Reliability Engineering and System Safety 114 (2013) 148–154

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Review

Accident precursors, near misses, and warning signs: Critical review and formal definitions within the framework of Discrete Event Systems

Joseph H. Saleh*, Elizabeth A. Saltmarsh, Francesca M. Favarò, Loïc Brevault

Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Article history:
Received 20 October 2012
Received in revised form
4 January 2013
Accepted 10 January 2013
Available online 8 February 2013

Keywords:
Accident precursor
Warning sign
Accident pathogen
Near miss
Discrete Event Systems

ABSTRACT

An important consideration in safety analysis and accident prevention is the identification of and response to accident precursors. These off-nominal events are opportunities to recognize potential accident pathogens, identify overlooked accident sequences, and make technical and organizational decisions to address them before further escalation can occur. When handled properly, the identification of precursors provides an opportunity to interrupt an accident sequence from unfolding; when ignored or missed, precursors may only provide tragic proof after the fact that an accident was preventable.

In this work, we first provide a critical review of the concept of precursor, and we highlight important features that ought to be distinguished whenever accident precursors are discussed. We address for example the notion of ex-ante and ex-post precursors, identified for postulated and instantiated (occurred) accident sequences respectively, and we discuss the feature of transferability of precursors. We then develop a formal (mathematical) definition of accident precursors as truncated accident sequences within the modeling framework of Discrete Event Systems. Additionally, we examine the related notions of "accident pathogens" as static or lurking adverse conditions that can contribute to or aggravate an accident, as well as "near misses", "warning signs" and the novel concept of "accident pathway". While these terms are within the same linguistic neighborhood as "accident precursors", we argue that there are subtle but important differences between them and recommend that they not be used interchangeably for the sake of accuracy and clarity of communication within the risk and safety community. We also propose venues for developing quantitative importance measures for accident precursors, similar to component importance measures in reliability engineering. Our objective is to establish a common understanding and clear delineation of these terms, and by bringing formal mathematical tools to bear on them, we hope to provide a richer basis and more interpretive possibilities for examining and understanding risk and safety issues.

Contents

1. Introduction

The concept and the term "precursor" are used extensively in technical literature, and they pervade a host of academic disciplines. For example, the Web of Science® database lists over

* Corresponding author. Tel.: +1 404 385 6711; fax: +1 404 894 2760.
E-mail address: jsaleh@gatech.edu (J.H. Saleh).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.01.006

58,000 articles whose titles include this term[1] , and approximately 100 different subject–matter areas make use of this concept, from cell biology, to environmental sciences, and a host of engineering disciplines. The risk analysis and safety community is also an avid "user" of the concept of precursor. NASA for example issued its "Precursor analysis handbook" [13] in December 2011, modeled to some extent on the US Nuclear Regulatory Commission (NRC) accident precursor program [12] and the extensive experience the NRC has with such analysis in nuclear power plants[2]. The National Academy of Engineering conducted a major study entitled "Accident precursor analysis and management" in 2004, and many scholarly articles continue to be published addressing various aspect of accident precursors, especially in the nuclear industry [22,8,2], the chemical industry [15], the aerospace industry [10], and the oil and gas industry [21,26]. In this work, we first provide a critical review of the concept of precursor within the risk analysis and safety literature, and we highlight important features that ought to be distinguished whenever accident precursors are discussed (Section 2). We then propose a formal definition of this concept based on elements from Event Tree Analysis and grounded in the modeling framework of Discrete Event Systems (Section 3). We also examine the related notions of "near misses", "accident pathogens", and "warning signs", and we introduce the novel concept of "accident pathway". While these terms are within the same linguistic neighborhood as "accident precursors", we argue that there are subtle but important differences between them and recommend that they not be used interchangeably for the sake of accuracy of thought and clarity of communication within the risk and safety community. We also briefly discuss the medical discipline of pathology and explore parallels between three of its pillars, namely etiology, pathogenesis, and clinical manifestations, and various aspects of engineering risk analysis, in particular the concepts examined in this work (Section 4). Our objective is to establish a common understanding and clear delineation of these terms, and by bringing formal mathematical tools to bear on them, we hope to provide a richer basis and more interpretive possibilities for examining and understanding risk and safety issues, and upon which more contributions can be built.

2. Definitions, critical review, and linguistic features of (accident) precursors

The Oxford English Dictionary (OED) defines a precursor as a "person who or thing which precedes another as a forerunner or presage; a person who or thing which heralds the approach of another; a thing that comes before another of the same kind as a forerunner, predecessor, or prototype" [16]. A precursor thus shares elements in common with what it heralds or precedes, but is not fully identical with it, e.g., "Robert Burns was a precursor of the Romantics" [Merriam-Webster dictionary] [17]. Narrowing this concept to the accident paradigm, an accident precursor temporally precedes an accident and shares elements in common, but is not completely identical with the accident. While this might sound self-evident, it provides an interesting opportunity to define an accident precursor through its difference with, or the missing elements from, a complete accident sequence. In other words, an accident precursor in this view is an accident sequence minus a few elements[3]. We will revisit and formalize this idea shortly.

