Coordinability and Consistency in Accident Causation and Prevention: Formal System-Theoretic Concepts for Safety in Multilevel Systems

Raghvendra V. Cowlagi,¹ Joseph H. Saleh²

Although a “system approach” to accidents in sociotechnical systems has been frequently advocated, formal system theoretic concepts remain absent in the literature on accident analysis and system safety. To address this gap, we introduce the notions of coordinability and consistency from the hierarchical and multilevel systems theory literature. We then investigate the applicability and importance of these concepts to accident causation and safety. Using illustrative examples, including the worst disaster in aviation history, the Tenerife accident, and recent incidents in the U.S. of aircraft clipping each other on the tarmac, we propose that the lack of coordinability is a fundamental failure mechanism causing or contributing to accidents in multilevel systems. We make a similar case for the lack of consistency. Coordinability and consistency become ingredients for accident prevention, and their absence fundamental failure mechanisms that can lead to system accidents. Finally, using the concepts introduced in this work, we identify several venues for further research, including the development of a theory of coordination in multilevel systems, the investigation of potential synergies between coordinability, consistency, and the High Reliability Organizations paradigm, and the possibility of reframing the view that “sloppy management is the root cause of many industrial accidents” as one of lack of coordinability and/or consistency between management and operations.

By introducing and expanding on the concepts of coordinability and consistency, we hope to contribute to the thinking about, and the language of, accident causation and prevention and to add to the intellectual toolkit of safety professionals and academics.

KEY WORDS: multilevel systems, coordinability, consistency, accident causation, system theory

1. INTRODUCTION

Sociotechnical systems, such as air traffic control, offshore platforms, and nuclear power plants are not merely technical or engineering systems, but have intrinsic organizational and managerial dimensions to them that contribute to their safety or the lack thereof. The accident analysis and system safety literature often reports on a distinct class of adverse events initially termed “man-made disasters”¹ and later characterized as “organizational” accidents² or “system” accidents.³ These two qualifiers, “organizational” and “system,” are used to indicate on the one hand an organizational contribution to accident causation beyond the traditional technical and human error factors, and on the other hand a recognition that accidents can occur due to the interactions between the elements of a system, rather than failures of the elements themselves.⁴

¹Aurora Flight Sciences Corp. R &D Center, Cambridge, MA, 02472, rcowlagi@mit.edu
²School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA 30332, jsaleh@gatech.edu
The following are two distinctive features of system accidents:

(1) The chain of causality, or chain influence, leading to the accident extends beyond the temporal vicinity of the moment the accident occurred, with build-up of accident pathogens occurring over different time-scales before an initiating event triggers an accident sequence. This characteristic can be termed the *temporal depth of causality* of system accidents.

(2) The safety value chain, that is, groups and individuals who influence or contribute to the accident occurrence/prevention, extends far beyond the immediate victims, who may or may not have contributed to the accident. This characteristic can be termed the *diversity of agency* in system accidents, and it will be in part the focus of this work.

This class of adverse events, system accidents, is different from occupational accidents, for example a "slip, trip, and fall" in which the agent and the victim are the same individual. Occupational accidents, of particular interest to epidemiologists, are not discussed in this article. System accidents, typically but not exclusively associated with large-scale releases of energy, are the focus of this work.

The wide variety of examples of system accidents described in the literature, from the nuclear industry,\(^5\) the oil and gas,\(^6,7\) chemical,\(^8,9\) and mining industries\(^10\) to name a few, highlights the importance of a thorough understanding of the etiology of system accidents, an understanding that in turn can serve to prevent or mitigate such accidents. When carefully analyzed, many system accidents share an underlying sameness in the way they occur, through a combination of technical design flaws, operational failings, and deficient organizational behaviors or poor management practices (sometimes unchecked by ineffective regulatory context). This underlying sameness may reflect deficiencies in the theoretical understanding of system accident causation and prevention, and it constitutes a compelling motivation for fundamental research in this area. This work contributes one step in this direction towards a formal foundation of safety in multilevel systems.

Two important ideas undergird the current literature on accident causation and system safety: 1) that safety is a “control problem”; and 2) that it requires a “system theoretic” approach to be dealt with.\(^11\) The present work builds on and extends these ideas. Other major contributions to this literature include the High Reliability Organizations (HRO) paradigm, which emphasizes managerial and organizational factors affecting system safety\(^3\), and the technical Probabilistic Risk Assessment (PRA) approach, which focuses on the modeling of stochastic chain of events progressing through various “risk scenarios” and leading to an accident, and the assessment of its consequences.\(^4\) For a review of these and other approaches to accident causation and system safety, the reader is referred to Saleh et al\(^11\) and the references therein. Important synergies between these and the current approach, especially between HRO and the present work, will be pointed out later in this work as important venues for future research.

1.1 System Safety as a Control Problem

The control perspective on system safety refers to the fact that accidents typically result from the absence or breach of defenses, technical and organizational safety barriers, or from the violation of safety constraints.\(^4,12,13\) Conversely, system safety is supported by the establishment of defenses and safety barriers – the general principle is known as defense-in-depth in the nuclear industry and layers of protection in the process industry. Defenses and safety barriers can be conceived of and are in effect as means of controlling the system state from drifting to an unwanted/hazardous region in the state space. Whereas the safety principle of defense-in-depth, which reflects an implicit recognition of accident prevention as a control problem, was first conceptualized in the nuclear power industry in the 1950s, the explicit recognition and articulation of this perspective was recently developed by several authors, including Rasmussen\(^12\) and Leveson\(^4\).

Control Theory however has been to a large extent absent from the discussions of safety as a control problem. One recent exception is the work by Bakolas and Saleh\(^14\) in which concepts and tools from the actual discipline of Control Theory, in particular the notions of controllability and observability, are applied to complex engineering systems or socio-technical systems, and analyzing different aspects of possible adverse events.

