and logicians often use for this, said to derive from a Greek word for "uncuttable". But in electrotechnology applications, especially with modern chip technology, the physics meaning of "atom" surely has priority.

An observation: Currently, in IEC 61508 on E/E/PE functional safety and in the IEC 62443 series on cybersecurity in IACS[12], there seem to be fourteen different terms used for such parts, with various distinguished additional properties (Ladkin 2019).

Second, these parts interact — the system engages in behaviour. Since we are talking of engineered systems, rather than systems which just exist as they are in nature (biological and ecological systems), we can speak of the purpose(s) of a system — it is teleological. Since a system has a particular condition at a particular moment of time (it has a state) and engages in behaviour (a series of events considered together; an event is a change in state of something), the purpose of a system is described using vocabulary appropriate for these states and events/behaviour. Such descriptions are key parts of a teleological system, then. Such an ontology is given in Ladkin (2001).

2. A vocabulary for descriptions of events, states, and behaviour

Teleological systems come with descriptions of (actual or desired) behaviour, but systems and descriptions are very different kinds of thing. The physical constitution of a teleological system is in itself key to its purpose; in contrast, the physical constitution of a description is not — it is not really relevant to the purpose of a description whether it is printed on yellow paper or white paper, size A4 or size A3, whether stapled together, or loosely bound, or held in a folder, or displayed on a computer screen. Descriptions are important for their denotational and semantic content, not their physical attributes. Standard concepts of the semantics of assertions, such as consistency and completeness, expressibility, and so on, are applicable to descriptions of this type.

Third, we have just observed that, in order to deal with teleological systems, we have two categories of thing: system parts themselves and their interconnections; and descriptions. Descriptions are in language; they say things about the system. Given that we have physical objects and descriptions, we can now ask if there is any relation. Yes, we might say, the systems are teleological — we certainly want there to be a relation: a requirements description is supposed to say what people want the system to do (and not to do). So there need not just be system properties and documentation properties but also system+documentation properties, such as concepts, which say how well a system fits its description, or not. Such concepts as "*reliability*" (= it fits, or it mostly fits to some specified degree). Such as concepts which say how characteristics of a system may breach the boundaries of its description ("*emergent properties*"). A technical word in logic for "types of thing" is: *sort*.

3a. A vocabulary of sorts: at least
- *architectural concepts and*
- *descriptions*

Besides system objects, documentation, system and object properties, properties of system-documentation, there is also an environment in which the system operates, generally taken to be a collection of objects which are not part of the system but with which the system interacts (in some of its behaviours, including unwanted behaviour). There are also usually people — assessors, operators, recipients of benefit from system operation, and so on. People may themselves be either individuals or grouped into organisations with specific purposes for, or expectations of, the system. Such people may be real people, or (some of) their interactions may be substituted by robotic agents (for example, telephone switchboards nowadays often do not have human operators). Systems which have functions or sub-functions executed by real people and human organisations are dubbed

[12] IACS = Industrial Automation and Control Systems.

sociotechnical systems. The "socio-" part of a sociotechnical system is generally considered part of the system, so there may be human or robotic agents both within the system operation proper and outside the system, interacting with it. There needs to be vocabulary to describe the environment-system relations and behaviour and the sociotechnical relations and behaviour.

3b. A vocabulary of sorts: including for
- *agents (human and artificial) and their organisation*
- *environment-system relations and behaviour*
- *sociotechnical relations and behaviour*

3.3 Components of a Conceptual Analysis

There are more than these different sorts involved in electrotechnology. They all need commonly-understood terms, a terminology in other words. As we have noted, systems and their parts are important for what they are and what they do; how they are constituted is often (mostly) crucial to their operation. Specifications and descriptions are important for what they say, it is relatively unimportant whether they are pixels on a screen, byte data in memory, or ink on a piece of paper. There are switch mechanisms, temperature, humidity, machine-code programs, bandwidth, assertions, test designs, and operator-cognitive saturation to talk about. These are all fundamentally different kinds of thing, with radically different properties, and different properties we care about. Assertions have logical consistency (or not); switches are not the kind of thing which can have logical consistency. Cognitive saturation is a property of a person (or not), or maybe a robotic agent; machine-code programs are not the kind of thing which can have (suffer) cognitive saturation. Philosophers talk about "categories" of thing, e.g. Ryle's "category mistakes" (Magidor 2019)[13] or "natural kinds" (Kripke 1980); things whose radical differences are to be treated as objective features of them, and not subjective distinctions invented by human observers. As noted above, logicians talk about "sorts". A language and logic which can accommodate different sorts is known as a sorted logic. We have used the formal language of sorted logic (first-order logic with sorts), "LSL", in SemAn (Ladkin et al. 2023).

Is a logic necessary for terminology construction? I would suggest it is. For example, definitions need to be checked for self-consistency. An object (in terminology, mostly a type of object rather than a specific instance) whose definition is self-contradictory[14] does not exist so there would be no point, and no place, in electrotechnical terminology for that definition.

One might suggest that self-contradictory definitions are silly things that will not be proposed by serious engineers. But one cannot necessarily tell that a definition is self-contradictory from its surface construction. In particular, if the definition uses terminology from a logically-formulated mathematical theory, which many terms in electrotechnology do (since much of it derives from the physics of electricity), it may propose something which is inconsistent with that theory, and for most interesting mathematical theories there exists no algorithm which can be relied upon to show it, if so (this is a corollary of various extensions of Gödel's Incompleteness Theorem, in particular one due to Rafael Robinson concerning Q, his "weak" formal theory of arithmetic (Robinson arithmetic. (2023)).

[13] For a much shorter version, see "category mistake" in Blackburn (1994).

[14] Inconsistent" is another term for "self-contradictory" here.

Also, a chain of definitions might well be inconsistent taken as a whole, and it does not take many such definitions to hide a mutual inconsistency effectively. I have experienced something like this. I wrote a conference paper in 1987 which used axioms for a specific theory, proposed by two well-known theoreticians in AI, and derived consequences from it. The paper was published in a prestigious conference (Ladkin 1987a), and went in to a draft of my thesis. When my thesis advisor, Ralph McKenzie, read it, it occurred to him that something was amiss, because the consequences did not match what he thought should be the case. It took him a while to realise where the problem was. One of the axioms was syntactically wrong. I had argued syntactically from the axioms to consequences that Ralph felt could not be what had been intended. Ralph and the original authors had worked from what they thought the axioms should be saying rather than, as I did, from what they in fact said. Anthony Galton published a paper in a prestigious journal analysing the mistake in my conference paper (Galton 1996). It had been of course corrected in my thesis after Ralph had pointed it out (Ladkin 1987b).

Michael Jackson points out (Jackson 2013), with examples, that many sets of requirements for complex systems are inconsistent; even that one can expect them to be inconsistent, given that they are proposed by different groups of domain specialists who do not cross-check each other's usage.

In summary, consistency is currently a poorly-addressed problem. It can be addressed, definitively, through using automated consistency checkers on terminology formulated in LSL (and other logical means).

4. Use LSL, in particular to enable consistency-checking

My colleague Bob Riemenschneider showed that Bertrand Russell's idea of conceptual analysis included what the "arity" of a predicate is (Riemenschneider 1984). The arity of a predicate (the number and sort/type of its arguments) is explicitly exhibited in LFOL[15], whose current notation Russell helped develop. We can illustrate its importance by considering at length the notion of reliability, which is important for electrotechnology.