Note that the OED definition does not specify whether the precursor must be *recognized* ex-ante (i.e., it must occur before the accident, but not necessarily be observed or understood as fulfilling a role of "precursing" before the accident). Consequently, an event or sequence of events preceding an accident but identified only ex-post (after the fact) still qualifies as an accident precursor, even though it has ceased to be "precurse". In other words, the definition of precursor is all encompassing with respect to the temporal dimension and it includes truncated accident sequences recognized as precursors either ex-ante or ex-post. It follows that any accident has precursors, and one important challenge consists in recognizing them ex-ante if they are to be useful and result in actions to prevent the full accident sequence from unfolding.

Another interesting point in the OED definition of precursor is its silence with regard to causality: the definition does not address whether the precursor is part of the causal chain of what it precedes—for our purposes, this would be the accident—or whether it can simply announce it or be correlated with it (and temporally prior, but not causal). Therefore precursors, by definition, are not specified with respect to causality, and our understanding of the concept should include but not be restricted to causal elements leading to an accident.

The study by the National Academy of Engineering [14] provided a broad definition of accident precursors as "conditions, events, and sequences that precede and lead up to accidents." The NASA precursor analysis handbook [13] defines an accident precursor as "an anomaly [defined in the Handbook as an off-nominal occurrence or condition] that signals the potential for more severe consequences that may occur in the future, due to causes that are discernible from its occurrence today." Carroll [4] restricted the definition of accident precursors to causal events, excluding conditions: "events that must occur for an accident to happen in a given scenario". The Accident Sequence Precursor (ASP) program, operated by the US Nuclear Regulatory Commission (NRC) since 1979, defines an accident precursor within the context of nuclear power plants as an "element or condition in a postulated sequence of events leading to some undesirable consequence [accident sequence] usually severe core damage" [24].

Note that the NRC's definition introduces the notion of a postulated accident sequence in the definition of precursor. This raises two issues. First, for **ex-ante precursors**, no accident sequence has fully unfolded, and as such, the notion of a **postulated** accident sequence is introduced and used as the background against which a precursor is justified/validated[4]. Ex-post precursors, while no longer "precursing", are validated as precursors in light of the accident that has occurred[5]. Second, and more importantly, the NRC definition (unintentionally?) restricts "precursors" to off-nominal events or plant conditions which are elements of **previously conceived accident sequences**, that is, the postulated accident sequence is prior to off-nominal events qualifying as a precursors. This restriction is uncalled for, and if intended in the previous definition, it is a flawed understanding of the

[1] The numbers exceeds 275,000 when keywords are also queried for "precursor(s)".

[2] Over 8000 documents in the NRC database examine various aspects of precursors (data, cases at particular plants, and methodology). [accessed 11.09.12].

[3] This view brings into sharp focus the keen interest in this topic in all hazardous industries, namely to prevent (ex-ante) precursors from falling through the proverbial cracks, and thus have the opportunity to "learn from precursors" instead of learning from their more fully developed and costly analogs, namely accidents.

[4] Anticipatory rationality in risk analysis, expressed in the form of a Probabilistic Risk Assessment (PRA) or Event Tree Analysis for example.

[5] This brings out the internal linguistic contradiction of an ex-post precursor, and requires a bit of mental gymnastics to accept.

concept: off-nominal events or chains of events can identify overlooked accident sequences, and as such, they can help refine previously conducted risk analysis and add new accident sequences, previously unforeseen or unconsidered. In short, the notion of a postulated accident sequence, while useful for conceiving of some ex-ante precursors, is not a necessary condition to define and decide what qualifies as a precursor.

One additional detail worth mentioning is that some definitions of accident precursors include "conditions and events" and others are restricted to "events". We propose to exclude conditions as they are better captured by other more precise concepts: for example a rusted pipe in a chemical plant is an adverse condition that can contribute to an accident but it does not constitute an accident precursor. Similarly cold weather is an adverse condition for shuttle launch but it is not a precursor. The phrases "latent error", "contributing factor" or "accident pathogen" are better suited for such a situation than the term "precursors", and more broadly for static or lurking adverse conditions that can contribute to or aggravate an accident.

In summary, an accident precursor can be conceived of as a truncated accident sequence, that is, a chain of adverse events following an initiating off-nominal event, and that can lead to an accident when compounded with additional adverse conditions. The accident sequence can be either real (instantiated), or postulated prior to or after the precursors have occurred.