\(^3\)HRO derives from a set of empirical studies that identified managerial practices and organizational behaviors of organizations that have been successful in handling risk and minimizing safety disruptions despite the hazardous nature of their work.

\(^4\)PRA can be conceived of as a formalization of an anticipatory Bayesian rationality, applied to complex engineering systems or socio-technical systems, and analyzing different aspects of possible adverse events.
were brought to bear on the intrinsically multidisciplinary problem of accident causation and prevention. The reader interested in further details is referred to the works cited herein.

1.2 System Theoretic Approach to Safety and Accident Causation

A system theoretic approach to accident causation and prevention is a synthesis of several ideas. The heading “system theoretic approach” is adopted to indicate a basis in general system theory. The main idea subsumed under this heading is that accidents can result “from dysfunctional interactions among system components” (4), not just component failures. While having greater importance in modern software-intensive systems, these “interactive” failure mechanisms have not yet received careful attention (17) and their theoretical basis is still lacking. A system theoretic approach to safety and accident causation is meant to address this deficiency. More specifically, it is intended to deal with attributes that emerge from the interactions of components, subsystems, and stakeholders in sociotechnical systems (see Fig. 1), and not only of single component failures for example.

1.3 Crosstalk between Academic Disciplines and Objectives of this Work

Different academic and professional communities have grappled with the multidisciplinary issues of system safety and accident causation, including psychologists, sociologists, engineers, and management scientists. Unfortunately, not enough crosstalk between academic disciplines occurs, and even within engineering, limited interaction has occurred between the risk/accident analysis and safety science community and the Control Theory community. This is an unfortunate state of affairs as the problems, methods, and tools of each community can be mutually helpful and enriching to the other in support of the safety agenda.

Bakolas and Saleh (14) brought together the disciplines of Control Theory and Risk Analysis to bear on the multi-disciplinary problem of system safety and accident prevention (see §1.1). In this work, we adopt a similar approach, except that instead of focusing on the control theoretic perspective, we tackle the system theoretic approach to safety (the idea presented in §1.2). It is surprising that just like Control Theory has been absent from the discussions of safety as a control problem, formal system theoretic concepts have also been absent from the discussions of safety as a “system theoretic problem.” It is useful to identify fundamental accident mechanisms and principles of safe design and operation of sociotechnical systems using sound theoretical foundations. Some of these foundations of hierarchical multilevel systems were first developed in the seminal work of Mesarović et al (18) but they are conspicuously missing in the safety literature. They will be introduced and discussed in this work.

Our two related objectives in this article are the following: 1) to introduce theoretical concepts from the literature on hierarchical and multilevel systems, in particular those of coordinability and consistency, to the accident analysis and system safety community; and 2) to investigate the applicability of these concepts to the identification of fundamental failure mechanisms causing or contributing to accidents in sociotechnical systems. By introducing these concepts, we hope to contribute to the thinking about, and the language of, accident causation and prevention and to help expand the intellectual toolkit of safety professionals and academics.

The rest of this paper is organized as follows: in §2, we introduce the system theoretic concepts of coordinability and consistency and present an illustrative example highlighting their importance in multilevel systems. In §3 and §4, we investigate, respectively, the implications of coordinability and consistency for accident causation and system safety, and we explore several examples of system accidents, which are related to a lack of coordinability or consistency. Finally, in §5, we provide a summary and critical assessment of coordinability and consistency.
in accident causation and system safety, and we indicate further extensions and possible applications of these concepts.

2. COORDINABILITY AND CONSISTENCY IN HIERARCHICAL MULTILEVEL SYSTEMS

In this section, we introduce the formal concepts of coordinability and consistency in hierarchical multilevel systems using the terminology and definitions of Mesarović et al.\(^{18}\) Our purpose is to lay the grounds for the use of these concepts in the analysis of accident causation and system safety in §3 and §4, in particular for the identification of failure mechanisms contributing to accidents in multilevel systems.

2.1 System Structure and Terminology

We represent a system as a mapping between a set of inputs and a set of outputs\(^5\). In particular, a decision-making system chooses a decision \(x\) to solve a decision problem \(D\). The output \(y\) of a decision-making system is a transformation \(\pi\) of the decision, i.e., \(y = \pi(x)\). A decision problem, in general, involves the selection of a decision that satisfies a pre-specified set of constraints and may involve the optimization of a cost or reward function. A two-level hierarchical system, consisting of a single higher-level unit and \(N\) lower-level units, and controlling a certain process, is shown in Fig. 2. Using the terminology of Mesarović et al.\(^{18}\), we refer to the higher level decision-making unit as the supremal unit and to the lower level decision-making units as the infimal units.

Each of the \(N\) infimal units contributes to controlling the process: the \(i\)th unit provides input \(y_i\) to the process and receives feedback \(z_i\) from the process. The supremal decision-making unit provides an input \(\gamma_i\) to the \(i\)th infimal unit, and receives feedback \(\omega_i\) from that unit. The decision problem of each infimal unit depends on the input \(\gamma_i\). These variables are summarized in Table I.

In this example, the input \(\gamma\) provided by the supremal unit to the infimal unit corresponds first to the runway number and taxiway provided by the ATC to the flight crew, and then to the signal of clearance for take-off. The feedback \(\omega\) from the infimal unit to the supremal unit corresponds to the acknowledgement of the runway number and taxiway assigned, to “holding short,” and to the request for clearance for take-off (and the acknowledgement when clearance is granted). The input \(y\) given by the infimal unit to the process corresponds to the aircraft control inputs that the flight crew uses to maneuver the aircraft (e.g., throttle and rudder pedal), and the feedback \(z\) corresponds to the feedback received by the flight crew from the various sensing and measurement equipment of the aircraft.