Reliability means, informally, in engineering that an engineered artefact does what you want; behaves in the way you wish it to behave. Airlines speak of "dispatch reliability"; it means how often an aircraft type can take off on a scheduled flight (if it does not satisfy the conditions for flight, for example some item on the Master Minimum Equipment List (MMEL) is not working, the aircraft may not take off). That a switch is reliable means that it switches a circuit on, and switches that circuit off, when it is activated so to do. Thus described, these are both on-demand functions: an aircraft dispatch (= take off into flight) is a discrete event, as is activating a switch.

An example of continuous-function reliability is the steering of a car. The activation of the steering wheel in the driver's compartment activates a change in angle of the steered road wheels, and there are constraints on the way it is done, so as to fulfil what the driver expects.

5. Determine the arguments (components), their sorts, of a concept, and thereby its arity

Systems are built from components and parts, and can become very complex (modern military and commercial aircraft are built from hundreds of thousands of parts, or more). Physical parts with a function wear out when, for example, they lose matter during use and thereby change shape. When they wear out, they cease to function in the intended way.

[15] The language of first order logic

And they wear out at different rates. How do you keep a system running, when all of its hundreds of thousands of parts have different wear-out behaviour? There is a technique to keep track of these situations, called FMEA[16] (Carlson 2012), which has been very successful in increasing the "dispatch reliability" (as above) of, for example, complex vehicles and aircraft.

Suppose we are to introduce a technical engineering term "reliability" that is supposed to reflect this high-availability facet of usability. The phenomena described above are important — we want our artefacts to behave in the way we want, and we want to develop techniques such as FMEA to enhance this if we can, so we do need to instantiate this concept somehow. As described above, dispatch reliability is a value property (called a fluent in symbolic AI[17]), which has a value usually measured in per-cent. Here, we already have a formal choice to make: could it be a Boolean property which something either has or does not have? The answer is that, purely formally, it does not matter[18]. So there is one result of conceptual analysis: a particular choice of representation is formally inconsequential. This observation is the result of considering the representation of a concept in a formal language.

Considering further the example of "dispatch reliability", or reliability in the FMEA sense, a system (a system part) can be generally expected to work for a time, and then wear out. We could, if we like, gather data on this. We put a switch on a rig which switches it on and off continually and see how many times this can be done before it mostly no longer works. We can do it for lots of switches, so we can estimate an "expected operating life" of the switch type: we can expect the switch to operate for N demands before it doesn't. So, if we install such a switch, can we expect it to operate for (N-1) demands correctly, and then swap it out for a new one? No, some will quit earlier and some will carry on working for more than N demands. So, next observation: we are in the realm of statistics, and statisticians have a good intellectual handle on all this, with their set of concepts which work. We can use them if we wish. Statisticians tell us, after our tests, that we can expect to the kit to work for N demands to a particular *level of confidence*. For example, if N is the (true) mean, then our confidence should surely be 50%. But we can mostly never get at the true mean: we just have our tests, and can estimate the mean from those tests, along with an expected error (or, again, confidence). Connecting statistical-parameter values with confidence in this way is quite well developed — confidence theory for classical statistical inference stems originally from Jerzy Neyman in the 1930's (Neyman 1937).

Note at this point that we are beginning to diverge from what a philosopher would do. A philosopher would say: what are statistics? How are our inferences justified? Is an "expected value" an objective thing, or a mental construction (or both or neither)? Are we Bayesians, for which the numbers tell us our best guess modified by experience, and are thereby subjective[19]; or are we frequentists, for whom the mathematical parameters of a statistical distribution have an objective presence out there in the world? Or are we Laplacians, for which the propensity of a die to come up six is a property on a par with the

[16] Failure Modes and Effects Analysis

[17] See https://en.wikipedia.org/wiki/Fluent_(artificial_intelligence). Accessed 26th January 2024.

[18] We can trivially turn any value predicate into a Boolean predicate by adding an extra argument for its value: when f(x,y,z) = a, we can reformulate as f'(x,y,z,a) = TRUE, along with a condition that f' is functional in its fourth argument: (for any x,y,z)(f'(x,y,z,a) && f'(x,y,z,b) → a=b). And vice versa; any Boolean predicate with at least one functional argument can be turned into a function with one argument fewer.

[19] Bayesians speak rather of "critical interval" rather than "confidence" or "confidence interval". The meaning of critical interval is arguably a more intuitive notion of confidence than the Neymanian version. The reason for the divergent vocabulary is clarity. Neyman bagged the term "confidence" first. Others with a different idea needed a different word.

colour of the shirt I am wearing, which is grey (and not yellow, and not blue). We don't do that in engineering. We say: statistics, well developed, great, let us use it.

It follows that there are at least a number of different sorts in this definition. We have the kit itself. We have some idea of an intended/expected function. We have a number of demands, or a period of time. We have an expectation. And we have a confidence in that expectation. All this, although we are not yet very far into our analysis. Next point: it is well to keep track of all the sorts which are hanging around.

Notice also that we are talking about things we can see and test. Suppose we were to try to connect this concept of reliability with Laplacian propensity: say, the reliability of a six-throw of this die is its propensity to come up six when thrown. We can throw it any number of times, and register the proportion of sixes which arise. Is that the propensity? Surely not, for I get a different proportion on the very next throw (no matter what the result), so the propensity would have changed without anything concerning the constitution of the die having changed in any non-negligible manner, whereas the propensity is supposed to be a property of the die which does not change if the constitution of the die has not changed in any non-negligible manner. It follows that we cannot identify propensity with observed proportion. Even if it is not directly observable, is there some god who will tell us in our dreams what the propensity really is? If there is one, that does not appear to be the way she chooses to work.

It turns out to be hard to connect propensity with any observable property, which is likely why statisticians and probability theorists themselves have given up on the concept. We have Bayesian subjectivists, who say probability is "*your best guess, modified by experience*", and frequentists, whose calculations follow the Humean idea of constant conjunction: run the tests for long enough and limit theorems tell you numbers converge; the limit number is the parameter of interest. But there are no (coherent) Laplacian propensitivists. We want our concepts and calculations to help us make a difference: to help us make this kit work more often, or better. We need to do stuff and observe the effects. Observable effects may lead us to useful concepts that are not themselves directly observable but, to be useful, their values will be manifest in observed/observable effects. Engineers have no use for Laplacian propensity. This might be another point of divergence from philosophers (although there have been and are philosophers who propose that any meaningful concept must be manifest somehow in observable effect — the so-called logical positivists, for example. But they, as well as Popperian refutationists, had a problem explaining how mathematics is thereby meaningful. As well as a problem determining what constitutes "observable"). It might well be that we can say that the engineering approach to meaningfulness is broadly that of logical positivism: concepts useful to engineering are based as far as possible on (naïvely) observable properties. So, another point of conceptual analysis: what is observable, directly and indirectly? Is everything we define based on direct or indirect observability? Do we have any hidden metaphysical notion such as propensity? (If so, let us get rid of it.) Let me call that notion d/i-observability.

6. Use, as far as possible, d/i-observable terms

To determine the reliability of the kit, then, the behaviour of the kit must be observable in such a way that we can say whether it is performing its intended function. We have just looked at observability. Let us look at some of these other terms more closely. "*Performing*", for example. Could we substitute with "*behaving*"? I take "*behaviour*" to be a logically definable term, as in say Ladkin (2001). We can surely say "*behaving according to its intended function*" and mean the same thing as "*performing its intended function*". Here is another point of conceptual analysis, a sort of Occam's razor. Build

concepts as far as possible on what is already well-defined; "new" concepts (such as "*performing*") shall be defined. This entails that concept definition be iterative, as far as possible.

What about "*intended function*"? Here it gets a little tricky.