One final linguistic feature is implicitly assumed in all definitions of accident precursors but is rarely articulated, namely that precursors need not be co-located with the accident sequence, and their applicability extends beyond the particular plant or system where they occurred. This intrinsic feature can be termed the **transferability or portability of accident precursors**. Learning from precursors should not be restricted to the location or the system where the precursors occurred. For example, foam hitting the space shuttle Endeavor during lift-off qualifies as an accident precursor for Discovery's lift-off and all the other shuttles as well. Similarly, a relief-valve that fails in the open position at the Davis-Besse nuclear power plant qualifies as an accident precursor for other similar nuclear power plants, the Three-Mile Island for example. Both the Davis-Besse and Three-Mile Island (TMI) nuclear reactors were designed by the same company, and it was found during the investigation of the TMI accident that a similar sequence of adverse events[6] (precursor) had occurred at the Davis-Besse plant a few months prior to the TMI accident. A detailed analysis of these two cases can be found in Hopkins [7]. The transferability of accident precursors across similar plants or systems, within a company or more broadly within an industry, raises several interesting challenges, in particular those of organizational structure and ownership of precursor management process (how to collect and communicate precursor information and lessons learnt across different business units within a company and across different companies within an industry; and who is or ought to be in charge). These issues of precursor lifecycle and ownership, and the related failure mechanisms in precursor management—how and why precursors are sometimes ignored or mishandled—are examined in Saltmarsh et al. [20].

Having examined definitions of "accident precursors" and identified distinctive features of this concept, we develop in the next section a formal definition of this concept based on elements from Event Tree Analysis and grounded in the modeling framework of Discrete Event Systems.

[6] Relief valve failing in the open position, resulting in loss of coolant; failure of operators to recognize what was going on, and their subsequent (wrong) decision to terminate high-pressure injection of water. The difference between the incident at Davis-Besse and the accident at TMI is that the former was operating at a low power output and the operators managed to de-escalate the situation in time before core uncovery, unlike the case at TMI [7].

3. Towards a formal definition of accident precursors

This section provides a first attempt at formalizing the concept of accident precursors discussed previously. The analysis is based on elements from Event Tree Analysis (ETA) and Discrete Event Systems (DES). These two modeling frameworks are briefly described, after which a formal definition is proposed.

3.1. Event Tree Analysis

The safety community is familiar with Event Tree Analysis (ETA), which is an inductive method in risk analysis (causally forward or "what if" approach). ETA typically starts with an initiating adverse event, and graphically displays how that event can propagate and affect the system. Multiple paths of possible conditions and events are considered in the analysis, each represented by a branch in the tree (sequence of events). The analysis then identifies outcomes and consequences of each branch[7] .

Fig. 1 represents a simplified version of an Event Tree Analysis for a generic reactor. The initiating adverse event considered is the break of the main coolant pipe.

In reading the event tree from left to right, consider for example the path leading to the fourth consequence from the top (explosion): the main coolant pipe breaks; electric power is available upon demand to support the activation of the flow detector and emergency pumps; the flow detector operates properly and detects loss of main coolant; information is conveyed to activate redundant emergency pumps; pump 1 fails to activate; pump 2 also fails to activate, and this sequence of events leads to the explosion. The event tree can be further expanded to examine more possibilities and add further resolution to the consequences of the explosion and other branches.

Event Tree Analysis provides an intuitive understanding of an "accident sequence", which is needed for formalizing the concept of "accident precursor", and it is more familiar as a modeling framework to the risk analysis and safety community than Discrete Event Systems (DES). The latter however, while exhibiting some similarities with the former, is both more theoretically grounded and has more interpretive possibilities than ETA. We provide next a quick introduction to DES for the reader who may not be familiar with this modeling framework, and then we proceed to examine accident precursors within this context.

3.2. Discrete Event Systems

Discrete Event Systems is a unified modeling framework which recently emerged integrating traditionally separate disciplines such as queuing theory, supervisory control, and automata theory. A Discrete Event System is defined as "a discrete-state, event-driven system, that is, its state evolution depends on the occurrence of asynchronous discrete events over time" [5]. The distinction between DES and the more familiar time-driven dynamical systems studied under Control Theory for example is subtle but important: the state-transition mechanism in the latter is driven by time alone or is synchronized by "clock ticks", whereas state transitions in DES are driven by "discrete events" (e.g., press of a button, arrival of a shipment) which can happen asynchronously (at various time instants not necessarily known in advance or coinciding with clock ticks). Typical DES include

[7] Probabilities and conditional probabilities are then associated with each event (frequentist or Bayesian probabilities, depending on the availability of data, more often the latter). The probability of each branch or sequence of events can thus be estimated. These probabilities, along with the consequences of each branch, constitute one form of Quantitative Risk Analysis.