2.1.1 Hierarchy of decision problems

In this example, the supremal decision problem consists of two sub-problems: first, the supremal unit (ATC) must select and assign a runway and how to taxi to that runway, and second, the supremal unit must decide when to clear the aircraft for take-off from the hold short line. Similarly, the infimal decision problem consists of two sub-problems: the first is to identify the runway and taxiway assigned by the ATC and taxi up to the hold short line, and the second to perform the take-off from the runway when the ATC clears it for take-off. Finally, the overall decision problem in this example can be set as ensuring safe ground movement and take-off. The hierarchy of decision problems, and the associated decision and output variables, are summarized in Table II.

Note that the overall problem in a hierarchical system is what the supremal and infimal units attempt to jointly solve by addressing their local
Table I. Summary of variables in a two-level hierarchical system.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supremal Unit</td>
<td>$\gamma_i$</td>
<td>Input provided by the supremal unit to the $i^{th}$ infimal unit (also referred to as the coordination input to the $i^{th}$ infimal unit)</td>
</tr>
<tr>
<td></td>
<td>$\omega_i$</td>
<td>Feedback received by the supremal unit from the $i^{th}$ infimal unit</td>
</tr>
<tr>
<td>Infimal Unit</td>
<td>$x_i$</td>
<td>Input provided by the $i^{th}$ infimal unit to the process (also referred to as the control input to the process by the $i^{th}$ infimal unit)</td>
</tr>
<tr>
<td></td>
<td>$z_i$</td>
<td>Feedback received by the $i^{th}$ infimal unit from the process</td>
</tr>
</tbody>
</table>

Fig. 3. Illustration of the concept of coordinability.

decision problems. The supremal unit cannot solve by itself the overall decision problem (e.g., ATC does not perform the taxiing and take-off) but provides the coordination inputs $\gamma$ to the infimal units, which define the latter’s decision problems, $D_{I,i}(\gamma)$. The infimal units in turn, by solving their $D_{I,i}(\gamma)$, affect the process in ways that would solve the overall decision problem (hence the importance of coordination or the selection of $\gamma$ for example). This observation will lead shortly to the concepts of coordinability and consistency.

In some cases (but not always) as noted by Mesarović et al. (18) the solution to the infimal decision problem $D_{I,i}(\gamma_i)$ is the input to the process. However in order to maintain the generality of the framework and subsequent analysis, the solution to the infimal decision problem is distinguished from the process input and noted as $x_i$, that is $D_{I,i}(\gamma_i) = x_i$. Consequently the input to the process, $y_i$, may be identical to or obtained through a transformation/implementation of $x_i$. In our ATC example, the solutions to the infimal decision problems $x_i$ are first the actual physical identification of the runway and taxiway with the runway number and taxiway designation assigned by ATC, and second, the binary decision to perform or abort the take-off.

Within this context of hierarchical multilevel systems, we first introduce the notion of coordinability of the infimal decision problem relative to the supremal decision problem (18). Coordinability is of central importance for multilevel systems. Conceptually, coordinability relative to the supremal decision problem means that there is at least one solution to the supremal problem such that each of the corresponding infimal problems has at least one solution. Recall that the each infimal decision problem is determined or specified by the solution of the supremal problem. Coordinability relative to the supremal decision problem therefore means that the supremal unit can solve its decision problem, and subsequently for that solution, all the infimal units can solve their associated problems (in other words, for every supremal decisions, at least one of the corresponding infimal decision problems has no solution). These issues are graphically illustrated in Fig. 3.

The way the concept of coordinability was devised, in relation to the decision problems, can be extended to introduce the concept of consistency. Consistency, as proposed by Mesarović et al. (18) relates all the decision problems noted previously (see Table II) – conceptually, the two-level system of Fig. 2 is “consistent” if the overall decision problem is solved when the supremal unit and each of the infimal units solve their own decision problems. In other words, consistency in multilevel systems means that by solving their local decision problems, the infimal and supremal decision units solve the overall

---

6Mesarović et al. (18) introduce a second concept called coordinability relative to the overall decision problem; this concept is not adopted in our work.
Table II. Summary of the hierarchy of decision problems and associated variables in a two-level system.

<table>
<thead>
<tr>
<th>Decision problem</th>
<th>Symbol</th>
<th>ATC example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall decision problem</td>
<td>$\bar{D}$</td>
<td>Ensure safe ground movement and take-off</td>
</tr>
<tr>
<td>Supremal unit decision problems</td>
<td>$D_S$</td>
<td>Select and assign a runway and taxiway (to the infimal unit)</td>
</tr>
<tr>
<td>Coordination inputs</td>
<td>$\gamma_i$</td>
<td>Decide when to clear the aircraft for take-off from the hold short line Runway number and taxiway designation (assigned to the infimal unit) Binary decision of withholding/providing clearance for take-off</td>
</tr>
<tr>
<td>Infimal unit decision problems</td>
<td>$D_{1,i}$</td>
<td>Identify the runway and taxiway assigned by the ATC, and taxi up to the hold short line of the runway</td>
</tr>
<tr>
<td>Process inputs</td>
<td>$x_i$</td>
<td>Perform take-off after requesting and being granted clearance by ATC Aircraft control inputs (e.g. throttle, rudder controls) to follow taxiway Aircraft control inputs to perform/abort take-off</td>
</tr>
</tbody>
</table>

Fig. 4. Illustration of the concept of consistency.

problem. More specifically, consistency requires that solutions to the supremal and infimal decision problems exist, i.e., that the system is coordinable, and that all these solutions result in the overall problem being solved. These issues are graphically illustrated in Fig. 4.

As a side note, it is interesting to quote the famous economist John Galbraith on consistency in the “industrial state”:

“The relationship between society at large and an organization must be consistent with the relation of the organization to the individual. There must be consistency in the goals of society, the organization, and the individual.” – Galbraith\(^{(19)}\), quoted in\(^{(18)}\).