3.4 Intended Function: An Example

A recent story — it is a little involved, but please bear with me.

The telephone connection of my housemate does not always work (she has a DSL connection for Internet and a WiFi access point, as well as DECT telephone service, all in the same box). There are access points/junction boxes attached to the outside of buildings, called APLs[20]. The telephone-system cabling up to and including the APL is the property of and responsibility of the network operator (pervasively Deutsche Telekom); the system cabling into the building and to the end-devices (telephones and other devices) is the property of and responsibility of, generally, the building owner.

First, a bit of topology (actually topography, but in telecommunications networks it is usually called topology). See Figure 1. My neighbours have an APL which I can see from my office. They are on Road y (Ry). Their house is, say, House v (Hv). My housemate's house line is connected to an APL which I can see to the right if I lean out of my office window on the first floor. She is on Connector 7 of that box. That building, House z, and thus the street address of the APL, is also on Ry.

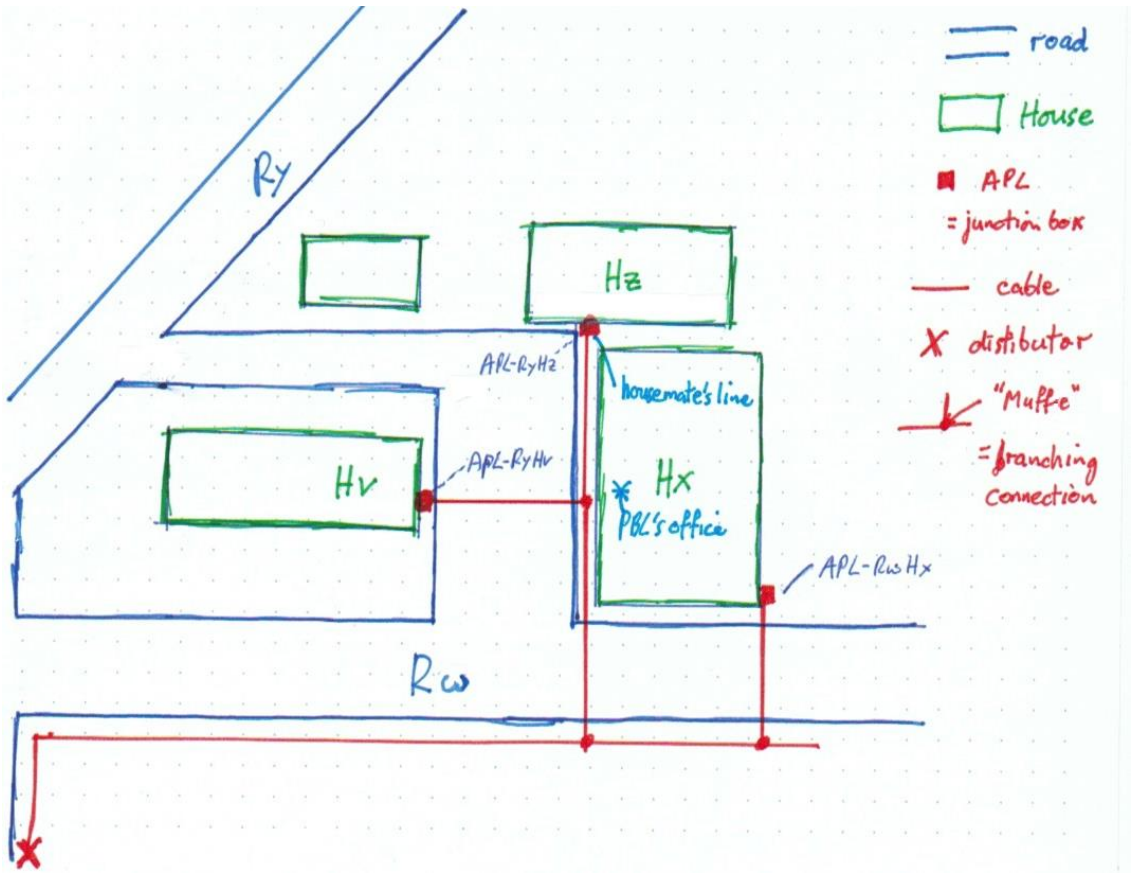

Figure 1 ~ The Street Telecommunications Connection Topology

[20] APL = Abschlusspunkt Linientechnik

I am not on Ry. My house has an address on a different road, Rw. My APL is on the other side of my house from my office, and my two lines, both on Connector 1, run in through the cellar to a point on the ground floor in the SE corner of the house directly below my office, where the Causalis router and WiFi sits. My address is, shall we say, Rw House x (RwHx), which is also the street address of my housemate as well as of my APL. However, my housemate's APL RyHz is attached to a building whose street address is on a different road, namely Ry. The APLs are connected to a grey distributor box on the sidewalk of a third road some 50 metres away. A cable runs from that distributor to a point on the opposite sidewalk to my house on Rw, and runs beyond that further along Rw. There is a branch point opposite my house from which a cable runs past my house under my office window to the APL at RyHz (it also branches under my window to the neighbour's APL on RyHv).

Every so often, my housemate's Internet/phone connection has ceased to work. She has called the provider (BITel, a branch of the city utility company) to file a service difficulty. They check the line in real time, which is displayed, but they do not see her modem/router. This happens because, every so often, a Deutsche Telekom service engineer has come out to work on something at the distributor box, somehow has seen my housemate with registered street address RwHz connected somewhere else (namely RyHz Connector 7), and has then reconnected to APL-RwHx (usually Connector 2). I recall this happened three times in a particular eight-month period.

The service provider BITel contracts with Deutsche Telekom, as it must, for service using Deutsche Telekom's already-installed hardware. The “last mile” infrastructure up to and including the APLs belong to Deutsche Telekom, so Deutsche Telekom gets to do what it wants with them and theoretically neither BITel nor I are formally allowed to unscrew the APL lid to find out what is going on. But ... we have X-ray eyes. Besides, this is repeating behaviour.

The final time, we had three engineers out to check: Deutsche Telekom, then BITel, then Deutsche Telekom again. A Deutsche Telekom engineer came out to check the lines. He appears to have made one mistake, which is that he checked APL-RyHz and determined there was no connection to my housemate's router, whereas there is, on Connector 7. He went to my APL-RwHx, observed there was a live connection to Connector 2, connected his equipment, and determined that that was indeed the connection associated with my housemate's BITel account.

And now the point of this story. Deutsche Telekom contracts to provide a connection to an APL associated with a street address. The street address of my housemate is RwHx. That is where she is connected. For Deutsche Telekom, that connection and service is fulfilling its intended function. It follows (per IEV definition — better said, the “preferred” IEV definition) that it is reliable. As owner of the building, it is according to Deutsche Telekom my responsibility to provide a line from APL-RwHx to my housemate's apartment. I do provide a line, conformant with my responsibility, and APL-RwHx is *not* where that line is. That line goes to APL-RyHz, and has done since long before I owned the property. Since that line was not connected to the Deutsche Telekom network (that is, to the distribution box), according to BITel and my housemate and the contract, she is not receiving reliable service.

So who is right? Deutsche Telekom claims it is providing reliable service; BITel and my housemate claim it is not. The facts “on the ground” are the same for both, and both are right according to their reasoning. But what they claim is contradictory. Can this really be

so? Is reliability really so subjective? Do we really need paraconsistent[21] logic to describe the reality of daily life?

Obviously not. Deutsche Telekom and BITel/housemate have different interpretations of "intended function". Deutsche Telekom thinks "intended function" is providing a live line to the APL at the street address. BITel/housemate think "intended function" is providing a live line to the APL where my housemate's telephone line is connected.

