*Formal Ontology in Information Systems*
*M. Donnelly and G. Guizzardi (Eds.)*
*IOS Press, 2012*

*doi:10.3233/978-1-61499-084-0-117*


# Preliminaries to a formal ontology of failure of engineering artifacts

Luca DEL FRATE[a,1]
[a] *Delft University of Technology, The Netherlands*

**Abstract.** The aim of this paper is to offer a conceptual analysis of the notion of failure of engineering artifacts focusing on aspects that are of import for a possible ontological formalization. Failure is a central notion in engineering, yet different taxonomies exist in the various industries and engineering domains that are not mutually compatible thereby hindering knowledge exchange. A formal definition of failure would contribute to improve knowledge exchange. However, in order to be successful such formalization should rest on shared conceptualizations. The paper analyses how the notion of failure is used in engineering, starting with the so-called "traditional definition". Then, it is shown that engineers are willing to consider as failures also events and circumstances that are at odds with this traditional definition. Therefore, it is argued that, in order to capture adequately engineering conceptualizations, three independent notions of failure should be distinguished, which are called *function-based failure*, *specification-based failure*, and *material-based failure*.

**Keywords.** Failure, Failure event, Fault state, Engineering artifacts

## Introduction

Failure is a vital concern to engineers of all disciplines. Understanding how failures happen is crucial for prevention and also for mitigation of potential outcomes. For these reasons, tools that allow effective archiving, reuse, and exchange of data about failures are valuable to engineers. Formal ontologies have been already deployed successfully for knowledge exchange in various domains. Attempts have been made to extend formal ontologies in order to characterize the notion of failure in engineering: Kitamura and Mizoguchi [1] provide an ontological analysis of fault processes and categories of fault; van der Vegte et al. [2], propose an ontology-based modeling of product functionality which addresses also the aspect of unintended behavior and malfunction; Koji et al. [3] investigate the feasibility of applying ontology-based transformations to a functional model in order to create FMEA sheets; Borgo and Leitão [4] discuss the foundations of a core ontology for manufacturing, including the concepts of disturbance and machine failure; Borgo and Vieu [5] offer an analysis of the category of artifacts in formal ontology and outline a definition of malfunctioning artifact.

However, the analysis of conceptualizations about failure shared among engineers has played a minor role in the ontological literature so far. Indeed, as observed by

[1] Faculty of Technology, Policy and Management – Delft University of Technology – Jaffalaan 5, 2628 BX Delft, The Netherlands – e-mail: L.DelFrate@tudelft.nl

Guarino et al. [6], formal specifications of concepts do not need to be specifications of *shared* concepts. Nonetheless, Guarino et al. promptly remark that an "ontology may turn out useless if it is used in a way that runs counter to the shared ontological commitment" (p. 14) of its stakeholders. In making this claim, they are endorsing the approach proposed by Borst [7] who argues that formal ontologies should bring out "what is really shared by the community [of users] in order to enhance reuse *within* this community" (p. 123, emphasis in original).

Therefore, an ideal starting point for a formalization of the concept of failure would be a definition which is widely shared in the engineering community and which is consistent with actual use. Unfortunately, the engineering terminology on failure and related concepts is highly fragmented and there is a lack of agreement even on the definition of failure itself. Separate disciplines tend to emphasize specific aspects of the notion of failure and to formulate definitions tailored to particular applications. As a result, conflicting definitions can be found in the engineering literature [8–10].

Therefore, circumstances may arise where engineering judgments about failure diverge. A paradigmatic case is failure of artifacts that have been abused, e.g., because of overloading or by exposure to environmental conditions harsher than specified. Harland and Lorenz [11], for example, do not see any problem in classifying as failed a component which stops performing its required function because the surrounding environment has become hotter than specified. Other engineers, however, disagree and think that such events should not be considered failures or, at least, not failures "in the usual sense" (p. 6) [12]. Disagreements may ensue also between engineers who would treat an artifact as being in a fault state because of degradation of its material properties, and those who think that a failure judgment would be unwarranted if the artifact is still functioning. Suess [13], for instance, describes the case of a stainless steel trailer barrel used to haul various chemicals which internal surface showed evidence of severe corrosion. Even though the barrel did not develop any leakage, Suess treats the episode as a clear-cut failure, more precisely a "*failure* [which] was caused by bacteria-induced corrosion" (p. 73, emphasis added). On the other hand, Grantham Lough et al. [14] discuss Suess' case and, by pointing out that the barrel was still able to perform its main function of storing fluids, they conclude that "the tank was still functioning properly" (p. 473).

The aim of this paper, then, is to perform a conceptual analysis of the notion of failure in engineering as preliminary work towards a formal definition which is informed by practitioners' intuitions and ontological commitments. The paper builds on the results of a previous survey of the engineering literature [10] where it is argued that the engineering community is subject to two conflicting demands. On the one hand, there is a quest for standardization and simplification; on the other, there is an acknowledgment of the multifaceted nature of failure phenomena which stimulates the development of definitions tailored on special purposes and needs. In fact, the tendency towards unification has coalesced into the definition offered by the *International Electrotechnical Vocabulary* [15] published by the International Electrotechnical Commission (IEC), where failure is defined as "the termination of the ability of an item to perform a required function". Being adopted by several international standards and influential textbooks, the IEC definition has achieved a prominent role and is often taken as "the traditional definition" [16]. Nevertheless, the IEC notion has not been fully successful in superseding alternative definitions and preventing new ones being proposed. With all its merits, it has proven unable to capture relevant engineering intuitions. On the one hand, it can be shown that engineers are willing to classify as

failures circumstances that do not fit the traditional definition. In this paper a proposal is made to the effect that, in order to capture engineering intuitions and to deal with the problematic cases, two additional notions should be introduced besides the traditional one. Thus, three different notions of failure should be distinguished: *function-based failure* (i.e., the IEC notion), *specification-based failure*, and *material-based failure*.