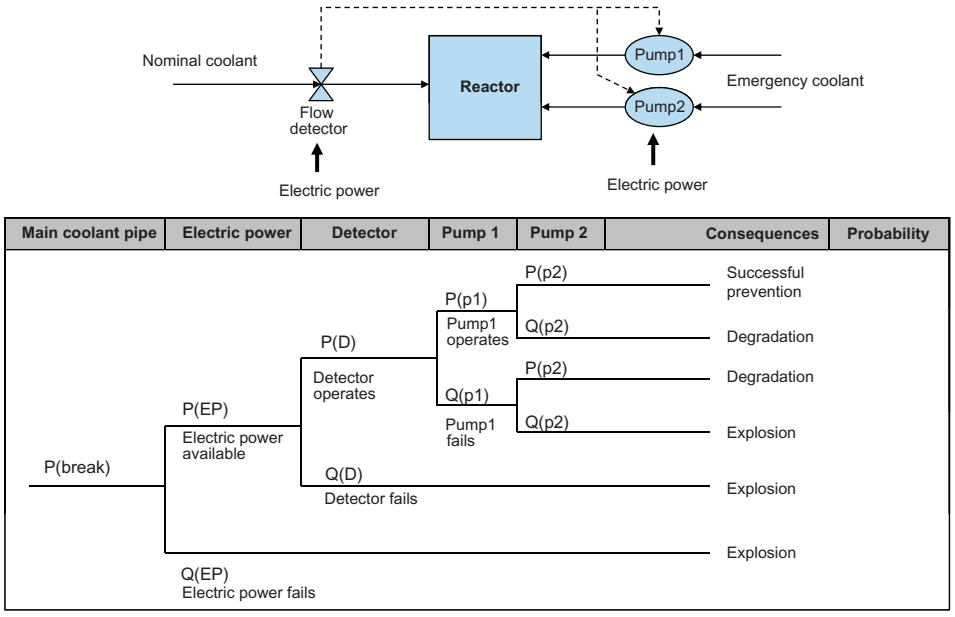

Fig. 1. Simplified Event Tree Analysis for a reactor following the break of main coolant pipe (initiating event). Adapted from Billington and Allan [3].

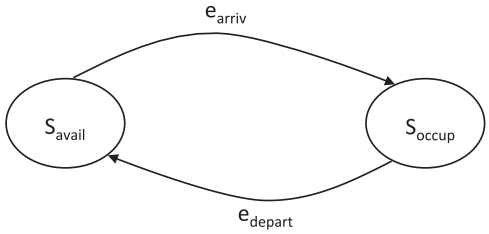

Fig. 2. Simple DES model with two states, dock available (S_{avail}) and dock occupied (S_{occup}), and two events, truck arrival, e_{arriv}, and truck departure, e_{depart}.

queuing systems, communication systems and telephony, databases, manufacturing and traffic systems to mention a few [1]. A DES can *move* from a state x to a new state $\boldsymbol{x}'$ **by the occurrence of event** e. This *motion* defines a *state transition*, and event **e** is said to *label* this transition. Consider the following illustrative example [1]: a warehouse has a single loading dock, which can be in two states, S_{avail} for available, and S_{occup} for occupied. Two events of interest in this example are "truck arrival", labeled e_{arriv}, and "truck departure", labeled, e_{depart}. The state transition diagram for this system is shown in Fig. 2. The event e_{arriv} transitions the system from S_{avail} to S_{occup}, and the event e_{depart} transitions the system from S_{occup} to S_{avail}.

The set of all executable events $\mathbf{e_i}$ associated with a DES constitutes the event space E. The concatenation of n events $\mathbf{e_i}$ is termed a *string* of events. We write $\boldsymbol{s}=\mathbf{e_1e_2}\ldots\mathbf{e_n}$, where $\mathbf{e_1}$ and $\mathbf{e_n}$ are the prefix and the suffix of $\boldsymbol{s}$ respectively. The idea of concatenating events into strings leads to the notion of language: the language L associated with a given DES is defined as the collection of all (finite) strings that can be generated with events $\mathbf{e_i}\in E$. Furthermore, the state transition from $\mathbf{x}$ to $\mathbf{x}'$ labeled by event $\mathbf{e_i}$ is noted as $\boldsymbol{x}'=\delta(\boldsymbol{x}, \boldsymbol{e_i})$. Within the DES framework, safety issues are related to the existence of undesirable strings within the language L, which can lead the system to a set of hazardous states and accidents. More details on DES can be found in the excellent introduction to the subject by Cassandras and Lafortune [5], and its applicability to safety issues can be found Bakolas and Saleh [1]. We now examine accident precursors in the context of DES[8].

Consider the illustrative situation shown in Fig. 3. The set of nominal operational states are grouped to the left of the figure (for example temperature, pressure, and other state variables evolving within the nominal prescribed range in a chemical reactor). A figurative barrier or set of barriers separates nominal from off-nominal operations and system states. Several initiating events (IE_i), for example main coolant pipe rupture, are shown to transition the system past the barrier to the off-nominal region of operations. Additional barriers can exist within this off-nominal region but they are not on the figure for the sake of clarity and to avoid visual clutter. Each initiating event can be propagated and its adverse effect on the system examined, through Event Tree Analysis for example as discussed previously or other risk analysis methods. A different tree, or to use the DES terminology, a different language L is thus associated with each initiating event, $\mathrm{L_i}\rightarrow \mathrm{L}(IE_i)$, and each one consists of multiple branches or strings $\boldsymbol{s}_{i,j}\in \mathrm{L_i}$, some of which may lead to an accident (the second subscript refers to the accident A_j, as will be explained shortly). Consider for example the upper sequence of events shown in Fig. 3: its prefix is IE_1, and the sequence is the concatenation of the events $\boldsymbol{e}_{j,1}$ with $j=1$ to n, leading to the accident event A_1:

$$\boldsymbol{s}_{1,1}(k)=IE_1\mathbf{e}_{2,1}\mathbf{e}_{3,1}\ldots\mathbf{e}_{n,1}A_1 \tag{1}$$