We will argue that a similar consistency should exist, on a smaller scale, within hazardous industries in order to prevent accidents and sustain system safety (e.g., between regulators, management, operators and the processes they oversee).

In what follows, to further motivate the importance of analyzing the interactions in a hierarchical multilevel system, we present an illustrative example of major importance in robotics, which we argue has important parallels in system accidents. We then provide formal definitions of coordinability and consistency.

2.1.2 Real-world issues

The model in Fig. 2, and the preceding discussion based on this model are simplified versions of the messy reality of multilevel systems and hierarchical decision-making. Complexities may arise due to the structure of the hierarchical system when more than two levels are present in the system, more than one supremal unit is considered, and multiple supremal inputs are received by an infimal unit. Furthermore, there may exist lateral interactions between infimal units mutually shaping each other decision problems. On the other hand, complexities may also arise due to the nature of the decision-making problems of the supremal and infimal units (e.g. multi-criteria optimization, ill-defined cost functions, etc.).

Nevertheless, simplification in any modeling effort is often necessary to isolate and identify particular phenomena of interest, and it is mainly justified on pragmatic terms and based on its ability to yield insights despite its limitations. Our simplified hierarchical model is meant to introduce
and formalize the concepts of coordinability and consistency, which are significantly rich in interpretive possibilities and actionable results for accident causation and prevention (despite the simple nature of the underlying model). The limitations of the model nevertheless have to be acknowledged; addressing them through a more involved model structure, for example, constitutes a good platform for future research.

2.2 Illustrative Example: Hierarchical Motion Planning and Coordinability

The example that follows represents the archetype of a coordinability problem in robotics and motion planning, which is the subject of a growing literature and research efforts in the control community. It is included here to further ground the concepts introduced in this work, and to give a tangible illustration of their importance, practical and theoretical, for addressing issues that emerge in hierarchical multilevel systems.

Autonomous vehicles, such as driverless cars, personal robots, and drones (unmanned aerial vehicles), are likely to be ever more present in our future. The ability to both plan and execute its own motion is a defining characteristic of an autonomous mobile vehicle. Autonomous motion planning and control is typically implemented using a two-level hierarchy. The higher level, called the geometric path planning level (the supremal unit), mainly addresses the satisfaction of the specifications of the motion planning problem, i.e., the completion of high-level tasks assigned to the vehicle (for instance, “Go from here to there while avoiding all obstacles”, or “Validate parking in this area”, or “Detect and defuse landmines in this region”). The higher level planner computes a geometric path through the environment that enables the satisfaction of the specified vehicle task. The lower level planner, called the trajectory generation level (the infimal unit), mainly addresses the “execution” of the geometric path computed by the higher level planner in accordance with the vehicle’s kinematic and dynamic constraints. Thus, the lower level planner computes feasible control actions to drive the vehicle along the higher level geometric path.

A critical problem emerges in this hierarchical structure: the geometric path planning level may specify a path – a solution to the supremal decision problem – that is not necessarily feasibly traversable by the vehicle. In other words, the lower level may be unable to execute the motion plan computed by the higher level. Figure 5 illustrates this situation: the obstacle-free path commanded is infeasible due to minimum turn radius capability of the vehicle. Consequently, the vehicle, while attempting to track the path specified by the motion planner (the supremal unit), will run into the obstacle, i.e., an accident will occur. This is fundamentally a problem of lack of coordinability between the infimal and supremal units (see the Appendix for additional details). The problem of designing motion planners with coordinable interactions between the higher and lower levels is an important subject of current robotic research.

2.3 Formal Treatment of Coordinability and Consistency

A formal mathematical treatment of coordinability and consistency brings additional precision to these concepts and provides them with a general interpretation not tied to any specific application. By the same token, such mathematical treatment can help identify fundamental principles and spur further investigation into their implementations in various contexts and industries.

The formal definitions of coordinability and consistency are based in part on predicate logic, the basic elements of which are briefly recalled here: a proposition is a statement that can be either true or false. For example, the statement “The Earth is flat” is a valid proposition, but the sentence “Will it rain today?” is not. A predicate indicates either a property of an object or a relationship between different objects. A predicate acting on a particular object is a proposition.

Returning to the two-level system depicted in
true
consistent
\( \gamma \)
i
\( x_i \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( D \)
i
\( \exists x \)
i
\( \exists x \)
i
\( P(x, D_{1,i}(\gamma)) \)
i
\( P(\gamma, D_S) \)
it
\( P(\pi(x_i), D) \)
i
\( \forall x \)
i
\( \forall x \)
i
\( (\forall x) \)
i
\( (\forall x) \)
i
\( (\forall x) \)
i
\( (\forall x) \)

Fig. 2, we denote by \( D_S \) the supremal decision problem and by \( D_{1,i} \) the decision problem of the \( i \)th infimal unit. Correspondingly, we denote the supremal decision by \( \gamma = (\gamma_1, \gamma_2, \ldots, \gamma_N) \), and by \( x_i \) the \( i \)th infimal unit’s decision. The output of the supremal unit is the supremal decision \( \gamma \) and the output of the \( i \)th infimal unit driving the process is \( y_i = \pi(x_i) \).

Recall that the supremal unit defines the decision problems of the infimal units through the coordination inputs \( \gamma \). To explicitly acknowledge this dependence, we denote by \( D_{1,i}(\gamma_i) \) the \( i \)th infimal decision problem, and \( D_1(\gamma) = \{D_{1,1}(\gamma_1), D_{1,2}(\gamma_2), \ldots, D_{1,N}(\gamma_N)\} \) the set of infimal problems. Similarly, \( x \) and \( y \) denote the collected \( N \)-tuple of the infimal units decisions and outputs. Finally, we denote the overall decision problem of the two-level system by \( \mathcal{D} \).