## 1. The traditional definition: Function-based failure

The IEC vocabulary [15] defines the term "failure" as follows:

> Failure: the termination of the ability of an item to perform a required function.
> NOTE 1 – After failure the item has a fault.
> NOTE 2 – *Failure* is an event, as distinguished from *fault*, which is a state.

The two notes appended to the definition make clear that, in order to understand the notion of failure, a second term should be defined as well: "fault". The IEC vocabulary definition of fault reads as follows:

> Fault: the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.
> NOTE 1 – A fault is often the result of a failure of the item itself, but may exist without prior failure.

Jointly, the two definitions characterize what can be considered a twofold notion of failure which in the rest of this paper will be called *Function-based failure* (FBF), in order to differentiate from the other two notions that will be discussed later on.

The motivation behind the distinction between failure events and fault states is that for engineers it is important to know when and how many times an item stopped delivering a required function (i.e., failure event), and also for how long the lack of performance persisted (i.e., fault state). The relation between the two notions has been illustrated by Rausand and Øien [17] by means of the diagram reproduced in Figure 1. The curve in Figure 1 plots the observed level of a performance variable of an item (e.g., a pump) against time. Initially, the observed performance conforms to the target value, but later it starts gradually deviating downwards until it trespasses the acceptable limit, after which the item is still producing some output though well below the target level. The term "failure", as defined by the IEC vocabulary, refers to the instant when the observed performance trespasses the acceptable limits (or tolerance limits), after which the item is said to be in a fault state that will persist until the item is repaired.

Sure, Rausand and Øien's figure is not meant for a philosophical audience and is far from perfect.[2] Nevertheless, it has the merit of pointing out, albeit in a crude manner, some aspects relevant for the present discussion. First of all, the diagram makes clear that the item enters into a fault state immediately after exceeding the acceptable limit when it is still able to deliver some performance, even if at a disappointing level. Hence, it can be seen that the term "termination" in the IEC definition should not be interpreted as total lack of ability to perform, but as the trespassing of the acceptable levels.

[2] For instance the diagram plots *actual performance* over time even though the IEC definition refers to the item's *ability to perform*. For the aims of the present discussion the distinction can be safely ignored.

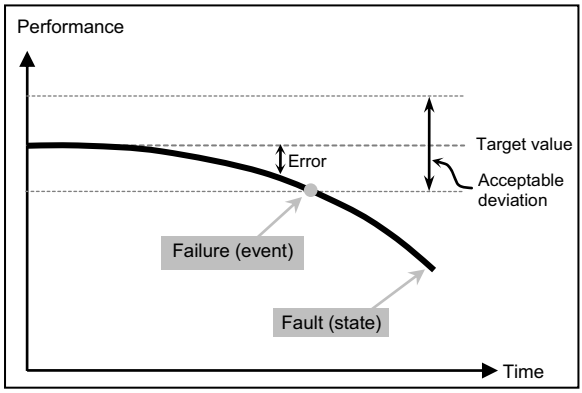


**Figure 1.** Illustration of the notions of failure event and fault state. Based on [17] with minor modifications

Moreover, the definition of fault state does not imply that fault states are necessary permanent. In fact, fault states can be temporary, in which case the IEC terminology introduces the term "transient faults", that is to say, faults "which persists for a limited time duration following which the item recovers the ability to perform a required function without being subjected to any action of corrective maintenance". Think, for instance, of a computer that hangs because of moderate overheating; after a while the electronic components will cool down and the computer will resume operating normally.

By analogy with the notion of "fault state" the interval preceding the failure event can be termed "functioning state", even though the term does not appear in the IEC nomenclature. According to the IEC nomenclature, the event depicted in Figure 1 is called a "gradual failure" for the failure event is preceded by the building up of a gap or "error" between the observed performance and the target level. Failure events where the performance departs abruptly from the target level to trespass the acceptable limits are termed "sudden failures". In these cases the gentle slope of Figure 1 would be replaced by a sharp turn either downwards or upwards. Another important distinction is the one between "complete failure" and "complete fault" on one hand, and "partial failure" and "partial fault" on the other. These notions are meant for items required to perform multiple functions. Therefore, a failure that results in the inability to perform some, but not all, required functions is called "partial failure"; while a failure affecting all required functions is called "complete failure".