The subscripts refer to the initiating event and the accident event respectively. We include the parameter k to clarify that multiple paths may exist that lead from a given initiating events to an accident event. This parameter is dropped in subsequent notation for compactness but the multiplicity of such paths is always assumed. Each initiating event can have multiple paths to one or more accident events. Similarly, an accident event, for example ignition of flammable gas in an aircraft fuel tank, can be reached through multiple paths and different initiating events. We note for clarity and with a slight abuse of notation the final event (e.g., ignition of the flammable mixture in the aircraft fuel tank) with the same variable as the final state, A_1 (e.g., aircraft fuel tank explosion).

[8] We are grateful for an anonymous reviewer who suggested that other formalisms could also be used to define accident precursors, e.g., statecharts and branching time temporal logic. A comparative analysis of precursors defined in different formalisms (with benchmarking along different criteria) constitutes an interesting topic for future work.

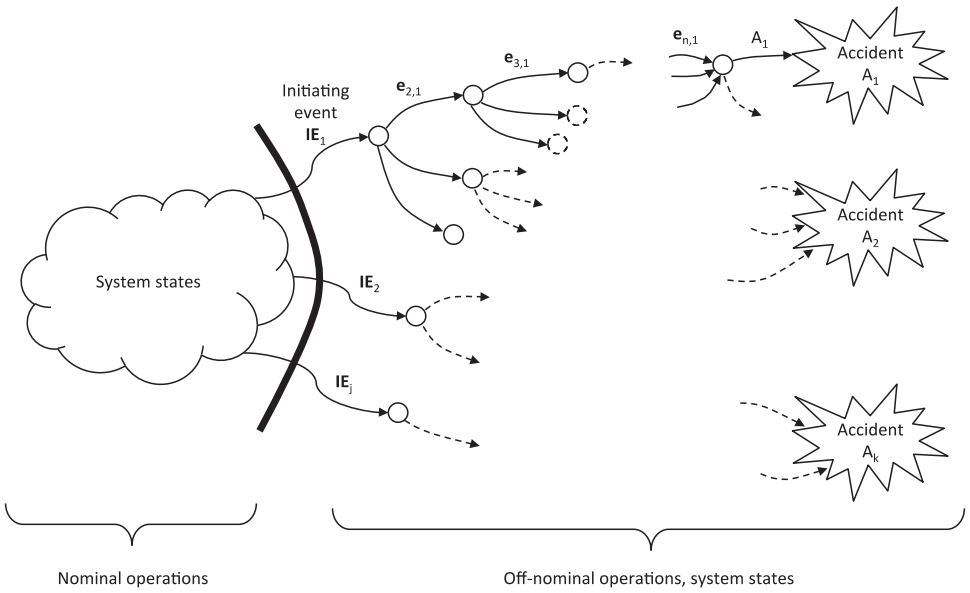

Fig. 3. Illustrative example of nominal and off-nominal system operations/states, with propagations of initiating events towards accidents.

Given these terms, an accident sequence (or accident trajectory) can be formalized using the DES parlance as a string of events within any language L_i and whose suffix is A_j. Said differently, the condition for any string $\boldsymbol{s}_{i,j}$ to qualify as an accident sequence is as follows:

$$\begin{aligned} &\forall i,\ \boldsymbol{s}_{i,j} \in L_i \\ &\boldsymbol{s}_{i,j} \in AcSq \text{ iff } \exists A_j \,|\, suffix(\boldsymbol{s}_{i,j}) = A_j \end{aligned} \tag{2}$$

AcSq is the set of accident sequences. Although embedded in this definition, it is worth clarifying that according to Proposition (2), all events preceding an initiating event (falling within the nominal operation of the system) are not part of an accident sequence.

3.3. Formalization of accident precursors within Discrete Event Systems

The concept of accident precursor is best framed and understood in light of the notion of an accident sequence. Having formalized the latter within the context of DES, we now examine the former within the same modeling framework.

