Managing Uncertainty in Life-Critical Systems

Guy André Boy

"The only thing that induction accomplishes is to determine the value of a quantity.
It sets out with a theory and it measures the degree of concordance of that theory
with fact. It never can originate any idea whatever. No more can deduction.
All the ideas of science come to it by the way of Abduction.
Abduction consists in studying facts and devising a theory to explain them."
(Peirce, 1965)[1]

Abstract. Uncertainty happens when people do not have enough information about a situation that compels them to act. The less correct information they have, the more their judgment will be based on beliefs and levels of trust. Conversely, the more they have correct information and knowledge, the more they will be certain of acting correctly. Uncertainty, ignorance, possibility, chance, and necessity are intimately related. Uncertainty is also related to situation awareness, which can be modeled as perception, comprehension, and projection. This is the reason people try to develop methods and tools to improve perception through various kinds of visualization techniques, comprehension through various kinds of reasoning techniques and tools (in the artificial intelligence sense), and projection through various kinds of abduction mechanisms (i.e., anticipate what will or could happen next). An accurate prediction can only refer, from a short-term perspective, to what happened before a situation is perceived (i.e., an event-driven or reactive causal approach). Conversely, longer-term anticipation allows for guessing and testing possible futures (i.e., a goal-driven or intentional approach). Claiming that uncertainty in systems engineering and complex operations is a matter of situation awareness, the proposed approach is based on a situational systemic framework, where complexity and flexibility are central factors to be considered to manage uncertainty in life-critical systems.

Keywords: abduction, flexibility, human-in-the-loop simulation, life-critical systems, problem-solving, risk, situation awareness, trust, uncertainty, unexpected situations.

1 Introduction

Per Grote's definition, "uncertainty is a state of lacking or ambiguous information about a task to be accomplished" (Grote, 2018, p. 2). In this chapter, uncertainty management in work organizations is considered information processing in the sense of situation awareness, decision making as abduction, and action taking. Uncertainty management is required when people do not have enough information about a situation where they need to act.

Uncertainty management in life-critical systems, such as aviation and nuclear energy, is necessarily related to the concept of risk (Nilsen & Aven, 2003). Risk is associated with danger and, more generally, the probable disadvantage to which one is exposed. Danger can be of different natures: medical, social, environmental, economic, etc. Risk is the likelihood of a specific effect within a specified context and is commonly viewed as a complex function of probability, consequences, and vulnerability.

Amalberti and his colleagues stated that the most important difference among industries lies "in an industry's willingness to abandon historical and cultural precedents and beliefs that are linked to performance and autonomy, in a constant drive toward a culture of safety"

[1] Peirce, C.S. (1965). Collected Papers. Cambridge, MA: Belknap. 5, p. 145.

(Amalberti et al., 2005, p. 756). They also proposed a categorization of life-critical activities and industries going from very unsafe to ultra-safe, in terms of probability of death per hour, going from Himalaya mountaineering (probability of death is around 10^{-2} per hour of effective practice), to microlight aircraft and helicopters (10^{-3}), to road safety (10^{-4}), to chartered flights (10^{-5}), to the commercial aviation and nuclear industry (10^{-6}). Commercial aviation, for example, qualifies as an ultra-safe sector where stakeholders (e.g., pilots, controllers, passengers, ultra-safe technology and organization) evolve within a safety culture.

In life-critical environments, such information processing is about risk-taking. Indeed, any time we decide in an uncertain situation, we also take a risk by transforming this decision into an action. Note that doing nothing can be a specific life-critical action. Therefore, we will consider that uncertainty is associated with *risk-taking*, which should result from anticipated well-prepared missions and processes (Boy & Brachet, 2010). Risk-taking provides a vivid meaning to uncertainty management. Risk takers detect all possible recovery situations to be safe when everything goes wrong. They also need to be aware of limitations for themselves and the whole system around them, which must be compatible with the risks they take. Investment is key in terms of preparation and risk assessment. This is why people involved in life-critical situations need to learn about risk-taking.

In addition, risk-taking is also associated with responsibility (of the risk taker) and trust (that includes self-confidence and the degree of trust in the environment). Risk-taking can be modeled as an abduction process. Consequently, in life-critical dynamic environments, people cannot avoid or eliminate all potential drifts (Dain, 2002; Perrow, 1999). Most drifts are usually qualified as normal, where actors manage to anticipate and adapt to them. Lazarus and Folkman qualified these adjustments as coping (Lazarus & Folkman, 1984). People cope with the uncertainty of extreme situations to reach their mission goals, survive, and/or protect other people in their environment. This adaptation has been described as a "cognitive compromise" between the resources required to manage the situation and the performance required to reach a mission goal (Amalberti, 2001; Amalberti & Deblon, 1992; Hollnagel et al., 2006).