It is interesting to note that the IEC terminology does not make provision for *gradations of fault*. This means that for a given item and a given function, the notion of fault is binary: either the item is able to perform the required function or it is not. Correspondingly, there are no gradations for the "ability to perform" either. Thus, it does not matter how close an item is to trespassing the threshold of acceptable performance for, to the extent that performance is within the acceptable limits, the item is described as being in a functioning state. Finally, the note appended to the definition of fault state (i.e., "A fault is often the result of a failure of the item itself, but may exist without prior failure") addresses a further important aspect of the relation between fault state and failure event. The phrasing of the note, though, is somewhat misleading because of the term "result" might mistakenly suggest a causal connection between failure and fault. Sure enough, for many items failure occurs after a period of

satisfactory performance. Nevertheless, the failure event is just the event corresponding to the transition between the functioning state (when performance is between the acceptable limits) and the fault state. Thus, the relation between functioning, failure, and fault is one of temporal sequence and not a causal one. In fact, by saying that a fault state "may exist without prior failure", the second part of the note makes clear that causality is not required. Simply, it may happen that an item never possessed the ability to perform its required function, possibly because of a design flaw or a manufacturing defect.

Evidently, in order to understand the gist of the IEC notion of failure, the meaning of "required function" should be clarified. This is a notoriously problematic notion which is given different definitions in the engineering literature, e.g., [18,19], and unfortunately the IEC vocabulary cannot be said to provide much clues on the issue. The vocabulary defines "required function" by means of the concept of service: "Required function: a function or a combination of functions of an item which is considered necessary to provide a given service". Then, the concept of service is defined by means of the term "function" itself: "Service: a set of functions offered to a user by an organization". However, since the definition of bare "function" is missing, one must conclude that the notion of "required function" is left undefined by the IEC terminology.

A more perspicuous discussion of the notion of function and its relation to the IEC terminology can be found in Rausand and Øien [17], from which the diagram in Figure 1 has been taken. Bypassing the IEC definitions of required function, Rausand and Øien elect to endorse the approach proposed by many design methodologists of treating item functions as black boxes which perform operations, expressed by means of verb-noun combinations (e.g., "transmit signal"), on the flows of energy, materials, and signals passing through them [20,21]. Rausand and Øien illustrate this approach by considering a "process shutdown gate valve" – a kind of safety valve often used in chemical plants – whose required function is to "close flow of fluid", typically in case of an emergency. In a black box model representation, the inputs are the material flow of fluid and the signal sent by the operator, and the operation consists in transforming the incoming signal in a cessation of the material flow of fluid. In normal situations, the valve is held open by a spring and the fluid can pass freely. When the need of stopping the fluid arises, the operator can send a signal and the valve performs its function by closing the flow. Thus, a failure will occur when, given that a signal has been sent by the operator, the material flow is not terminated.

Even though Rausand and Øien's characterization of the notion of function is derived from the influential work of Pahl and Beitz, other interpretations can be found in the literature – see, for instance, [18,19] –, which could possibly result in different criteria for failure. In this paper, the decision has been made to follow Rausand and Øien's characterization because, differently from most of other works on the subject, Rausand and Øien – whose field of expertise is reliability engineering – discuss the notion of function from the perspective of engineers dealing with failure phenomena. Moreover, a similar stance on the notion of function can be found in many other engineering publications which deal with failure phenomena and related subjects [14,22–26].

Looking at Figure 1 again, it can be seen that knowing the black-box description of the function of an item (e.g., "close flow of fluid") is not sufficient for making a failure judgment: at least one performance parameter is needed (e.g., voltage, pressure, torque, etc.), alongside with a target level and acceptable deviation. In fact, Rausand and Øien

observe that in order to "identify the failure modes we have to study *the outputs* of the various functions" (emphasis added) performed by the items. For shutdown valves the needed output or performance parameter is given by the time it takes the valve to close the flow of fluid: if the valve closes too fast, dangerous pressure shocks may ensue; if it closes too slowly, it will be ineffective. Thus, a typical target level for shutdown valves is that they are able to close within 10 seconds, with an acceptable deviation of plus or minus 4 seconds. So, the curve in Figure 1 can be interpreted as representing a valve which, at the beginning, is able to close in 10 seconds; after a while the valve becomes increasingly faster such that a failure event occurs when the closing time drops below the 6 seconds threshold, after which the valve is in a fault state.

The combination of the failure-related definitions given by the IEC vocabulary together with the black-box concept of function gives rise to the *Function-based* notion of failure (FBF) which can be considered the traditional notion of failure in engineering. The main ontological commitments behind FBF could be summarized as follows. Engineering artifacts or "items" (which the IEC vocabulary defines as "any part, component, device, subsystem, functional unit, equipment or system that can be individually considered") are *continuants* characterized by the attribution of the ability to perform one or more required functions. Even though the IEC terminology offers only scant support, it can be assumed that the attribution occurs when the item completes successfully the manufacturing or construction stage and is approved by the quality checks. When the abilities which actually inhere in the items coincide with the attributed abilities, the items *participate* to functioning states. Since functioning states have temporal parts (e.g., during the first month the solar panels produced 300 kWh of energy) they are *non-atomic occurrents*. Participation to functioning states does not imply that the items have to be actually performing their required functions. They can be in stand-by mode, like a back-up power unit waiting to be called into action, or standing on the shelves of a store. If the attributed abilities do not match the actual abilities, the items participate in fault states. Similarly to functioning states, fault states have parts (e.g., the engine was making rattling noises for a while and then it stopped completely) and are *non-atomic occurrents*. Since actual abilities of items can change in time, the IEC terminology stipulates that the transition from functioning to fault states is singled out as the failure event. Failure events are *atomic occurrents* to which items participate. It should be stressed that failure events do not need to be anything spectacular. It can be that an item, say a printer, is shipped to a dealer's store while being in a functioning state. Then, for some reason, the printer may lose the ability to print while standing idle on the shelf. Thus, a failure event has occurred, even though no one noticed.