An accident precursor was described previously as a truncated accident sequence. For example, one truncation of the accident sequence shown in (1) is the string of the first three off-nominal events:

$$\boldsymbol{pr} = IE_1 \mathbf{e}_{2,1} \mathbf{e}_{3,1}$$

Note that one set of accident precursors, Δ_1, can be generated by subtracting the suffix of the set of accident sequences:

$$\begin{aligned} \Delta_1 = \{ &\forall i \forall j,\ pr \,|\, \boldsymbol{s}_{i,j} \in AcSq \quad \text{and} \quad pr = \boldsymbol{s}_{i,j} - suffix(\boldsymbol{s}_{i,j}) \\ &\text{for which} \quad prefix(pr) = IE_i \} \end{aligned} \tag{3}$$

Δ_1 consists of all the accident sequences from which the final precipitating event A_j has been removed. Another set of accident precursors Δ_2 can be defined recursively by subtracting the suffix of the precursors in Δ_1. We note as a shorthand the operation as $\boldsymbol{s}_{i,j}$—suffix$^2(\boldsymbol{s}_{i,j})$. More generally, an accident precursor can be defined as follows:

$$\begin{cases} \text{Given } \boldsymbol{s}_{i,j} \in AcSq, \text{ a string of events } pr_{i,m} \text{ qualifies as an accident precursor iff} \\ prefix\,(pr_{i,m}) = IE_i \text{ and } pr_{i,m} = \boldsymbol{s}_{i,j} - suffix^m(\boldsymbol{s}_{i,j}) \end{cases} \tag{4}$$

The set of all such precursors can be noted as Δ_m. In this Proposition (4), the first subscript i of the precursor refers to the initiating event IE_i, the prefix of the accident sequence; the second subscript $m \in \mathbb{N}^*$ refers to the order or depth of truncation of the accident sequence, as indicated in the operator "–suffix$^m(\boldsymbol{s}_{i,j})$". As such, it can serve as one indication of the closeness of an accident precursor to the accident sequence. In the following section, we further examine this idea along with the notions of near miss, warning sign, and accident pathogen in light of this definition of accident precursor.

4. Near miss, warning sign, and accident pathogen

Having defined an accident precursor through the truncation operator of suffixes applied to accident sequences, we can qualify a precursor by its closeness to the complete accident sequence or the extent of this truncation. In this view, a near miss is a special type of accident precursor for which the truncation is minimal (close to the accident end-state or suffix of the accident sequence) and the accident is close to being released. In other words, a near miss is very similar to an accident sequence with the exception of a few missing elements or ingredients, which translate into a few missing events (truncation) in the accident sequence. For example, using the accident sequence in (1), one near miss can be written as:

$$IE_1 \mathbf{e}_{2,1} \mathbf{e}_{3,1} \ldots \mathbf{e}_{n-1,1}$$

A near miss is thus a qualification of an accident precursor and it can be contrasted for example with an "early precursor" for which the truncation of an accident sequence is extensive and much further back from the accident end-state. This idea can be further extended to derive, like the metrics of component importance in reliability and risk analysis [18,25], a measure of the closeness of the precursor to a complete accident sequence I_{pr} as the conditional probability the complete sequence would unfold given that the precursor has occurred:

$$Given\ \boldsymbol{s}_{i,j} \in AcSq,\ I_{pr_{i,m}} = P(\boldsymbol{s}_{i,j} \,|\, pr_{i,m}) \tag{5}$$

The measure I_{pr} can be extended to all accident sequences and over all accidents, and we can define an infinity norm of the

vector I_{pr} for example as follows:

$$|I_{pr_{i,m}}|_{\infty} = \max_{i,j}[P(\boldsymbol{s}_{i,j}|pr_{i,m})] \tag{6}$$

This approach, in which the probabilities considered are Bayesian, can be used in conjunction with accident consequences to prioritize accident precursors and help guide safety interventions. In addition, we define an **accident pathway** as an intermediate string of events within an accident sequence (truncated from both its prefix and suffix). For instance, using the accident sequence in (1), one accident pathway is $u=\boldsymbol{e}_{2,1}\boldsymbol{e}_3$. We can thus extend the precursor importance concept to an accident pathway by analyzing its frequency of overlap with accident sequences. To this effect, we define the function $f_{i,j}$ as follows:

$$\boldsymbol{s}_{i,j} \in AcSq$$
$$f_{i,j} = \begin{cases} 0 & \text{if } u \cap \boldsymbol{s}_{i,j} = \emptyset \\ 1 & \text{otherwise} \end{cases} \tag{7}$$

One relative measure of importance of the accident pathway u (when compared with that of another pathway w) is its frequency or number of participation in various accident sequences leading to accident A_j for example:

$$I_j(u) = \sum_{all\ i} f_{i,j} \tag{8}$$

$I_j(u)$ represents the numbers of accident sequences the string u participates in or contributes to and that lead to accident A_j. The measure can also be extended to all accidents (not just A_j). When used in conjunction with accident consequences, this measure can help prioritize accident pathways and identify where additional barriers within a defense-in-depth strategy [19] would be efficient in blocking multiple accident sequences. This research direction of importance measures for precursors and accident pathways is left as a fruitful venue for future work.