This demonstrates that the concept of "intended function" must be unambiguous in order to have a workable concept of "reliability", namely one in which all engineers ascribe the same reliability properties to the exact same world state.

The story of course was resolved. Out came a BITel engineer to verify the topology; he then put in a request to Deutsche Telekom to connect my housemate's account back to APL-RyHz Connector 7; who sent an engineer the next day to do so. End of story. It's worked for a couple of years now.

3.5 Unambiguous Specification

There is an existing engineering term for "description of intended function such that all (rational, non-delusional, observation-capable) engineers ascribe the same meaning to that description in a given state of the world". It is *unambiguous specification*.

Furthermore, according to the observability condition elucidated above, that unambiguous specification shall involve only terms which are d/i-observable.

It is obvious in the story in Sub-section 3.4 that there are two descriptions of intended function, that these descriptions involve only d/i-observable phenomena (via the engineers' signal-generators and reception devices), and that these descriptions are different. There is no unambiguous d/i-observable specification of the telecommunications service. It follows that there is no way of ascertaining the reliability of that service.

From this observation, we can derive the principle:

> *7. Descriptions shall be, as far as possible, unambiguous d/i-observable specifications*

Where are we so far? We have devised seven principles, as well as some observations about the notion of reliability (as an example of what we take conceptual analysis for engineering to consist in).

The observations we have made about the notion of reliability are:

- There is engineered-kit, K, an artefact, to which we wish to ascribe a reliability, loosely an ability to function
- Such reliability is helpful as a value parameter: some kind of proportion of delivered-function to all actuations
- The value is dependent on a temporal parameter: number of demands (since new); hours of operation
- There must be an unambiguous d/i-observable specification of the function
- Various sorts are involved in an ascription of reliability to the kit K.

[21] Paraconsistent logic allows contradictions. In order not to be technically trivial, it must give up on the usual classical inference rule of "*ex falso quodlibet*": that from a contradiction, anything follows. In symbols, FROM (A && NOT A) INFER B, where A and B are arbitrary proposition symbols (called "propositional variables" in formal logic).

To determine an ability to function, one must be able to determine, for an observed behaviour within the range of behaviours of interest, whether it is consistent with the specification or not.

This leads to a further condition, on the kit K, that behaviour relevant to the function be d/i-observable, otherwise no comparison with a d/i-observable unambiguous specification of that function is possible. Also, there is a condition on the specification, that inference from the specification be relatively easily performed, for relevant behavioural characteristics. These conditions should be kept in mind when devising a definition of the term *reliability*. They follow as indicated from the loose conception *ability to function*, so they are strictly speaking part of the ConcAn of the term *reliability*. However, one could obviously formulate a general principle that:

> *8. As far as possible, where a term is defined in which an artefact is to be compared with a specification, the characteristics of behaviour coming within scope of the specification shall be d/i-observable, and the inferences from the specification concerning those characteristics shall be relatively easy.*

4 ConcAn Principles and the Definition of Reliability in IEV 192-01-24

4.1 The Principles

The principles elucidated in Section 3 are:

1. There is a vocabulary of architectural terms (for systems and parts of systems)
2. There is a vocabulary for descriptions of events, states, and behaviour
3. There is a basic vocabulary of sorts: at least:
    1. architectural concepts
    2. descriptions
    3. agents (human and artificial) and their organisation,
    4. environment-system relations and behaviour
    5. sociotechnical relations and behaviour
4. Use LSL, in particular to enable consistency-checking
5. Determine the arguments to (components of) a concept, their sorts, and thereby its arity
6. Use, as far as possible, d/i-observable terms
7. Descriptions shall be, as far as possible, unambiguous d/i-observable specifications
8. As far as possible, where a term is defined in which an artefact is to be compared with a specification, the characteristics of behaviour coming within scope of the specification shall be d/i-observable, and the inferences from the specification concerning those characteristics shall be relatively easy.

The definition of general *reliability* in the International Electrotechnical Vocabulary (IEV n. d.) is in Part 192, entry 192-01-24:

> *ability to perform as required, without failure, for a given time interval, under given conditions*

There are other definitions. The full list of definitions of reliability in the IEV is given in Appendix A. I shall consider variations below, after the initial analysis of 192-01-24.

4.2 Redefining Reliability Conformant with the Conditions

Let me call the terms *for a given time interval* and *under given conditions* the *auxiliary constraints*. Looking at the terms used, we have:

- ability
- perform
- as required
- failure
- the auxiliary constraints

According to Principle 5 of ConcAn, then, we need to establish what sorts are associated with these terms/phrases (including of course the auxiliary constraints).

We note that there is nothing about

- a measure
- a measured value
- (inferred parameter) the confidence in the measured value
- a specification
- what success or failure is
- what one can say about on-demand functions, for there seems to be no notion of *demand*, just that of *time interval*

There are some formal strictures required by the IEC terminology guidelines. *Reliability* is an *-ity*, a noun, its transcription as a definition must be more or less substitutive, that is, one should be able to replace any occurrence of the term *reliability* in an engineering assertion with its definition *ability to perform …* and retain the self-same meaning.

To analyse what is here being said, one might wish to broaden the syntactic categories used. Let us look at an adjectival form:

> Artefact K is *reliable* <in conditions, over a time interval> if and only if it is *able to perform* <in those conditions, over that time interval> <according to precept: namely, *as required, without failure*>

So ascribing an *ability* to K, as definition 192-01-24 seems to require, disappears when the syntactic form changes. The term *ability* is simply an artefact of the syntactic guidelines for IEC terminology.

Let us look instead at the phrase *able to perform*. When I say, “I am able to cycle into town now”, I do not mean, “I am cycling into town now”. I mean something like, “If called upon to do so, I will (successfully) cycle into town now”. Providing of course that my bike does not have a puncture, and that I don't have a stroke or a heart attack in the next little while (the auxiliary constraints). And I also don't mean “right now, this very second”, because I don't have my cycling shoes or helmet on, and my bike is still in the shed, locked up, so I would have to prepare, which takes a little time. So I mean <over a time interval>, the time interval being appropriate for the required preparation and execution of the action. So the inclusion of the auxiliary constraints <given conditions> and <given time interval> seem intuitively consonant with common usage of a term such as *able to perform*. We may conclude: the auxiliary constraints are appropriate for the intended use of the phrase *able to perform.*

What about the term *perform*? In common usage, it has something to do with expectation (of others). You *perform* when you are trying to execute some kind of behaviour of an

expected variety (by others). A play, a piece of music, a series of jokes at a microphone, taking part in a game. That expectation is implicit in 192-01-24, in the term *as required*: if something is required, surely there is a requirement?

It turns out we have all the terms to describe this already, in our basic vocabulary in the principles. *Able to perform as required, without failure* is nothing more or less than *behaves conformant with its specification*. (To get this to work, though, we need to presume here a condition on on-demand functions that a specification of an on-demand function allows dormant behaviour, namely that there is no specification-relevant state change when no demand is present[22].)

Using principles of ConcAn, namely 1, 2, and 3, we have succeeded in paraphrasing the IEV definition of *reliability*:

> *behaviour conformant with its specification, over a given time interval, under given conditions*

Let me call this definition *ConcAn-modified-192*. We have fulfilled Principle 5 in that we have basis sorts; an additional sort over the phrasing in 192-01-24, explicitly introduced, namely that of *specification*, which is also a basis sort, and whatever sorts are associated with the auxiliary constraints. We have the sorts:

- behaviour (a basis sort)
- specification (also a basis sort)
- the sorts of the auxiliary constraints

This definition is clearly Boolean. K is reliable (or not) under the auxiliary constraints.