To present precise definitions of coordinability and consistency, we introduce a logical predicate \( P(\cdot, \cdot) \) defined as \( P(x, D_{1,i}) \equiv "x \text{ is a solution to the decision problem } D_{1,i}." \). Then, the infimal decision problems \( D_{1,i}(\gamma_i) \) are said to be \textit{coordinable relative to the supremal decision problem} if the following proposition is true \(^{(18)}\):

\[
(\exists \gamma)(\exists x) \left[ P(x, D_{1,i}(\gamma)) \right. \left. \land P(\gamma, D_S) \right]. \tag{1}
\]

Proposition (1) is read as follows: there exists a \( \gamma \) and a \( x \), such that \( \gamma \) solves the supremal decision problem and \( x \) solves the infimal decision problems. In other words, there exist some solution(s) to the supremal decision problem for which the infimal units can also solve their problems (defined by \( \gamma \)). Said differently, the supremal unit can solve its decision problems \( D_S \) and its coordinating inputs define problems \( D_{1,i}(\gamma) \) for the infimal units, all of which can be solved (by the decisions \( x \)).

The infimal and supremal decision problems are said to be \textit{consistent} if the following proposition is true \(^{(18)}\):

\[
(\forall \gamma)(\forall x) \left[ P(x, D_{1,i}(\gamma)) \right. \left. \land P(\gamma, D_S) \right] \implies P(\pi(x), \mathcal{D}). \tag{2}
\]

Proposition (2) is called the \textit{consistency postulate} in Mesarović et al. \(^{(18)}\) and its reads as follows: if a system is coordinable, and for all joint solutions to the supremal and infimal units (\( \gamma \) and \( x \) respectively), the outputs \( \pi(x) \) of the infimal units solve the overall decision problem \( \mathcal{D} \), then the system is said to be consistent. In other words, if a system is consistent, the overall decision problem is solved whenever the supremal decision unit coordinates the infimal units relative to its own objective \( D_S \).

Next, we examine the concepts of coordinability and consistency and their potential contributions to accident causation and system safety.

3. IMPLICATIONS OF
COORDINABILITY FOR ACCIDENT
CAUSATION AND SYSTEM SAFETY

We propose that the lack of coordinability – specifically, the lack of coordinable input by the supremal unit \( \gamma \) – is a fundamental failure mechanism leading to system accidents. We analyze two examples of accidents, the first specific and the second generic, to illustrate the lack of coordinability as an accident causation mechanism. In what follows, we clearly delineate the facts and descriptions of the accidents from our analyses of these accidents.

3.1 Civil Aviation: The Tenerife Disaster

The Tenerife accident is considered the worst disaster in aviation history. A brief description of the accident is here provided as it appeared in the accident investigation report:\(^{(25)}\)

3.1.1 Facts and Description

On March 27, 1977, about 1706 local time, Pan Am Flight 1736, a Boeing 747-121, collided with KLM Flight 4805, a Boeing 747-206B on the only runway of Los Rodeos Airport, Tenerife, Spain. The Pan Am flight was back-taxiing along the runway and was instructed to take exit C-3 off the runway towards the hold-short line, but missed the exit. The KLM flight was holding short at the same runway, and attempted take-off while the Pan Am flight was still on the runway. The KLM flight was traveling at approximately 160 mph when its landing gear and its engines collided with the fuselage of the Pan Am flight. All 234 passengers and 14 members of the flight crew aboard the KLM flight were killed in the accident. Of the 380 passengers and 16 members of the flight crew aboard the Pan Am flight, only 61 passengers and 5 crew members survived. Overall, the accident involved a loss of 583 lives.

The disaster was the result of a significant number of contributing factors: a bomb scare at the original destination of both aircraft (Gran Canaria Airport); a crowded airport at Tenerife as a result of the closing of Gran Canaria; an
undermanned ATC that weekend at Tenerife and inexperienced in handling high traffic load; fog descending on the single runway and significantly limiting visibility; and communication problems and ambiguities between ATC and crew. These factors have been thoroughly commented upon in the press and the technical literature and will not be repeated here. Instead, we focus on one aspect of the disaster, described as follows:

The investigation of the accident\(^2\) reveals that the ATC instructed the Pan Am flight crew to begin taxiing to the start of the only runway of the airport at about 1702 local time. Due to congestion at the airport, the Pan Am flight crew was instructed to taxi along a portion of the runway itself in the reverse direction (this process is known as “backtaxiing”) and take exit C-3 off the runway. However, the Pan Am flight crew was unable to identify and follow the assigned taxi route, specifically, they were unable to locate exit C-3 and continued backtaxiing along the runway. The fatal coincidence in this disaster was the premature take-off of the KLM coupled with the taxiing too far of the Pan Am. It is interesting to note that the Dutch authorities conducted separate ground tests and concluded “in all probability no fatal collision would have occurred if the Pan Am aircraft had not taxied farther than the third intersection, which was emphatically instructed by the tower controller”\(^2\)\(^6\). Degraded visibility at the airport and other evidence clearly support the conclusion that the exit was not identifiable for the Pan Am crew.

3.1.2 Analysis

The hierarchical control structure is familiar: we identify the ATC as the supremal unit and the flight crews of the two aircraft as the two infimal units. As before, the overall decision problem $\mathcal{D}$ is the problem of ensuring safe take-off for both aircraft.

Our analysis hinges on the observation that the Pan Am crew was required to identify the runway exit C-3, which, by all accounts and supporting evidence, was a task that was not feasible for the Pan Am crew. In other words, one of the infimal units in the overall system, i.e., the Pan Am crew, was not coordinable with respect to the supremal unit’s decision. This point deserves further emphasis in light of the discussion in §2: the supremal unit

\(^{7}\)Due probably to a confusion between a departure clearance and a take-off clearance.