Even though FBF can deal with a large variety of circumstances deemed relevant in engineering practice and has reached a prominent status among the community, dissenting views have emerged that will be discussed in the next section.

## 2. Specification-based failure

One of the main critiques leveled at FBF is that it does not make clear who is in charge of deciding the acceptable limits of the functional output. So, are the users allowed to decide what counts as satisfactory performance or is that the job of engineers? Chillarege [27] openly takes the side of the users by claiming that "customer expectation largely determines whether a failure has occurred or not" (p. 354). Other

authors claim this will result in untenable judgments. On the one hand, as observed by Yellman [28], customers might be satisfied with the output they get even though the product is performing demonstrably below the specifications. In his opinion, such cases represent a clear instance of failure "whether or not any customers have explicit current expectations for the unsuccessful functionality" (p. 7).

On the other hand, lack of expected output might be the result of the product being abused or operated outside the stated operational conditions. Mountaineer Neal Mueller [29], for instance, complained publicly that his iPod fell silent while he was climbing to the top of Mount Everest. The claim, however, conflicts with the product specifications which state a maximum operating altitude of 3000 meters [30]. Remarkably, engineers themselves frequently exploit the interpretative flexibility of FBF to describe as failed items that have been misused. Harland and Lorenz [11], as already mentioned in the Introduction, accept that a sensor which stops working because it is operated into an overly hot environment is described as having failed. Many similar examples can be found in the engineering literature. Kieselbach [31], for example, reports the results of the investigation on the bursting of a silo and concludes that "it can be said that *failure* of this silo was caused by filling it to too high a level with liquid instead of forage" (p. 55, emphasis added). Similarly, Ross et al. [32], who describe the collapse of a heavy lift crane, use the term failure even though the investigation determined that the "loads which provoked incipient *failure* […] were almost 2–1/2 times greater" (p. 961, emphasis added) than the requisite design condition.

However widespread this kind of judgments may be, many engineers think that an item which is operated outside the acceptable limits and does not perform as desired "should not be considered failure in the *usual sense*" [12]. Similarly, Nieuwhof [33] states that if a one-ton truck is utilized to carry a 25-ton load, then when the truck eventually collapses "we should not talk about a truck failure" (p. 54). Engineers like Ezrin and Nieuwhof advocate a notion of failure that looks at items within the context in which they are operated and also at the expectations that are legitimized by the intentions of the designers. In fact, Nieuwhof proposes to distinguish between two notions of failure. One, called "equipment failure", is based on the intended functions and the "specified operational conditions for which [items are] designed" (p. 54). The other, "mission failure", is grounded on the idea of "required feasible actions" which can be assimilated to required functional output, and does not make any reference to operational conditions. Haasl [34], urges a similar distinction, though his terms of choice are "primary failure" and "secondary failure" respectively.

As a result, in this paper a second notion of failure is proposed, i.e., *Specification-Based Failure* (SBF):

> Specification-based failure event: the termination of the ability of an item to perform as specified provided it has been operated under the stated operational environment for which it is designed.
>
> Specification-based fault state: the state of an item characterized by inability to perform as specified under the specified operational conditions for which it is designed, excluding (i) the inability during preventive maintenance or other planned actions, or (ii) the inability due to lack of external resources, or (iii) the inability due to previous violations of specified operational conditions.

Clearly SBF is heavily influenced by FBF from which it inherits the terminology and the main ontological assumptions. Hence, also in SBF "termination" means the trespassing of the acceptable limits as depicted in Figure 1. However, instead of the

term “required function”, the expression “perform as specified” is utilized to underline the fact that the criteria for failure are the “specifications” established by the designers of the product. Moreover, a clause has been added which requires compliance with “the stated operational environment”. Thus, the new concept aims at dispelling the ambiguities which make FBF a very permissive notion and, as a result, failure judgments like those expressed by Mueller, Harland and Lorenz, and others could not be passed.

It has to be stressed that, although SBF is less a liberal notion than FBF, it can be only as precise as the set of product specifications on which it relies upon. Even if stricter regulations and threats of legal actions force manufacturers into issuing more comprehensive specifications, in practice they cannot address all potentially relevant product properties. In particular, products age by the very fact of being utilized. For instance, fuel mileage and power output of a car can be maintained within specifications only on condition that the car is periodically serviced as recommended by the manufacturer.

Many SBF are, of course, also FBF, yet in section 4 it will be shown that FBF and SBF are independent concepts. In the next section a third notion of failure will be analyzed which runs parallel to the other two already discussed and which is characterized by its focus on the material properties of items.

## 3. Material-based failure

The example of the corroded trailer barrel mentioned in the Introduction has shown that engineers can arrive at contradictory evaluations about failure: based on material properties Suess [13] described the barrel as failed while, on functional grounds, Grantham Laugh et al. [14] pronounced it fit for purpose. Sometimes the mixing of material-based and function-based assessment can occur within the same paper. Henshaw et al. [35] analyze “*the failure* of a particular brand of automobile seat belts” (p. 13, emphasis added). The failure consisted in the seat belt latch assembly losing the ability to fasten properly the belt clasp, even when operated according to the specified procedures. The investigators found that small fractured pieces from the press release button (one of the components of the latch assembly) could become lodged within the assembly and interfere with its correct operation. Henshaw et al. remarked that “it is ironic that the breaking away of these small pieces *does not impede the function* of the release button itself” (p. 17, emphasis added). Nevertheless, few sentences later, when looking closely at the offending component, they speak of “degradation *and failure* of the release button” (p. 18, emphasis added) and conclude that “failure of the release buttons involved a combination of (1) repeated, low-level impact damage and (2) degradation of the material” (p. 19).