The list of matters about which I noted above there was "nothing" explicit in the 192-01-24 definition can be revised. Specification and failure have been dealt with in the revised definition. The notion of time interval does not refer to what kind of behaviour (on-demand or continuous) which K exhibits, but rather the scope of the attribution of reliability, the period of time over which observations pertinent to reliability are made (this why this is part of the auxiliary conditions, but I still have to say what auxiliary conditions are).

4.3 Variations

We have:

- Reliability is an "ability" (most definitions) or a "probability" (192-05-05, 444-07-01, 448-12-05). These are fundamentally different notions, and thereby sorts. We have dealt with the term "ability" above; we shall consider "probability" below. What we can conclude in any case is that, even within IEV Section 192, "reliability" is a homonym, because two definitions of it attribute it to two different sorts. Homonyms are, however, excluded by IEC terminology guidelines. This is not an issue for ConcAn, though. Both ConcAn and SemAn are (I claim), *inter alia*, means of discovering synonyms and homonyms where they might be concealed. Here, that "reliability" exhibits homonyms is apparent on the surface.

[22] This is a principle of on-demand functionality, it is not a principle of terminology or ConcAn. We could aim to try to turn it into a terminological issue by using it explicitly in the definition of "*on-demand function*". But if we did that, we would need a further definition of "*intended-to-be on-demand function*" which we can call any function which reacts on demand, but which doesn't satisfy or cannot be shown to satisfy the statis-on-no-demand condition. Turning it into terminology does not avoid the issue that the condition is (meta-)physical, not terminological.

- How the "item" shall operate: "perform as required" or "perform a required function". One could discuss whether performing "as required" is broader in scope than performing a required function, for example, there might be additional properties of a performance which are desired/required other than that of executing a function. For example, that a programmable-electronic chip shall not heat up beyond a certain point when performing its required calculations. It is not strictly speaking a function that it shall not heat up, but we can certainly make such a requirement. I have analysed the definition using the possibly broader scope, and suggest this suffices for our purposes here.
- The auxiliary conditions are "given..." (most definitions), or they are "stated..." or "specified..." (the two definitions from Section 603). It would be very much a secondary issue to inquire whether these identifiers for means of expression all have the same meaning. More important is for the auxiliary conditions to be explicitly expressed. I do not pursue this further here.

The matters in the list which are not dealt with in the new ConcAn-modified-192, which (I claim) is semantically equivalent to that in 192-01-24, are *measure* and its *value*, thereby necessarily introducing a *confidence* in the value. This is the "probability" concept given in 192-05-05 and 444-07-01.

There is, of course, also a confidence involved in assessing whether behaviour conformed to specification under the auxiliary constraints — not everything may have been as practically observable as we might have wished, but this is not intrinsic to the definition, it is a consequence of empirical connection with the world in general. In contrast, the *confidence* involved in a measure of reliability is intrinsic to the use of the measure: for the self-same set of observations, there are different measure values associated with different confidence levels (in fact, an infinite set of pairs of <value, confidence>).

Conformant with the notion of "dispatch reliability", and indeed the notion of software reliability as construed by those who study it, as well as in other engineering contexts (Bedford and Cooke 2001, Section 3.2, p41), we might wish to say that reliability is rather something like:

> *over a given time interval, under fixed auxiliary conditions, the proportion of time (for continuous processes) or the proportion of demands (for on-demand processes) for which the ConcAn-modifed-192 is fulfilled, along with the confidence in this measure.*

Let me call this *measure-reliability*. Rather than being a Boolean value for given auxiliary conditions, as ConcAn-modified-192 is, the measure-reliability of K has type:

> (<auxiliary conditions>, <a proportion or percent>, <confidence>)

It should be clear that measure-reliability, which is just called "reliability" by statisticians and people who calculate it, is a pervasive concept in reliability engineering. Here a quote from a major textbook in the field (Birolini 2014, p1):

> *The expectation today is that complex equipment and systems are not only free from defects and systematic failures at time t = 0 (when they are put into operation), but also perform the required function failure free for a stated time interval and have a fail-safe behaviour in case of critical or catastrophic failures. However, the question of whether a given item will operate without failures during a stated period of time cannot be simply answered by yes or no, on the basis of a compliance test. Experience shows that only a probability for this occurrence can be given*

Indeed, measured-reliability is used in IEC standards. Tables 2 and 3 of IEC 61508-1:2010 give Safety Integrity Level requirements on random failures in terms (almost) of measure-reliability. What is missing in those tables is the notion of confidence. Over a given time interval, it is possible to be almost completely confident that <under auxiliary conditions> the function will execute correctly at least once, and at the same time have zero confidence that it will correctly execute all the time (respectively, on every demand). Indeed, this is the case with most software, and *ipso facto* with most devices which are software-based, which is the category of devices with which IEC 61508 is explicitly concerned. In the (misleading, and in part incorrect) explanation of statistical evaluation of the operational history of software in IEC 61508-7:2010, Annex D, Table D.1 gives measured-reliability conditions for both on-demand and continuous functionality, and attempts to relate it to safety integrity levels (SILs) — and also includes "confidence level". So it is clear that measured-reliability is relevant to electrotechnology, at least to safety. Indeed, a Software Safety Integrity Level is defined in IEC 61508-4:2010 Subclause 3.5.10 as a *measure of … confidence*…. So the notion of *confidence* specifically occurs. Here, again, is Birolini on the reliability of electronic components (Birolini 2014, Section 3.1.6 Reliability, p86):

> *The reliability of an electronic component can often be specified by its* failure rate λ. *Failure rate figures obtained from field data are valid if* intrinsic *failures can be* separated *from* extrinsic *ones and reliable data/information are available. Those figures given by component manufacturers are useful if calculated with appropriate values for the* activation energy…… *and* confidence level….

We may conclude that the definition of reliability in IEV 192-01-24 leaves a lot of questions open, and is not adequate to all the reliability concepts used in IEC standards, in particular those in IEC 61508. We might think that 192-05-05, measured-reliability, satisfies these additional needs: the probability of performing as required under the auxiliary conditions.

With "probability", though, we come up against Principle 6 of ConcAn. It should be d/i-observable. However, in any practical case we can only estimate it to a given level of confidence, as the quotations from Birolini (2014) indicate. The definition 192-05-05 gives no hint that, to fit any one given situation (collection of data), a variety of estimates of probability, each with a different confidence level, can be given. It may be disputed whether a definition is the correct place to say how a presentation of the item in question should look, but as a practical matter it could be hinted in a note that any given probability can only be an estimate, and needs to be accompanied by a confidence level.

This concludes this example of ConcAn (for now). It remains to say something about auxiliary constraints and the role they play in electrotechnical definitions, and thus in ConcAn.

5 Auxiliary Constraints — A Final Condition

Many concepts are general in that they apply to many sorts of thing. The concept of *reliability*, for example, applies to cars, software, and operator perceptions in a chemical plant. A statement of reliability of a car will be subject to certain constraints: the temperature outside, the road condition of the road or other surface on which it travels, the amount of water on the road (most cars do not do well in more than a few centimetres). A statement of reliability of a jet engine will include the flow of water it may ingest, as well as a mass of birds it might resiliently shred. A statement of reliability of software will

include none of those physical constraints. It may simply be conditioned on the ConcAn-modified-192 reliability of the hardware on which it is running. Reliability of operator perceptions will be conditioned on fatigue, biorhythmic parameters, perceptual capacity (acuity of eyesight, for example).