Within the DES context and given the previous definitions of accident sequence and accident precursor, a **warning sign** is both related to and different from both. Consider the accident sequence in (1), $\boldsymbol{s}_{1,1}=IE_1\boldsymbol{e}_{2,1}\ \boldsymbol{e}_{3,1}\ \ldots\ \boldsymbol{e}_{n,1}A_1$. A warning sign can be the flagging of any event occurrence in this sequence[9] . For example, a signal associated with the occurrence of $\boldsymbol{e}_{n,1}$ is warning sign for imminent danger; a signal associated with the occurrence of $\boldsymbol{e}_{2,1}$ is an early warning. More generally, a warning sign can be conceived of as a signal associated with the occurrence of any one event within a string that constitutes an accident sequence, or an indication that the system has assumed a hazardous state labeled by an event in an accident sequence. As such, a "warning sign" or the proverbial "canary in the mine" should not be used interchangeably with "accident precursor" as they cover distinct concepts.

The last expression to be defined is "accident pathogen." A pathogen in a biological sense is by definition a causative agent. Since this term is anchored in the discipline of pathology, a quick overview of this discipline is in order. Pathology as a medical discipline is the study of disease as well as mechanisms and processes of cell/tissue/organ/system "injury" and death. The core of this discipline revolves around four aspects: (1) etiology, (2) pathogenesis, (3) morphological changes, and (4) clinical manifestation [11]. These aspects bear important parallels with risk analysis and can help articulate many safety concepts in an engineering context as will be shown shortly. We will focus on (1), (2), and (4). **Etiology** is the study of causes of diseases, including the identification of pathogens, genetics, and environmental factors (not just a single etiologic agent). **Pathogenesis** is particularly interesting for our purposes as it refers to the "sequence of events in the response of cells or tissues…from the initial stimulus to the ultimate expression of the disease. Even when the initial infectious or molecular cause is known, it is many steps removed from the expression of the disease" [11]. **Clinical manifestation** is the end-result of pathogenesis and morphological changes leading to the expression/manifestation of the disease and the corresponding functional abnormalities at the cell/tissue/organ/system level.

The parallel between pathology and engineering risk analysis are as follows: clinical manifestation corresponds to the analysis and characterization of the accident end-state (A_j) and its consequences (equivalent of injury characterization and death in a biological context); pathogenesis corresponds to the analysis of sequences of events from an initiating adverse event and leading to the accident (the focus of Section 3); and etiology corresponds to the analysis of local factors/causes at each state labeled by an event within an accident sequence that "cause" the subsequence event in the chain to occur (why the transition occurs). These local factors or causes get the system to transition to a more hazardous state until the accident is reached, and can be subsumed under the general term of agonist effects; by contrast, antagonist or inverse agonist effects would correspond to safety barriers or risk de-escalation means.

Having briefly described pathology and its constitutive elements, we can now examine the term accident pathogen in an engineering and risk analysis context.

An accident pathogen is an adverse latent or pre-existing condition, which when compounded with other factors or occurrence of adverse events, can further advance an accident sequence, precipitate an accident (it is a causal factor in an accident sequence), or aggravate its consequences [1]. As such, it is distinct from an accident precursor. For example, a failed emergency power system is an accident pathogen at a nuclear power plant: should the main power system fail, this latent adverse condition will precipitate the accident, or it will cause the sequence to further advance toward a core meltdown. Similarly, trailer siting for contractors and temporary workers below a blow-down drum (open system with no flare) at a chemical refinery, as was the case in the BP Texas City refinery accident (CSB, 2007 [23]; Kaszniak and Holmstrom [9]) is neither an accident precursor nor a warning sign, but an accident pathogen: should the blow-down drum overflow and the volatile raffinate ignite, the consequences of this accident will be significantly more dire in the presence of this accident pathogen than in its absence (all the 15 fatalities at the BP Texas City refinery were in the trailers or the area surrounding them). This distinction completes the discussion in Section 2, which separated adverse events from adverse conditions, and subsumed accident precursors under the former and accident pathogens under the latter.

5. Conclusion

While the terms "accident precursor", "warning sign", and "accident pathogen" are within the same linguistic neighborhood, there are subtle but important differences between them and it is recommended they not be used interchangeably for the sake of accuracy of thought and clarity of communication within the risk and safety community. Finally we note that while DES provides a powerful modeling framework for accident precursors and the other concepts here examined, we believe that **hybrid systems** modeling combining both time-driven and event-driven dynamics would provide an even more compelling modeling

[9] We can also exclude the event A_1 and state that a warning sign is the flagging of any event in any accident precursor.

framework for these concepts than DES. We will explore this research venue in future work.

We believe the medical discipline of pathology, combined with a proper mathematical framework (DES or hybrid systems), provide a richer basis and more interpretive possibilities for examining and understanding risk and safety issues than the pungent but stale Swiss cheese metaphor[10] .

References

[1] Bakolas E, Saleh JH. Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems. Reliability Engineering and System Safety 2010;96(1):184–93.

[2] Bier VM, Yi W. The performance of precursor-based estimators for rare event frequencies. Reliability Engineering and System Safety 1996;50(3):241–51.