3.2 Marine Transport: Accidents due to Shipmaster-Pilot Interactions

3.2.1 Facts and Description

The Maritime Transport System (MTS), in particular two of its elements, cargo ships and tankers, are vital for the functioning of the world economy. Whereas marine accidents rarely get media attention, the reality is that “there continue to be many hundreds of [marine] accidents every year, with a substantial proportion leading to significant vessel damage, pollution and/or loss of life.”\(^{27}\) For example, in 2010 and within EU waters alone, 644 vessels were involved in 559 “significant accidents,” 80% involved large ships (greater than 500 gross tonnage, gt), with collisions and groundings as the major accident modes. Worldwide, the situation is bleaker, and about 90 total loss of vessels are reported to occur per year.\(^{28}\) In the context of this
paper, we focus on the specific aspect of pilotage waters and the role of the marine pilot, described as follows:

Harbors, channels, and other waterways with restricted depth or width, worldwide, are classified as compulsory pilotage waters. The classification as a compulsory pilotage waters implies that any vessel involved in trade or commerce, above a certain size (e.g., greater than 750 gt in the San Francisco area) has to employ the services of a licensed marine pilot. A pilot is not member of the crew of a ship, but boards the vessel close to the boundary of the pilotage waters and takes control of the ship’s conduct and maneuvers within these waters and during berthing/unberthing. In other words, large ships for example entering a harbor and docking are not piloted by the captain or shipmaster, but by an outsider to the ship, the pilot, who has local maritime knowledge (e.g., of local hazards) and experience in the area.

A study by the Transportation Safety Board of Canada of 273 vessel accidents in Canadian pilotage waters identified 42% of the accident as the result of misunderstanding or breakdown in communication between pilot and master (and 46% involved misjudgment by pilot or master). Although no similar data exist for the worldwide maritime transport system, it is fair to assume that shipmaster-pilot relationship contributes to a large number of shipping accidents worldwide.

3.2.2 Analysis

The interactions between the pilot (supremal unit), the shipmaster (infimal unit), and the vessel (process) are similar to the hierarchical structure in Fig. 2. We propose that shipping accidents that may be attributed to shipmaster-pilot interactions are rooted in the lack of coordinability. In light of Fig. 2 and the variables in Tables I and II, the lack of coordinability manifests by an inappropriate formulation of the infimal decision problem $D_{1,1}(\gamma)$, which is, in turn, based on the supremal decision $\gamma$.

In the context of the shipmaster-pilot example, $D_{1,1}(\gamma)$ corresponds to the set of maneuvers/directions for the shipmaster to execute, and it depends on the pilot’s choice of the ship’s trajectory based on expert knowledge of the local waterway. The maneuvering characteristics of the vessel, however, can be unclear to be the pilot, and the resultant set of maneuvers/directions may be infeasible for the shipmaster to execute. As reported in the Canadian study, “pilots and masters do not always share a common idea of what is required.” Additionally, miscommunication between pilot and shipmaster may result in the latter not properly evaluating the feasibility of the pilot’s directed maneuvers, thus leading to (or contributing to) the lack of coordinability.

To summarize, coordinability can provide a novel reading grid of causes of shipping accidents. Academic literature on shipping accidents tends to be epidemiologic in nature, providing descriptive statistics, but is seldom actionable. On the other hand, we proposed in this discussion that the lack of coordinability is a fundamental failure cause or contributing factor to a significant number of such accidents (namely, those involving the shipmaster-pilot interactions). This proposition can form the basis for further research, and is may yield useful results for improving safety in the shipping industry.

4. IMPLICATIONS OF CONSISTENCY FOR ACCIDENT CAUSATION AND SYSTEM SAFETY

The lack of consistency is easier to conceive of than the lack of coordinability as a fundamental failure mechanism in multilevel hierarchical systems. It presupposes that the organization or the system posits as one of its overall decision problems that of ensuring safety of operations. We analyze a specific aspect of the Piper Alpha disaster as an illustration of the lack of consistency in accident causation.

4.1 The Piper Alpha Disaster and Permit-to-Work

The Piper Alpha disaster occurred in July 1988 on board an offshore platform in the North Sea and resulted in 167 deaths and several billions of dollars in losses. The complex set of contributing factors...
Coordinability and Consistency in Accident Causation and Prevention

Factors leading to the accident have been thoroughly discussed in the literature—see, for example, the excellent analysis by Paté-Cornell. Here, we focus on the primary initiating event of this tragedy, described as follows.

4.1.1 Facts and Description

In addition to oil production, gas was also handled on the Piper Alpha platform and compressed prior to its export to shore. Heavier components were removed from the gas, collected, and then pumped back into the main oil line, via an injection pump. There were two such pumps, A and B, one as a standby redundancy for the other. Each pump was connected to a pressure safety valve (PSV). The following sequence of events is simplified for illustrative purposes and so as not to distract from the main purpose of this discussion:

Pump B was in operation, and maintenance was being performed on the safety valve of pump A. The day crew did not complete the work on the PSV, which was removed and temporarily replaced with a (loosely fitted) blind flange until maintenance resumed. Thus a safety-critical equipment for pump A was removed by the maintenance crew, which meant that this pump was unavailable for service and should not be started. The night shift crew and the offshore installation manager (OIM) were not informed of this situation, nor was an update on the status of this maintenance job requested or provided. During the night shift, pump B failed, thus creating a decision problem for the OIM: to stop production or to switch operation to pump A (other options may also have been considered). In the absence of information regarding the condition of pump A and its PSV—crucially, no permit-to-work (PTW) was either made, closed, or updated about the maintenance job on the safety valve, and no oral communication to this effect occurred between the interested parties during shift turnover - it was assumed that the back-up equipment was available for service, and the OIM decided to start pump A. The night shift crew then executed this decision and started the pump. It was a few seconds after pump A was started that the flange leaked, producing a flammable cloud that ignited/exploded and started the accident sequence.