This leads to the notion of *auxiliary constraint*: conditions specific to the sort, as well as the branch of engineering, under which the term is to be used.

The reliability of a piece of kit K can only be made sense of when K is operational, so a general constraint is that one can only meaningfully talk of the reliability of K over at most its operational lifetime, and not beyond. This lifetime will likely include periods when K is not operational, for example during maintenance of K. During these periods, it also does not make sense to talk of the reliability of K[23].

Since the auxiliary constraints are dependent on the sort of the object to which the term is being applied, it does not necessarily make sense to list them when giving a general definition. However, it should be said that there do exist sort-specific auxiliary conditions for the definition to be applicable.

> *9. Where a definition is applicable to many different sorts, and the conditions under which the definition is applicable differ from sort to sort, the phrase "under sort-specific auxiliary constraints" or some equivalent ("under given conditions") should appear in the definition*

6 Matters Not Dealt With in (Current) ConcAn

There are some important issues in terminology which are not addressed, or not addressed adequately, by the ConcAn principles that have been formulated here. Here are some.

6.1 Goal Use Versus Actual Use

When defining a concept, the definer usually has some idea of why, wherefore, and how she intends the term to be used. This may or may not reflect the way in which electrotechnologists actually use the term (if it is already in use). Indeed, if the term is in use, it may well have different meanings to different users, in which case fixing on even one of those meanings, which is what a terminological definition does, inevitably alienates all other uses[24].

If those uses "in the field" are unknown, then they can sometimes be detected using machine-learning techniques on restricted corpora (namely, engineering documents in use) (Arndt and Schnäpp 2018). This is a key result of Project Harbsafe[25] (within which the initial work on ConcAn was performed). Two issues in applying such techniques are:

- the definition of a large-enough domain-specific corpus (Project Harbsafe used selected IEC documents in cybersecurity and safety; it is not clear at time of writing which corpus size is "large enough")

[23] It may be, though, that the reliability of the overall system S of which K is part is important during periods in which K is not operational (is undergoing maintenance, for example). So it may be important for the reliability of S that the function of K is substituted for during K's "down time"

[24] …and users.

[25] See Acknowledgments, below

- the acquisition of enough volunteers to render judgements which enable reliable results from the machine-learning techniques

ConcAn does not employ such techniques; it is intellectual/symbolic analysis.

Sometimes, divergent use "in the field" is known. The authors of IEC 61511:2016, the process-industry-specific specialisation of IEC 61508, have noted the following divergences of their terminology from that of IEC 61508, explicitly because of common usage in their field. Many of these are key terms!

- 3.2.1 architecture
- 3.2.26 functional safety assessment.
- 3.2.29 hardware safety integrity.
- 3.2.56 process risk. A synonym for "EUC risk" in IEC 61508.
- 3.2.57 programmable electronics.
- 3.2.64 redundancy
- 3.2.67 safe state
- 3.2.69 safety function
- 3.2.73 safety integrity level
- 3.2.75 safety manual
- 3.2.79 software
- 3.2.84 system
- 3.2.91.1 type A device
- 3.2.91.2 type B device

Technically, these terms are thereby homonyms in the IEC corpus. As noted above, IEC terminology guidelines say that homonyms shall be avoided: these homonymic variant definitions are intentional, and occur within the responsibilities of one IEC Subcommittee, SC65A. ConcAn currently implements no proposals or guidelines for how to deal with deviant usage based on practicality.

6.2 Coherence

ConcAn recommends the use of LSL, and (semi-)automated proof checking, to check for consistency of a definition/mutual consistency of groups of definitions. But currently ConcAn includes no guidelines as to how to pick candidate (sets of) definitions for consistency analysis. It is left to the analyst's thoroughness and judgement.

6.3 Efficacy and Coverage

A key question in devising terminology is whether all technical questions related to a concept (or set of concepts) allow themselves to be concisely expressed using the concept (set of concepts). For example, I had observed confusions generated in discussion through and about use of the technical definitions concerning harm, risk and safety in IEC 61508 and devised my own set of definitions which I felt avoided the problems (Ladkin 2008).

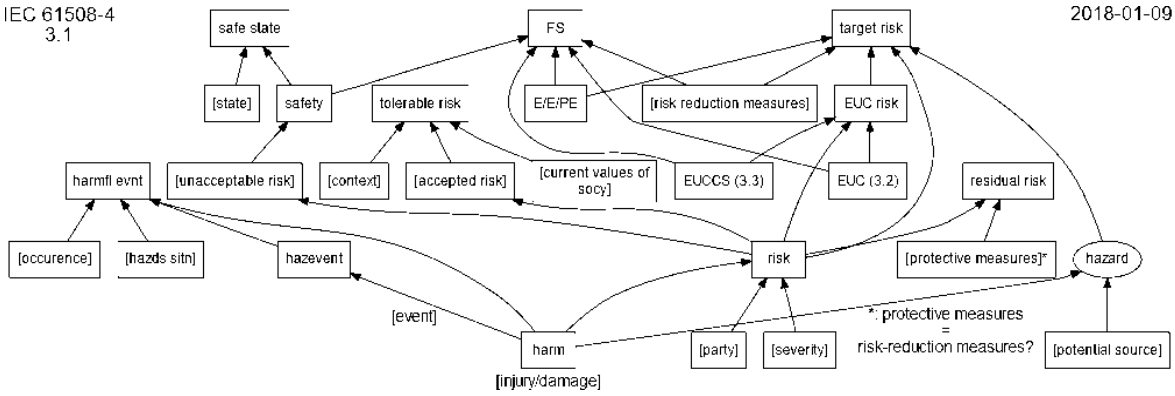

Figure 2 ~ Semantic Dependency Graph of the Terminology in IEC 61508-4 Subclause 3.1

Semantic dependency graphs (SDGs) indicate a more efficient use of terminology. These are discrete directed graphs (composed of nodes and directed edges between them) in which a node represents a term, and a directed edge from the node labelled A to the node labelled B indicates that the term "A" occurs in the definiens of term "B". Figure 2 shows the semantic dependencies in this terminology in IEC 61508-4 Subclause 3.1.

Figure 3 shows the semantic dependencies amongst the similar terms in Ladkin (2008), with some terms grouped (a "high-level" SDG).