In the aerospace domain, experience shows that pilots' actions are almost all life-critical by nature, and pilots have to take risks in unexpected situations. Similarly, are we taking risks whenever we act under uncertainty in our everyday lives? For example, are currently available systems, such as smartphones, life-critical? Imagine that you lose your smartphone—you will immediately realize that it is life-critical in many ways, including the security of the data you stored on it and the fact that you will be disconnected from the current modern world for a while. Life-critical uncertainty management deserves deeper thinking and leads to the following questions, which frame the content of this chapter: What is the contribution of risk-taking and trust? How can we evaluate risk to improve uncertainty management? Shouldn't we take risks to learn uncertainty management? How should we deal with the unexpected? How can trust influence uncertainty management and risk-taking?

This chapter constitutes an attempt to answer these questions by better grasping what **situational uncertainty management** means based on a human systems integration background. There are situations where risk may take important and, in some cases, crucial proportions, leading to very difficult problem-solving and, ultimately, crisis management. A crisis is typically defined by its progressive emergence, breakdown, specific management of its evolution, and return to normal. During the emergence phase, only preventive actions are relevant when the context is favorable. Ignorance, uncertainty, and lack of data often limit preventive actions. In the breakdown phase, the most serious problems of decision-making and action arise. The evolution phase is about recovering an acceptable way of life and returning to "normal," which should translate into communication actions and experience feedback to capitalize on the achievements for the future. Besides, can we not ask ourselves if life itself is not permanent crisis management? Can we categorize risk situations and systems? A few

contemporary cases will be used to illustrate how uncertainty could be managed by taking reasonable risks.

2 A situational framework for uncertainty management

The term "situation" is commonly used to denote something that happens, such as an event, a person's state of affairs, a location, a process at a particular time, or even a context that specifies a set of persistent conditions in time and space. A situation can be a generic pattern or an episodic set of conditions. In summary, according to the common sense of control theory, we will consider that a set of states defines a situation. More formally, a situation S may refer to a dynamic set of states (i.e., a situation varies in time), $S(t) = \{s_i(t); i = 1,n\}$, including multiple derivatives, in the mathematical sense, such as velocity and acceleration (i.e., a situation is not only a static description but also an evolution).

Let us clarify the concept of situation in more detail within the scope of uncertainty management. A situation can be viewed in many ways (Figure 1). Ideally, the real world is characterized by infinite, highly interconnected states. This is what we call the "real situation." Some states of the real situation are not available to us, either because there is no mechanism to make them accessible or because we do not know them. For example, many states describing market evolution are not directly available to finance traders.