Again, two rather different meanings of failure are at stake here: one based on functional grounds (latch assembly) and one relying on material properties (press button). In the previous sections, while dealing with FBF and SBF, there was no need to mention material properties for the simple reason that engineering artifacts can fail for a variety of reasons that do not involve any kind of material degradation. Take, for instance, a printer where, because of a design flaw, the rolls feeding the sheets of paper from the paper drawer exert insufficient pressure. The printer and all its components are in pristine conditions and meet all the specifications. Still, the sheets of paper get jammed in the mechanism and the printer fails to perform its required function.

Another example, even more eloquent, is given by Collins and Daniewich [36] who remark that a shear pin which *does not* separate into two or more pieces upon the application of a preselected overload must be regarded as a failure, "as surely as a drive shaft has failed if it *does* separate into two pieces under normal expected operating loads" (p. 860, emphasis in original). Both events (i.e., shear pin and drive shaft) qualify as FBF and SBF, but there is a material aspect with the second that sets it apart: the material properties of the item have changed – it has fractured – such that it has lost the ability to perform its required function. Therefore, the shaft separating in two pieces counts also as a *Material-Based Failure* (MBF).

Even though fracturing and rupturing can be considered the paradigms of MBF, engineering taxonomies contain many other failure mechanisms which do not result necessarily in fracture or rupture of the affected items. In fact, as noted by Dasgupta and Pecht [37], although engineers may be tempted to think of failure in a binary manner as something being obviously fractured or not, "most real failures are more complicated than that" (p. 531), which means that also non-fractured items can be said to have failed. What Dasgupta and Pecht are referring to are the numerous physical and chemical processes (i.e., the *failure mechanisms*) that result in permanent degradation of material properties. Fracturing is just one of these processes, alongside fatigue, corrosion, wear, creep, radiation damage, buckling, and so on [38,39].

What has to be established now is whether MBF can be considered as a separate notion or just as a sub-kind of the other two notions. Indeed, the engineering literature suggests that MBF can qualify as a separate notion. The reason is that materially degraded items may be classified as failed even though they are still able to deliver their required functional output (albeit close to the acceptable limits) and do not satisfy the criteria for SBF. These cases occur when items have degraded, for whatever reason, much faster than anticipated making the items less reliable and safe to use and, ultimately, increasing the likelihood of an incoming FBF or SBF. To put it differently, considerations based on the material properties may induce engineers to declare items to be in a fault state even though considerations based on functional output would not (yet) sanction such judgments. Let us consider again the case of the stainless steel trailer barrel analyzed by Suess [13]. The investigation found that the chemical composition of the steel did comply with the requirements and that "*failure* was caused by bacteria-induced corrosion". The most likely explanation was that water contaminated by sulphate-reducing bacteria was used to wash the barrel. Since it is known that this kind of bacteria can attack stainless steel, barrels should be dried immediately after washing. In the case at hand, the barrel had not been dried, and the material was exposed to environmental conditions for which it was not designed. Thus, it would be inappropriate to describe the event as an instance of SBF. Moreover, as noticed by Grantham Lough et al. [14], the barrel was still able to perform its required function and FBF should be ruled out as well. Suess assessment, then, results from the observation of the negative impact of corrosion on the remaining life and residual strength of the barrel. Thus, it was an instance of MBF.

Therefore, MBF is proposed as a third notion of failure with the following definition:

> Material-based failure event: any permanent change in the values of geometrical or physicochemical properties of the materials of an item which (i) renders the item unable to perform as specified or (ii) increases substantially the likelihood that the item will become unable to perform as specified.

> Material-based fault state: the state of an item resulting from any permanent change in the values of geometrical or physicochemical properties of the materials of an item which (i) renders the item unable to perform as specified or (ii) increases substantially the likelihood that the item will become unable to perform as specified.

Here, the term "permanent" should not be interpreted in an absolute sense: changes are considered permanent when repairs are needed to restore the condition of the item. Certainly, temporary changes in geometrical properties, like reversible thermal expansion, can cause an FBF or an SBF (e.g., seizure of a valve), but are not classified as MBF because there has not been any degradation in material properties. As soon as the loads are removed, the items recover spontaneously their original conditions. On the contrary, the notion of MBF rests on the assumption that degradation processes can change permanently the abilities of items.

It is worth emphasizing that the focus of the notion of material-based failure is on the changes occurring to the properties *of materials* of which items are constituted: wear can change geometric properties without affecting physicochemical properties of materials; embrittlement and radiation damage act only on physicochemical properties; and corrosion can change both. The notion of material-based failure is not concerned with geometrical changes occurring *to the item* as a whole, like the displacement of a component within an assembly because a screw got loose. The event in which a car and one of its wheels part company because the retaining nut had not been tightened adequately counts as an FBF of the car; however there is no contextual material failure of the car (not yet, at least) nor of the retaining nut. On the other hand, if the wheel gets loose because the retaining bolt snapped, then the snapping of the bolt counts as a an MBF as well as an FBF of the bolt itself. To decide whether the snapping counts also as an SBF the operating conditions must be known: if the bolt was utilized according to the specifications, then an SBF has occurred. If the bolt was not utilized appropriately, e.g., it was not the right bolt, then no SBF has occurred.