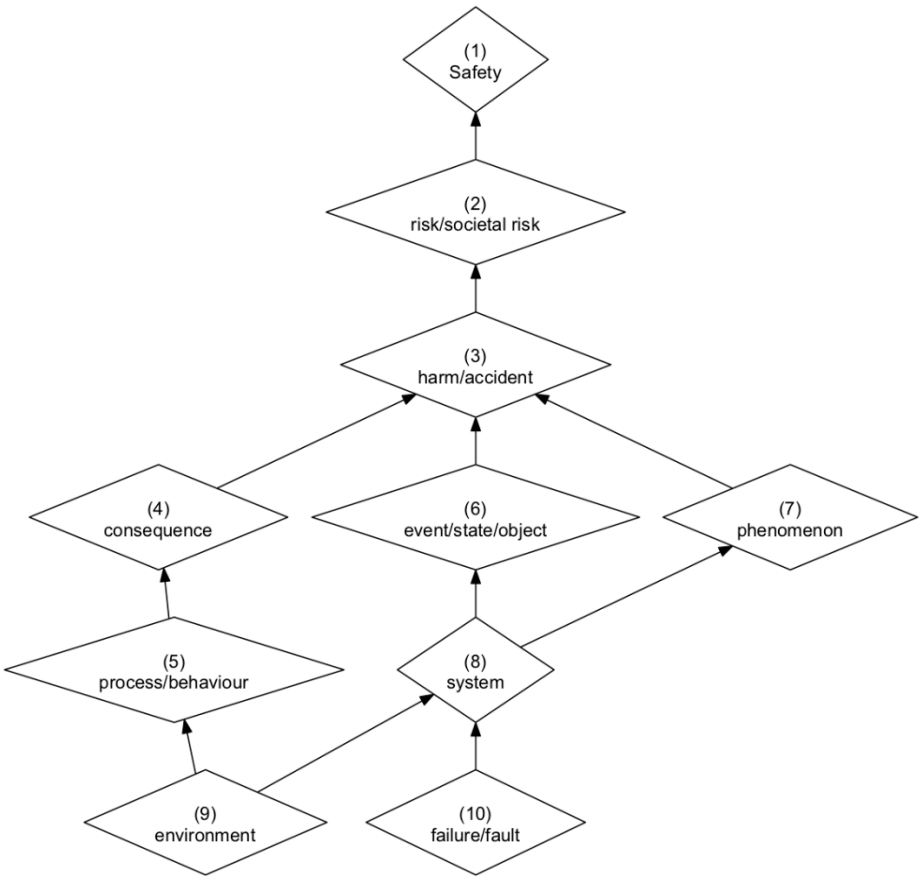

Figure 3 ~ High-level SDG of the Vocabulary of Ladkin (2008)

ConcAn currently provides no mechanisms or guidelines for assessing efficacy or coverage.

7 Summary

Conceptual analysis is a term from philosophy with varied meanings. I have argued that some of the varied techniques are applicable to electrotechnological vocabulary, and I call this adaptation ConcAn. I have illustrated ConcAn most simply on a specific IEV term, 151-11-03 *electric*, and devised a collection of principles under which ConcAn proceeds by considering the IEV term 192-01-24 *reliability*. These principles (so far) are:

1. There is a vocabulary of architectural terms (for systems and parts of systems)
2. There is a vocabulary for descriptions of events, states, and behaviour
3. There is a basic vocabulary of sorts: at least

    1. architectural concepts
    2. descriptions
    3. agents (human and artificial) and their organisation,
    4. environment-system relations and behaviour
    5. sociotechnical relations and behaviour

4. Use LSL, in particular to enable consistency-checking
5. Determine the arguments to (components of) a concept, their sorts, and thereby its arity
6. Use, as far as possible, d/i-observable terms
7. Descriptions shall be, as far as possible, unambiguous d/i-observable specifications
8. As far as possible, where a term is defined in which an artefact is to be compared with a specification, the characteristics of behaviour coming within scope of the specification shall be d/i-observable, and the inferences from the specification concerning those characteristics shall be relatively easy.
9. Where a definition is applicable to many different sorts, and the conditions under which the definition is applicable differ from sort to sort, the phrase “under sort-specific auxiliary constraints” or some equivalent (“under given conditions”) should appear in the definition

~

Correspondence Address

Corresponding e-mail address: ladkin@causalis.com.

Acknowledgments

The initial work on ConcAn was performed 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. Causalis Ingenieurgesellschaft worked in Harbsafe as a subcontractor to the Technical University of Braunschweig.

References

Arndt S. and Schnäpp D. (2018). *Harbsafe-162 — A Domain-Specific Data Set for the Intrinsic Evaluation of Semantic Representations for Terminological Data*. Preprint submitted for publication, Technical University of Braunschweig IVA — Institute for Traffic Safety and Automation Engineering, 2018.

Beaney M. (2003). *Analysis*. In: Stanford Encyclopedia of Philosophy. 2003, revised 2014. Available from https://plato.stanford.edu/entries/analysis/. Accessed 27th July 2023.

Bedford T. and Cooke R. (2001). *Probabilistic Risk Analysis*. Cambridge University Press, Cambridge.

Birolini A. (2014). *Reliability Engineering: Theory and Practice*, Seventh Edition, Springer-Verlag, London.

Blackburn S. (1994). *The Oxford Dictionary of Philosophy*. Oxford University Press, Oxford.

Carlson C. S. (2012). *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis*. John Wiley & Sons, Hoboken NJ.

Collins J., Hall N., and Paul L. A. (editors). (2004). *Causation and Counterfactuals*. MIT Press, Cambridge, MA.

Fodor J. (2004). *Water's water everywhere; Review of Hughes on Kripke*. London Review of Books 26(20), 21 October 2004. Available from https://www.lrb.co.uk/v26/n20/jerry-fodor/waters-water-everywhere. Accessed 27th July 2023.

Galton A. (1996). *Note on a Lemma of Ladkin*. J. Logic and Computation 6(1):1-4, February 1996.

IEC61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. IEC 61508, in 7 parts, 2nd Edition, 2010. International Electrotechnical Commission, Geneva.

IEC61511. (2016). *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements*. IEC 61511-1, 2nd Edition, 2016. International Electrotechnical Commission, Geneva.

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

IEC Glossary. (no date). *IEC Glossary*. International Electrotechnical Commission. Available from https://std.iec.ch/glossary. Accessed 29th July 2023. In particular, the entry for "reliability" as in 191-02-06 is available at https://std.iec.ch/terms/terms.nsf/3385f156e728849bc1256e8c00278ad2/b73f2f0202273857c1257c46004f0134?OpenDocument. (Note that there are many other entries for "reliability", and that this particular entry may not be found by using the internal searching techniques of the Glossary.)

IEV. (no date). *International Electrotechnical Vocabulary*. International Electrotechnical Commission, IEC 60050. Available from https://www.electropedia.org. Accessed 29th July 2023.

Jackson M. A. (2013). *Topsy-Turvy Requirements*. In: Meyer B. (editor). *Modelling and Quality in Requirements Engineering : Essays dedicated to Martin Glinz on the occasion of his 60th birthday*. Verlag-Haus Monsenstein u. Vannerdat, Münster.

Kripke S. (1980). *Naming and Necessity*. Blackwell, Oxford.

Ladkin P. (1987a). *Models of Axioms for Time Intervals*. Proceedings of AAAI-87. The Association for the Advancement of Artificial Intelligence. Available at https://www.aaai.org/Papers/AAAI/1987/AAAI87-042.pdf. Accessed 29th July 2023.

Ladkin P. B. (1987b). *The Logic of Time Representation*. Ph.D. Thesis, Group in Logic and the Methodology of Science, University of California, Berkeley. Available from https://www.researchgate.net/publication/2242666_The_Logic_of_Time_Representation. Accessed 29th July 2023.

Ladkin P. B. (2001). *Causal System Analysis*. RVS Group, Bielefeld University. Available from https://rvs-bi.de/publications/books/CausalSystemAnalysis/index.html. Draft e-textbook accessed 29th July 2023.

Ladkin P. B. (2008). *Definitions for Safety Engineering*. Causalis Limited. Available from https://causalis.com/90-publications/99-downloads/DefinitionsForSafetyEngineering.pdf. Accessed 29th July 2023.

Ladkin P. B. (2017). *Digital System Safety*. RVS Group, Bielefeld University. Available from https://rvs-bi.de/publications/RVS-Bk-17-02.html. Draft e-textbook accessed 29th July 2023.

Ladkin P. B. (2019). *Architectural Concepts in Key TC 65 Standards on Safety and Cybersecurity*. Project Harbsafe Working Paper, Version 1 of 2019-05-14, Causalis Ingenieurgesellschaft mbH.