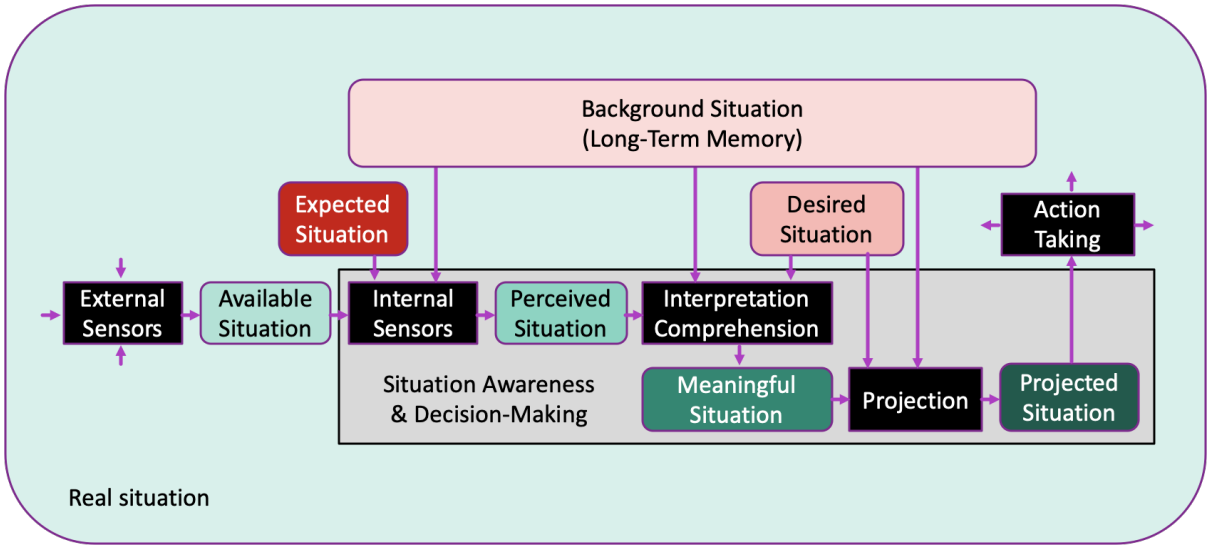

Figure 1. Various interconnected human-centered meanings of the situation concept.

States available to a human observer through external sensors (e.g., physically measured variables, human-provided key performance indicators) define the "available situation" (e.g., market evolution states available to traders). The available situation is typically a subset of the "real situation." In addition, the available situation may not be perceived by the observer. For example, visualization techniques can improve how people perceive it in human-computer interaction. The "perceived situation" depends on the availability and quality of internal sensors (e.g., eyes, audition, gesture sensors). Note that internal sensors are influenced by the "expected situation" and the background situation. Therefore, part of the perceived situation is a subset of states of the available situation, directed, augmented, and/or transformed by what is being expected (i.e., the expected situation) and the long-term memory of the agent (i.e., the "background situation"). The expected situation supports event-driven behavior (i.e., what we anticipate may happen).

Following what Endsley already described in her situation awareness model, the perceived situation must also be understood at a conscious level. We can talk about an interpretation process at this point. Therefore, another type of situation is constructed, that is, the "meaningful situation," a subset of the perceived situation augmented by the "desired situation" (i.e., what we want to do) and the background situation (i.e., directed by experience and habits). The desired situation typically expresses goal-driven behavior (e.g., what we want to get from what we are doing in the current situation). Understanding what is going on is useful for action, which requires another set of conditions, which Endsley calls a projection. The "projected situation" can then be considered a subset of the meaningful situation augmented by the background situation (e.g., experience and habits).

When people expect something to happen with high confidence, they may be confused and mix the perceived situation with the expected situation (i.e., this is usually related to cultural context, distraction, and focus of attention—people see what they want to see!). There is a huge difference between monitoring activities and controlling activities. People involved in a control activity are usually goal-driven. Their situation awareness process is directed by the task they need to perform (i.e., their role in the context of where they are). Conversely, people who only have to monitor a process and do not have to act on it need to use and sometimes construct an artificial monitoring process in real time that may be difficult, boring, and sometimes meaningless to handle. In this second case, the situation awareness process has many chances not to be accomplished correctly. Consequently, uncertainty management in very life-critical complex industrial environments, such as aerospace, should be handled with educated tradeoffs between goal-driven and event-driven approaches (i.e., people involved should be fully involved in the process and not in a remote monitoring role).

Finally, the meaningful situation is not necessarily a vector of some available states but a model, scenario, or polysemic image that emerges from a specific combination of these states, incrementally modified over time (i.e., human operators build their mental models or mental images of the real situation). This mental image depends on people, cultural context, current activities, and other factors specific to the domain under study. The influence of cognitive context on physical context should be considered seriously because what people comprehend is not the real situation but something perceived from the available situation, their own expected and desired situations, and their background knowledge and skills.

In sum, uncertainty may be in all these various kinds of situations. Therefore, locating where uncertainty is and how it can be formalized is crucial. Uncertainty management, seen along the lines of situation awareness, decision-making, and action-taking, leads to the problem of risk-taking. The next section describes risk-taking as chance (i.e., events we have to react to and the related problem) and necessity (i.e., required actions to solve a problem).

3 Chance and necessity: Dealing with the unexpected

Chance and necessity are not new complementary concepts; the Greek philosopher Democritus claimed they were the source of everything in the universe. According to Barnes, Democritus's "chance" term should be understood as "absence of purpose" rather than a denial of necessity (Barnes, 1982). Nobel Prize winner Jacques Monod, a pioneer in molecular biology and modern genetics, was interested in the origin of life and the evolution of species; he proposed a new humanism integrating related scientific data. He claimed that human beings emerged in the universe by chance and necessity (Monod, 1970).