In the next section, the trailer barrel case story will be used as a test bed for showing the mutual independence of the three notions of failure.

## 4. A case story: the mutual independence of the three notions

The case story discussed by Suess [13] deals with a stainless steel trailer barrel which, albeit severely corroded, had not developed leaks and was still capable of performing the required function "to store fluid". The failure investigation found evidence of bacterial attack. Stainless steel is not designed to withstand this kind of environment. Indeed, the investigation did conclude that changes in the washing procedure were to be implemented for preventing recurrence. The fact that the barrel was utilized under harsher conditions than specified implies that the barrel cannot be said to have incurred in SBF. Summing up, the original version of the case story, i.e., scenario (1), features the following combination: FBF, no; SBF, no; MBF, yes.

As observed by Suess, given the appropriate conditions bacteria-induced corrosion can be very fast and, if undetected, can result in perforation of the tank and leakage. In that case, the barrel loses the ability to perform its required function and an FBF is said to have occurred. Hence, in scenario (2) of the case story the following failures would occur: FBF, yes; SBF, no; MBF, yes.

**Table 1.** Eight failure scenarios that illustrate the mutual independence of the three notions of failure

| Scenario | Function-based failure | Specification-based failure | Material-based failure |
|---|---|---|---|
| (1) | N | N | Y |
| (2) | Y | N | Y |
| (3) | N | Y | Y |
| (4) | Y | Y | Y |
| (5) | Y | Y | N |
| (6) | N | Y | N |
| (7) | Y | N | N |
| (8) | N | N | N |

As a third variation, let us assume that the same amount of corrosion was found on the internal surface of the barrel, i.e., no leakage, but the investigation established that nothing was wrong with the water or the washing procedure, the culprit being the defective quality of the steel. Then, even though the barrel performs the required output, an engineer would describe the situation as an instance of SBF due to the thickness of the barrel being below the specifications. Hence, scenario (3): FBF, no; SBF, yes; MBF, yes.

If the situation depicted in the previous scenario progresses until corrosion opens a hole in the barrel, FBF will occur. Therefore, in scenario (4) the barrel suffers all three kinds of failure: FBF, yes; SBF, yes; MBF, yes.

As already mentioned above, a product may be in a state of FBF even though it has not suffered any MBF. The barrel may be leaking because of a fissure resulting from a manufacturing defect, e.g., inadequate welding. Then, since the leaking violates the product specifications, also SBF is present. Summing up scenario (5): FBF, yes; SBF, yes; MBF, no.

In a further permutation, thanks to a fortunate circumstance the fissure happens to be located in the uppermost part of the barrel. Since the user does not fill up the tank until the very top, the tank is never observed leaking and is considered to be fully functional. Still it falls short of the specifications which require the tank to store fluid up to the rated capacity. Therefore, scenario (6): FBF, no; SBF, yes; MBF, no.

In the last failure scenario, the barrel has been filled above the specified limit. During transportation the fluid expands and leaks through the flanges, thus without causing material damage. The event does not qualify as an SBF or as an MBF, hence scenario (7): FBF, yes; SBF, no; MBF, no.

To conclude, scenario (8) represents successful operation: FBF, no; SBF, no; MBF, no. The eight failure scenarios are summarized in Table 1.

## 5. Discussion of main ontological commitments

In this paper the notion of failure as defined by the IEC vocabulary has been used as a guideline and a template for the identification and the analysis of three independent notions of failure. As a consequence, a number of conceptual aspects and ontological assumptions are shared by the three notions. At the most fundamental level is the ontological assumption that both failures and faults are *occurrents* to which engineering item participate. The term “item” recurs in all definitions and refers to physical entities characterized by a complex quality, namely the quality of being

attributed the ability to perform required functions. In turn, required functions are seen as operations on flows of energy, materials, and signals.

Moreover, the notion of failure demands that the functional outputs of operations on flows of energy, materials, and signals are specified by means of appropriate target levels and acceptable limits. For the notion of FBF it is sufficient that the manufacturer of the item specifies the acceptable limits of the functional output; while, the notion of SBF demands that acceptable limits are defined for inputs, outputs, and operational environment. Let us assume that the curve in Figure 1 represents the torque generated by an electrical motor which happens to be operated at an environment hotter than specified. After a while, the motor overheats and the functional output drops below the acceptable level. According to FBF, a failure event has occurred which could be further qualified as a "misuse failure" if the incorrect operational environment was due to actions or omissions on the part of the user. Thus, an FBF failure event can be defined as an atomic occurrent, to which an engineering item participates which is characterized by a transition from correct functional output to incorrect functional output. The ensuing FBF fault state will be defined as a non-atomic occurrent to which an engineering item participates which is unable to perform the required functional output. Differently from failure events, fault states are not atomic because they can have temporal parts. For instance, at the beginning of the fault state the overheated electric motor is still able to provide some amount of torque. Then, if utilization continues nevertheless, the motor can stop working altogether and perhaps for good.