Ladkin P. B. (2020). *IEC TR 63069, Security Environments and Security-Risk Analysis*. In: Parsons M., Nicholson M. (editors) *Assuring Safe Autonomy, Proceedings of the Twenty-eighth Safety-Critical Systems Symposium, York, UK*. SCSC-154, SCSC C.I.C. 2020.

Ladkin P. B., Lou X., and Schnäpp D. (2023). *The Terminological Analysis Method SemAn and its Implementation*. Safety-Critical Systems eJournal 2(1). SCSC-183. Safety-Critical Systems Club. Available from: https://scsc.uk/r183.4:1#page=55. Accessed 29th July 2023.

Lewis D. K. (1973a). *Causation*. Journal of Philosophy 70(17):556-567, 1973. Reprinted with postscripts in (Lewis 1986).

Lewis D. K. (1973b). *Counterfactuals*. Blackwell, Oxford, 1973, reissued 2001.

Lewis, D. K. (1986). *Philosophical Papers* (Vol. II). Oxford University Press, Oxford.

Littlewood B. & Strigini L. (1993). *Validation of Ultrahigh Dependability for Software-Based Systems.* Communications of the ACM (CACM), 36(11), pp. 69–80. Available from https://openaccess.city.ac.uk/id/eprint/1251/1/CACMnov93.pdf. Accessed 29th July 2023.

Magidor O. (2019). *Category Mistakes*. In: Zalta E. N., Nodelman U. (editors) *Stanford Encyclopedia of Philosophy, Fall 2022 Edition*. https://plato.stanford.edu/archives/fall2022/entries/category-mistakes. Accessed 14th November 2023.

Margolis E. and Laurence S. (2005). Concepts. In: Stanford Encyclopedia of Philosophy. 2005, revised 2019. (Section 5 talks specifically about conceptual analysis). Available from https://plato.stanford.edu/entries/concepts/. Accessed 27th July 2023.

Neyman J. (1937). *Outline of a Theory of Statistical Estimation Based on the Classical Theory of Probability*. Philosophical Transactions of the Royal Society of London A, 236:333–380. 30th August 1937.

Paul L. A. and Hall N. (2013). *Causation: A User's Guide*. Oxford University Press, Oxford.

Quine W. V. O. (1951). *Two Dogmas of Empiricism*. The Philosophical Review 60(1):20-43, Jan., 1951.

Quine W. V. O. (1960). *Word and Object*. The M.I.T Press, Cambridge, MA.

Ricque B. (2019). Bertrand Ricque: personal communications with the author, various dates in 2019.

Riemenschneider R. (1984). Robert Riemenschneider: personal communications with the author, in Berkeley, CA and environs, 1976-1984

Robinson arithmetic. (2023). In Wikipedia. Accessed 29th July 2023. https://en.wikipedia.org/wiki/Robinson_arithmetic

Spafford E. H., Metcalf L., and Dykstra J. (2023). *Cybersecurity Myths and Misconceptions*. Addison-Wesley/Pearson Education, Boston MA.

Appendix A. Definitions of "Reliability" in the On-Line International Electrotechnical Vocabulary

The definitions here are all those in the on-line version of the International Electrotechnical Vocabulary (IEV n.d.) which define "reliability" of something or other. It does not include terms which use the word "reliability" only as part of their designation, for instance "reliability block diagrams" (which are diagrams) or "reliability model" (which is a probabilistic model).

There are some minor syntactic violations of IEC guidelines in these definitions; in 395-07-131, 448-12-05, 603-05-01, 603-05-02, the initial "the" should not appear.

In 312-07-06, the definition is said to be taken from 191-02-06. This refers to the previous IEC 60050 Section 191: Dependability and quality of service. According to the IEC Webstore, this section was replaced in 2015 by Section 192: Dependability.

The numerical designation of a definition is threefold. The first number refers to the electrotechnical branch classification, and associates the definition with a specific Technical Committee of the IEC. The second number relates to that technical committee's classification of its areas of concern. The third number is just a sequence number of a series of definitions. The main branch and the subclassification are given after the definition number below.

Each definition has three parts:

- Number, along with branch and subclassification. Number is shown in bold-face font.
- Definiendum: the term which is defined (this may include qualifications, in angle brackets "<...>").
- Definiens: the definition, which is mainly meant to be substitutive. "Substitutive" means that the definiens may substitute for the definiendum in any syntactic context while retaining the exact same meaning. This may or may not be literally the case here, but substitutional definition is a well-researched area of philosophical logic and I suggest it is more or less clear what the intention is, even if it may be imperfectly realised in the IEV.

192-01-24 Dependability / Basic concepts

reliability <of an item>

> ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures

192-05-05 Dependability / Reliability related concepts: measures

reliability <measure>

> probability of performing as required for the time interval (t1, t2), under given conditions

Note 1 to entry: Given conditions include aspects that affect reliability, such as: mode of operation; stress levels; environmental conditions; and maintenance, where applicable.

Note 2 to entry: It is usually assumed that the item is in a state to perform as required at the beginning of the time interval.

Note 3 to entry: When t1 = 0 and t2 = t, then R(0, t) is denoted simply as R(t) and termed the reliability function, or survival function of the item. See IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms, for more details.

Note 4 to entry: See also reliability, <of an item> (192-01-24).

312-07-06 Electrical and electronic measurements — General terms relating to electrical measurements / Performance

reliability (performance)

> ability of an item to perform a required function under given conditions for a given time interval

[SOURCE: 191-02-06]

(PBL Note: see preliminary comments to this Appendix. Section 191 no longer exists in the IEV. The definition 191-02-06 does exist, though, in the IEC Glossary, which contains the following entry for "reliability", inter alia:

> *ability of an item to perform a required function under given conditions for a given time interval*
> *NOTE 1 It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval.*
> *NOTE 2 The term "reliability" is also used as a measure of reliability performance (see IEV 191-12-01).*
> *[IEV191-02-06]*

The notes here are important, in particular NOTE 1, which however is not adopted in 312-07-06. The References entry for the IEC Glossary (n.d.) contains the precise URL for this entry in the glossary.)

395-07-131 Nuclear instrumentation: Physical phenomena, basic concepts, instruments, systems, equipment and detectors / Nuclear fission reactors, including the nuclear fuel cycle and thermonuclear facilities

reliability

> the ability of an item to perform a required function under given conditions for a given time interval

Note 1 to entry: It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval.

Note 2 to entry: Generally, reliability performance is quantified using appropriate measures. In some applications, these measures include an expression of reliability performance as a probability, which is also called reliability.

444-07-01 Elementary relays / Endurance

relay reliability

> probability that a relay can perform a required function under given conditions for a given duration or number of cycles

Note — It is assumed that the relay is able to perform this required function in its initial condition.

448-12-05 Power system protection / Reliability of protection

reliability of protection

> the probability that a protection can perform a required function under given conditions for a given time interval

Note — The required function for protection is to operate when required to do so and not to operate when not required to do so.

603-05-01 Generation, transmission and distribution of electricity — Power systems planning and managements / Power system reliability

reliability of an item

> the ability of an item to perform a required function under stated conditions for a specified period of time

603-05-02 Generation, transmission and distribution of electricity — Power systems planning and managements / Power system reliability

service reliability

> the ability of a power system to meet its supply function under stated conditions for a specified period of time

692-01-13 Generation, transmission and distribution of electrical energy — Dependability and quality of service of electric power systems / System concepts

reliability <of an item>

> See 191-01-24.

692-01-14 Generation, transmission and distribution of electrical energy — Dependability and quality of service of electric power systems / System concepts

service reliability

> ability to adequately satisfy the demand under given operating conditions for a given time interval…

This collation page left blank intentionally.