4.1.2 Analysis

We identify a decision-making hierarchy consisting of the OIM as the supremal unit and the night shift crew as the infimal unit. We propose a novel interpretation of its cause, namely, the lack of consistency of the supremal unit’s input with the process condition.

This lack of consistency is self-evident: the supremal unit (OIM) solved his decision problem (switch to pump A), the infimal unit (night shift crew) easily executed it, and the initiating event, the first explosion, resulted. This lack of consistency was evidently the result of a mismatch between process condition or characteristics (absence of PSV ⇒ pump A unavailable), and the internal model the supremal unit had of the process (see Fig. 2). One of the PTW functions is to ensure that no asynchronous evolution occurs of the process characteristics and its models as held by the supremal and infimal units. The failure of the PTW on-board Piper Alpha enabled this asynchronous evolution, and resulted in a supremal unit decision that was inconsistent with the new condition (unbeknown to the OIM) of the process after the maintenance job.

Beyond the Piper Alpha tragedy, the PTW seems to be involved in many industrial accidents. For example, 30% of the accidents that occur in the UK chemical industry are said to be maintenance related and involving the PTW: “most [of these accidents] were due to errors in the way the equipment was prepared for maintenance or handed over. Sometimes the permit-to-work system was poor, sometimes it was not followed.” Framing the PTW as an instrument for ensuring, among other things, consistency, and clarifying during personnel training how its breakdown can result in failure mechanisms (lack of consistency) that lead to system accidents can make a more persuasive case of its importance and the need to comply with it among operators, maintenance crew, and supervisors. This is clearly an important area for further research and field investigation, as it has the potential to positively affect safety across many industries in which the PTW is deficient or broken.

As noted in the accident report, the PTW procedure was knowingly disregarded; operations representatives did not inspect the job site before suspending or closing the work indicating that the work has been completed; and supervisors often left permits on the control room desk at the end of the shift, rather than personally returning them to the responsible operations representative.
4.2 Further Examples and the Lack of Consistency in System Safety

The recent incidents of aircraft clipping each other while taxiing at New York John F. Kennedy airport\textsuperscript{11} and at Boston Logan airport\textsuperscript{12} can be conceived of in part as a problem of lack of consistency with the overall problem of ensuring safety of ground operations: the supremal unit solved its scheduling and ground movement problem, the two infimal units solved their assigned problems, and the incidents occurred. Media outlets asked, “who’s to blame?” (e.g., CBS News) and several commentators indicated that this was a “pilot error.” The pilot is indeed ultimately responsible for the safe operation of his or her aircraft.

However, an error can be conceived of as a consequence, not a cause\textsuperscript{13}, and assigning blame to culprits does not directly identify, or translate into, actions that help avoid similar accidents in the future. If, on the other hand, we identify these incidents as the result of lack of consistency in a multi-level system, we expand the range and nature of solutions we can seek to these problems. For example, we can reflect on how to include process characteristics (in this case, the aircraft) within the decision-making units, infimal and supremal (see Fig. 2), and how to check on and verify the consistency of decisions with the overall problem of ensuring safety of operations. The prevention of these incidents, when viewed as the result of a lack consistency, can encompass more than “avoid pilot error” and may include technological innovations (e.g., some form of a ground-based TCAS; or a virtual safety range bubble around each aircraft, like a berthing distance, for ATC to consider in coordinating ground operations) as well as procedural changes to support the consistency of decisions with the overall problem of ensuring safety of operations.

As noted earlier in the Piper-Alpha example, the lack of consistency may be a self-evident failure mechanism in hierarchical systems, resulting for example from a lack of compatibility between process dynamics and supremal unit decisions (we discuss shortly why this might happen). However the important point in this case is not only the recognition of this failure mechanism, but the questions that follow from recognizing it, such as: how to ensure, or test for, the consistency of supremal unit inputs and the overall decision problem of ensuring safety of operations, given the characteristics of the process? And how to recognize and flag an inconsistent supremal unit input and adjust/modify it? These questions should be quite relevant, for example, for management (supremal unit) in industries that handle hazardous processes (e.g., mining, oil and gas). Framing the problem in this manner, and asking these questions can result, for example, in (better) training of the workforce, which would be sensitive to consistency problems, and empowered to question supremal unit inputs that are inconsistent with the overall problem of ensuring safety given their knowledge of the process dynamics. More generally, filters can be designed and put in place at the management and operators levels for identifying and eliminating inconsistent supremal unit inputs.

5. SUMMARY AND CRITICAL ASSESSMENT

Multilevel systems pervade many aspects of modern life. Whether in a purely technical context or socio-technical context, multilevel systems are omnipresent. Whereas an ontological discussion of these systems is beyond the scope of this work, it is worth simply pointing out the relationship between (functional) specialization, multiplicity of decision-making units, and the emergence of hierarchical multilevel systems. Functional specialization can be thought of as related to a breakdown of an overall goal into sub-goals or objectives and organizing for their pursuit.

For our purposes, multilevel systems pose an immediate problem of coordination\textsuperscript{14}. From a system-theoretic perspective, we reviewed in §2 the theory of coordination, in particular the two concepts of coordinability and consistency. These concepts are fundamental properties of multilevel systems, whether these are purely technical systems as in the case of the autonomous robot discussed in §2.2, or sociotechnical as in the cases discussed in §3 and §4.