The sequence of events just described does not qualify as an instance of SBF because of the violation of the product specifications. An SBF failure event can be regarded as as an atomic occurrent to which an engineering item participates. An SBF consist in the transition from compliance with specification to lack of compliance while the operational environment remains within the specifications. The ensuing SBF fault state is defined as a non-atomic occurrent to which an engineering item participates and characterized by the inability of the item to meet the specifications while the operational environment remains within the specifications. A SBF fault state can be the effect of a previous SBF event or of an FBF event; alternatively, in case of a design flaw or of a manufacturing defect, the item can find itself in a fault state from the very beginning.

So far, the discussion has dealt only with the first two notions and MBF has not been mentioned. In fact, even though the basic distinction between events and states holds also for MBF, this notion appears more challenging and complex. First, it introduces a distinction between properties of the materials that constitute an item and the item itself. Second, the changes in material properties that are relevant are only the permanent ones. Finally, the notion of material fault state depends on the previous circumstances. While an item can be in a FBF fault state from the very beginning, say because of a manufacturing defect, an item needs to go through an MBF failure event in order to enter into a MBF fault state.

## 6. Conclusion

The possibility of failure is a persistent source of concern for engineers. Failure can be subtle and minor changes in design or in manufacturing techniques can turn a robust product into an unreliable or even a dangerous one. Tools could be devised to assist engineers in archiving, retrieving, and reusing information about failure. Formal

ontologies are one of the candidates. However, as argued by Borst [7] and by Guarino et al. [6], in order to be effective these tools need to be based on clear and shared conceptualizations. Unfortunately, the engineering literature offers a multitude of definitions partially conflicting with each other. Even the IEC definition of failure, which is often considered to be "the traditional definition", has met with critique. In this paper a conceptual analysis of the notion of failure as used by engineers has been performed. As a result, it is argued that three mutually independent notions can be identified: FBF, SBF, and MBF. The paper has examined the three notions and has sketched their main ontological assumptions.

It should be stressed that, although in this paper the analysis has been confined to the domain of engineering artifacts, the notion of failure plays a relevant role also beyond the artifactual domain. Avizienis et al. [40], for instance, discuss the notion of failure within the context of a taxonomy of basic concepts for information systems and secure computing. Moreover, the notion of failure has strong conceptual and practical connections with the issue of human error or, more generally, of human and social factors especially within the context of complex socio-technical systems. At the most basic level, social practices such as supervision, training, and knowledge sharing have considerable influence on the likelihood of failure events. Formal ontologists are already actively investigating this area of research where technology and social factors interact closely, e.g. [41–43]. Even though these studies have not addressed explicitly the notion of failure yet, it is reasonable to expect that it will attract more attention in the near future.[3] Therefore, future research might explore the possibility of expanding the conceptual analysis performed in this paper into the socio-technical domain.

## References

[1] Y. Kitamura, R. Mizoguchi, An ontological analysis of fault process and category of faults, in: *Proceedings of Tenth International Workshop on Principles of Diagnosis (DX-99)*, 1999: pp. 118–128.

[2] W.F. van der Vegte, Y. Kitamura, R. Mizoguchi, I. Horváth, Ontology-based modeling of product functionality and use – Part 2: considering use and unintended behavior, in: *Proceedings of The Third International Seminar and Workshop Engineering Design in Integrated Product Development*, Zielona Góra, Poland, 2002: pp. 115–124.

[3] Y. Koji, Y. Kitamura, R. Mizoguchi, Ontology-based transformation from an extended functional model to FMEA, in: *Proc. of ICED*, 2005.

[4] S. Borgo, P. Leitão, Foundations for a core ontology of manufacturing, in: R. Sharman, R. Kishore, R. Ramesh (Eds.), *Ontologies: a Handbook of Principles, Concepts and Applications in Information Systems*, Springer, 2007: pp. 751–775.

[5] S. Borgo, L. Vieu, Artefacts in formal ontology, in: A. Meijers (Ed.), *Handbook of Philosophy of Technology and Engineering Sciences*, 2009: pp. 273–308.

[6] N. Guarino, D. Oberle, S. Staab, What Is an Ontology?, in: S. Staab, R. Studer (Eds.), *Handbook on Ontologies*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009: pp. 1–17.

[7] W.N. Borst, *Construction of engineering ontologies for knowledge sharing and reuse*, University of Twente, 1997.

[8] D. Prasad, J. McDermid, I. Wand, Dependability terminology: similarities and differences, *Aerospace and Electronic Systems Magazine, IEEE* **11** (1996), 14–21.

[9] A.S.. Tam, I. Gordon, Clarification of Failure Terminology by Examining a Generic Failure Development Process, *International Journal of Engineering Business Management* **1** (2009), 33–36.

[10] L. Del Frate, M. Franssen, P.E. Vermaas, Towards a trans-disciplinary concept of failure for Integrated Product Development, *International Journal of Product Development* **14** (2011), 72–95.

[11] D.M. Harland, R. Lorenz, *Space Systems Failures*, Praxis, New York, NY, 2005.