[3] Billington R, Allan RN. Reliability evaluation of engineering systems. 2nd edition New York: Plenum Press; 1992.

[4] Carroll JS. Knowledge management in high-hazard industries: accident precursors as practice. In: Phimister JR, Bier VM, Kunreuther HC, editors. Accident precursor analysis and management: reducing technological risk through diligence. Washington, DC: The National Academies Press; 2004 p. 127–36.

[5] Cassandras CG, Lafortune S. Introduction to discrete event systems. Boston, MA, US: Springer-Verlag; 2008.

[6] Cowlagi RV, Saleh JH. Coordinability and consistency in accident causation and prevention: formal system-theoretic concepts for safety in multilevel systems, Risk Analysis, in press, DOI: 2010.1111/j.1539-6924.2012.01886.x.

[7] Hopkins A. Was three mile island a 'normal accident'? Journal of Contingencies and Crisis Management 2001;9(2):65–72.

[8] Johnson JW, Rasmuson DM. The US NRC′s accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information. Reliability Engineering and System Safety 1996;53(2):205–16.

[9] Kaszniak M, Holmstrom D. Trailer sitting issues: BP Texas City. Journal of Hazardous Materials 2008;159:105–11.

[10] Kirwan B, Gibson WH, Hickling B. Human error data collection as a precursor to the development of a human reliability assessment capability in air traffic management. Reliability Engineering and System Safety 2007;93(2):217–33.

[11] Kumar V, Abbas AK, Fausto N, Aster J. Robbins and Cotran pathologic basis of disease. Philadelphia, PA: Saunders Elsevier; 2005.

[12] Minarick JW. The US NRC accident sequence precursor program: present methods and findings. Reliability Engineering and System Safety 1990;27(1): 23–51.

[13] NASA. Nasa accident precursor analysis handbook (NASA/SP-2011-3423). Available from: 〈http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120003292_2012003430.pdf〉. [accessed 2011].

[14] Phimister JR, Bier VM, Kunreuther HC, editors. Accident precursor analysis and management: reducing technological risk through diligence. Washington, DC: The National Academies Press; 2004.

[15] Phimister JR, Oktem U, Kleindorfer PR, Kunreuther H. Near-miss management in the chemical process industry. Risk Analysis 2003;23(3):445–59.

[16] Precursor 2011, In Oxford English Dictionary. Available from: 〈http://www.oed.com/viewdictionaryentry/Entry/149764〉. [accessed 08.05.11].

[17] Precursor 2012, In Merriam-Webster Dictionary. Available from: 〈http://www.merriam-webster.com/dictionary/precursor〉. [accessed 16.10.12].

[18] Rocco CM, Ramirez-Marquez JE. Innovative approaches for addressing old challenges in component importance measures. Reliability Engineering and System Safety 2012;108:123–30.

[19] Saleh JH, Marais KB, Bakolas E, Cowlagi RV. Highlights from the literature on accident causation and system safety: review of major ideas, recent contributions, and challenges. Reliability Engineering and System Safety 2010;95(11):1105–16.

[20] Saltmarsh EA, Saleh JH, Mavris DN. Accident precursors: critical review, conceptual framework, and failure mechanisms. In: Stig O. Johnsen (Chair), Proceedings of the 11th international probabilistic safety assessment and management conference and the annual European safety and reliability conference, Helsinki, Finland, June 2012.

[21] Skogdalen JE, Vinnem JE. Combining precursor incidents investigations and QRA in oil and gas industry. Reliability Engineering and System Safety 2011;101:48–58.

[22] Smith CL, Borgonovo E. Decision making during nuclear power plant incidents: a new approach to the evaluation of precursor events. Risk Analysis 2007;27(4):1027–42.

[23] US Chemical Safety and Hazard Investigation Board, Investigation report: refinery explosion and fire, 2007.

[24] US NRC. Precursors to potential severe core damage accidents: 1998 (NUREG/CR-4674 ORNL/NOAC-232 vol. 27). Available from: 〈http://pbadupws.nrc.gov/docs/ML0037/ML003733843.pdf〉. [accessed 1998].

[25] Van der Borst M, Schoonakker H. An overview of PSA importance measures. Reliability Engineering and System Safety 2001;72(3):241–5.

[26] Vinnem JE, Hestad JA, Kvaløy JT, Skogdalen JE. Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. Reliability Engineering and System Safety 2010;95(11): 1142–53.

[10] The metaphor is over-used in safety discussions, and while useful in some ways, it seems to have crystallized a flawed understanding of accident causation and prevention. For example, the slices (defenses) act as passive antagonist features in the metaphor, preventing an accident sequence from progressing, but absent are risk de-escalation means (inverse agonist), critical elements of any proactive accident prevention strategy; and the alignment of the holes in the metaphor can convey the false impression than an accident sequence is instantaneous and does not progress by jerks, when this is often the case and accident pathogens build-up over different time scales before an accident is released (temporal depth of causality of system accidents, see for example Cowlagi and Saleh [6]).