\textsuperscript{11}April 11, 2011. An A-380 clipped the horizontal stabilizer of a CRJ-700 and spun it violently.
\textsuperscript{12}July 7, 2011. A B-767 struck the horizontal and vertical tail of a CRJ 900ER, which sustained substantial damage.
\textsuperscript{13}Error as a result or consequence of something prior; a basic idea in psychotherapy. This observation can be stated casually as “one person’s cause, (i.e., what one person identifies as a “cause”) is another person’s consequence.” (11)

\textsuperscript{14}That specialized operations, for example, have to be coordinated to achieve certain overall objectives.
We then proposed that coordinability and consistency ought to be important concepts for accident causation and system safety. More specifically, we argued that the lack of coordinability is a fundamental failure mechanism causing or contributing to system accidents. Our discussion was narrower in scope than the concept of coordinability introduced by Mesarović et al.\textsuperscript{18} in that we described the failure mechanism as resulting from a lack of coordinability of a specific suprimal unit input. In other words, we identified the failure mechanism not as a general lack of coordinability of a multilevel system, but the selection of a particular non-coordinable input by the suprimal unit, resulting in one or more infimal units not being able to solve their particular decision problems, which in turn can precipitate a system accident (see discussion in section 1 about this class of adverse events). We then argued that the lack of consistency is also a fundamental failure mechanism in multilevel systems, albeit an easier one to conceive of than the lack of coordinability. But this simplicity brought to the forefront the important consideration of how to test for, verify, and ensure consistency across the multilevel decision units with an overall goal of ensuring safety of operations. We proposed for example that the recent incidents of aircraft clipping each other on the tarmac are instances of lack of consistency, and that framing the problem this way helps expand the scope and nature of solutions that can be sought to these problems.

We believe coordinability and consistency are important concepts for thinking about accident causation and prevention. In cognitive science, the term of “hypocognition”, recently been popularized by the linguist G. Lakoff\textsuperscript{30} refers to the lack of a concept or term for an issue, leading to one’s inability to fully understand or comprehend it (and act upon it). Coordinability and consistency may not address a state of hypocognition in the safety community, but they can help expand the intellectual toolkit of safety professional and academics. For example, the identification of lack of coordinability as a fundamental failure mechanism in multilevel systems can raise awareness of this path to system accidents in hazardous industries, and we hope, will prompt reflection about ways, technical and organizational, for ensuring this failure mechanism does not occur. A similar argument can be made about the lack of consistency.

In short, we proposed that coordinability and consistency are ingredients for accident prevention, and their absences are fundamental failure mechanisms causing or contributing to system accidents. This perspective offers several avenues for further research, and it provides an opportunity to revisit some established views on accident causation and system safety. For example, it has been advanced that “sloppy management” is the root cause of many industrial accidents.\textsuperscript{(5,1)} The concepts of coordinability and consistency may add further nuance to, or displace the narrative of, the culpability of “sloppy management”, which, like “operator error”, is a retrospective construct for assigning blame, but is of limited forward-looking value or help in contributing toward accident prevention. By reframing the problem of “sloppy management” as one for example of lack of coordinability and/or consistency (if that is the case), we avoid the litigious connotation of the former and pose the problem in a theoretically sound and value-neutral way. This in turn invites a new emphasis on shared responsibility and organizing for ensuring coordinability within sociotechnical systems for preventing accidents and sustaining safety (sloppy management implies coordination is the responsibility of the supremal unit, whereas the lack of coordinability is a result of flawed interactions between supremal and infimal units, and as such, it requires a multilevel approach to be tackled, not just a suprimal unit change). Reframing “sloppy management” as a problem of lack of coordinability and/or consistency is also more likely to entice various stakeholders to participate in accident prevention and safety efforts, including companies’ management and senior executives.

One additional venue worth exploring in future work is the possible connection between coordinability, consistency, and the High Reliability Organizations (HRO) paradigm (an extensive literature exists on the subject; see for example\textsuperscript{(31,32,33)})). HRO are a “family of organizations that operate continuously under trying conditions and have fewer than their fair share of major accidents”.\textsuperscript{(34)} Despite the difficulties and objections by some academics to defining high reliability organizations, the literature on HRO has made important contributions in identifying managerial and organizational issues that contribute to accident prevention and safety. It would be interesting to examine the extent to which some of the characteristics of HRO are aligned with or contribute to ensuring coordinability and consistency in organizations and multilevel systems. These two approaches to safety, HRO’s managerial/organizational approach, and the system-theoretic approach with its emphasis on coordinability and consistency, may
have important synergies and can be mutually helpful in further advancing the safety agenda.

ACKNOWLEDGMENT

The authors would like to thank the anonymous Reviewers, whose constructive comments and criticisms significantly contributed to the improvement of this paper.

REFERENCES


R. V. Cowlagi and J. H. Saleh


APPENDIX

The hierarchical structure for the motion planning and control problem is not strictly speaking necessary, but it has been to date the preferred practical method for dealing with the complexity of the problem. To better understand this complexity and the need of a hierarchical solution, consider the fact that motion planning involves two distinct sub-problems: (1) the satisfaction of specified high-level vehicle tasks, and (2) the design of vehicle control laws. Vehicle tasks are typically specified using formulae of predicate or temporal logic in discrete states, and finding the set of states satisfying these formulae involves tools from the discrete mathematical disciplines of combinatorics and formal...
methods. On the other hand, vehicle dynamics are typically modeled using differential equations in continuous states, and the design of vehicle control laws for governing the solutions of these differential equations involves tools from dynamical systems and control theory. This inherent dichotomy is further deepened by a traditional disconnect between the academic communities involved in these two areas. Consequently, the combinatorial techniques used in the higher level geometric path planner usually assume (for practical purposes and to be able to solve their problems within acceptable timeframes) the sake of practicable implementation) simple models of the vehicle’s motion, and thus ignore the vehicle’s kinematic and dynamic constraints. Conversely, the control theoretic techniques used in the lower level planner usually assume as given a reference (to track or “execute”), the generation of feasible reference signals to satisfy high-level tasks is not addressed.