[3] An exception is recent work by Bottazzi and Ferrario [44] which examines the notion of "faulty institutional object"

[12] M. Ezrin, *Plastics failure guide: cause and prevention*, Hanser Verlag, Munich, 1996.
[13] M.E. Suess, Bacteria-Induced Corrosion of a Stainless Steel Chemical Trailer Barrel, in: K.A. Esaklul (Ed.), *Handbook of Case Histories in Failure Analysis*, ASM International, 1992: pp. 70–73.
[14] K.A. Grantham Lough, R.B. Stone, I.Y. Tumer, Failure Prevention in Design Through Effective Catalogue Utilization of Historical Failure Events, *Journal of Failure Analysis and Prevention* **8** (2008), 469–481.
[15] IEC 60050(191), *International Electrotechnical Vocabulary (IEV), Chapter 191 – Dependability and quality of service*, International Electrotechnical Commission, Genève, Switzerland, 1990.
[16] K.M. Blache, A.B. Shrivastava, Defining failure of manufacturing machinery and equipment, in: *Proceedings of Annual Reliability and Maintainability Symposium (RAMS)*, Anaheim, CA, USA, 1994: pp. 69–75.
[17] M. Rausand, K. Øien, The basic concepts of failure analysis, *Reliability Engineering and System Safety* **53** (1996), 73–83.
[18] M.S. Erden, H. Komoto, T.J. Van Beek, V. D'Amelio, E. Echavarria, T. Tomiyama, A review of function modeling: Approaches and applications, *Artificial Intelligence for Engineering Design, Analysis and Manufacturing: AIEDAM* **22** (2008), 147–169.
[19] P.E. Vermaas, The Flexible Meaning of Function in Engineering, in: *Proceedings of the 17th International Conference on Engineering Design (ICED'09), Vol. 2*, Design Society, Stanford, CA, 2009: pp. 113–124.
[20] G. Pahl, W. Beitz, J. Feldhusen, K.-H. Grote, *Engineering Design: A Systematic Approach*, 3rd ed., Springer, London, 2007.
[21] R.B. Stone, K.L. Wood, Development of a functional basis for design, *Journal of Mechanical Design, Transactions of the ASME* **122** (2000), 359–370.
[22] M. Bellgran, K. Säfsten, *Production Development*, Springer, London, UK, 2010.
[23] A. Birolini, *Reliability Engineering: Theory and Practice*, 5th ed., Springer, Berlin, 2007.
[24] W.R. Blischke, D.N.P. Murthy, *Reliability: modeling, prediction, and optimization*, Wiley-IEEE, 2000.
[25] I. Tumer, R.B. Stone, Mapping function to failure mode during component development, *Research in Engineering Design* **14** (2003), 25–33.
[26] T.W. Yellman, Redundancy in designs, *Risk Analysis* **26** (2006), 277–286.
[27] R. Chillarege, What Is Software Failure?, *IEEE Transactions on Reliability* **45** (1996),.
[28] T.W. Yellman, Failures and related topics, *IEEE Transactions on Reliability* **48** (1999), 6–8.
[29] N. Mueller, Van Halen Fell Silent On Top of the World, *Washingtonpost.com* (2006),.
[30] Apple Inc., Apple iPod classic technical specifications., *Apple* (2011),.
[31] R. Kieselbach, Bursting of a silo, *Engineering Failure Analysis* **4** (1997), 49–55.
[32] B. Ross, B. McDonald, S.E. Vijay Saraf, Big blue goes down. The Miller Park crane accident, *Engineering Failure Analysis* **14** (2007), 942–961.
[33] G.W.E. Nieuwhof, The concept of failure in reliability engineering, *Reliability Engineering* **7** (1984), 53–59.
[34] D.F. Haasl, Advanced concepts in fault tree analysis, in: *System Safety Symposium*, Seattle, Wash, 1965.
[35] J.M. Henshaw, V. Wood, A.C. Hall, Failure of automobile seat belts caused by polymer degradation, *Engineering Failure Analysis* **6** (1999), 13–25.
[36] J.A. Collins, S.R. Daniewicz, Failure modes: performance and service requirements for metals, in: M. Kutz (Ed.), *Mechanical Engineers' Handbook – Materials and Mechanical Design*, 3rd ed., Wiley, Hoboken, N.J., 2006: pp. 860–924.
[37] A. Dasgupta, M.G. Pecht, Material failure mechanisms and damage models, *IEEE Transactions on Reliability* **40** (1991), 531–536.
[38] J.A. Collins, *Failure of Materials in Mechanical Design: Analysis, Prediction, Prevention*, 2nd ed., Wiley, New York, 1993.
[39] H.M. Tawancy, A. Ul-Hamid, N.M. Abbas, *Practical Engineering Failure Analysis*, M. Dekker, New York, 2004.
[40] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing* **1** (2004), 11–33.
[41] E. Bottazzi, R. Ferrario, A Path to an Ontology of Organizations, in: *Proceedings of International EDOC Workshop on Vocabularies, Ontologies and Rules for The Enterprise*, Centre for Telematics and Information Technology, University of Twente 2005, Enschede, The Netherlands, 2005: pp. 9–16.
[42] R. Ferrario, N. Guarino, Towards an Ontological Foundation for Services Science, in: J. Domingue, D. Fensel, P. Traverso (Eds.), *Future Internet - FIS 2008*, Springer Berlin / Heidelberg, 2009: pp. 152–169.
[43] A. Scherp, C. Saathoff, T. Franz, S. Staab, Designing core ontologies, *Applied Ontology* **6** (2011), 177–221.
[44] E. Bottazzi, R. Ferrario, Faulty Institutional Objects. A threat for the Infallibilist (and the Fallibilist as well), in: *Seventh European Conference of Analytic Philosophy*, Milan, 2011.