Talking about a critical situation or a crisis is also the first time! The moment when we had to invent something that we had not prepared in advance. Understanding a risk is modeling, formalizing, and learning the acts required to control it. At first, a model should be developed, and little by little, it should be refined in terms of its pairing with the real world. Such modeling

can be done individually or collectively, depending on the topics and problems. Experience feedback should also support this modeling approach and be incrementally integrated into our knowledge on life-critical actions.

Unexpected situations on a few examples

Dealing with unexpected events is one of the most crucial contemporary issues in aviation safety (Pinet & Bück, 2013), and it involves chance (i.e., unexpected events) and necessity (i.e., maintaining safety onboard). Pilots are unique resources to handle such events and situations. For example, the Qantas A380 recovery around Singapore after an engine explosion on November 4, 2010, turned out to be a successful accident. Other successful accidents can be cited, such as the US Airways A320 landing on the Hudson River after losing both engines on January 15, 2009; the DHL A300 landing in Bagdad after being shot by a missile on November 22, 2003; and the aborted Apollo 13 mission after an oxygen tank exploded on April 13, 1970. Such successful accidents will be developed later in the chapter. They show that people can handle very complex and life-critical situations successfully when they have enough time and are equipped with the right functions, be they in the form of training and experience or appropriate technology or organizational setups; these functions should be handled in concert.

Take an example of an unexpected event in commercial aviation (Boy, 2013a). Shortly after takeoff from the Baghdad airport, terrorists shot a DHL A300 cargo plane. A surface-to-air missile struck the left-wing tip, causing the loss of hydraulic flight control systems; the aircraft was uncontrollable from a classical perspective. No procedure was available for such a configuration of the aircraft. Pilots managed to land safely without injuries, using differential engine thrust as the only pilot input. They had to use their educated experience (i.e., using nonlinear flight dynamics and mechanics basic principles), and they did so successfully. In this case, uncertainty was managed using deeper expertise and skills.

Another example is US Airways Flight 1549, which suffered a double bird strike after takeoff from LaGuardia Airport (National Transportation Safety Board, 2010). No engine was available. Consequently, the aircrew had to fly the aircraft as a glider. This was very challenging, especially in a populated area such as New York. The captain had to make a decision that was not in the handbook! He was faced with a tremendous problem. Once he decided, he managed the situation until he successfully landed the Airbus A320 on the Hudson River (i.e., using goal-driven behavior in a highly constrained environment). Again, all crewmembers did their jobs, but outside usual procedural constraints. The captain's expertise and skills were the best available resources.

One more example is Qantas A380 Flight 32, where an engine exploded over Batam Island, Indonesia. The explosion damaged the fuel system, causing leaks; disabled one hydraulic system and the antilock brakes, causing engines 1 and 4 to go into a "degraded" mode; and damaged landing flaps and the controls for the outer left engine 1. It took 50 minutes to complete the initial assessment of damages due to the interconnectivity and nonlinearity of numerous operational procedures. The plane returned to Singapore and landed safely with four tires blown. The situation was managed with all crewmembers doing their jobs without panicking and behaving as they would have in a simulator (Pinet & Bück, 2013). Note that aeronautics is an industrial sector where simulation is routinely used for recurrent training. This practice can potentially reduce uncertainty in many typical flight conditions because pilots learn how to solve problems in extreme situations.

How can we be more prepared for these kinds of situations?

Unexpected situations may, however, be foreseeable. The uncertainty factor lies in circumstances and the moment of their occurrence. This is why, in engineering design and systems engineering, if we do not want to discover such situations during operations, it is

crucial to use human-in-the-loop simulation (HITLS) during the design and development of systems. No matter how well structures and functions are designed and developed if they are only based on tasks (i.e., what is prescribed), the HITLS will contribute to handling emergent behaviors and properties when activity happens (i.e., what is effectively done at operations time). Human-machine systems should then be considered as living entities, which are incrementally defined through chance and necessity—that is, beyond functions and structures that are deliberately defined, emergent functions and structures should be discovered by experience and incrementally integrated. In other words, emergent functions and structures should be assimilated and accommodated in Piaget's sense (Piaget, 1952, 1954, 1971).

This notion of emergence comes from philosophy, complexity science, system science, and the arts (Goldstein, 1999; Lichtenstein, 2016; Norman et al., 2018). The properties of a system qualify it for being emergent when they are different from the properties of its parts. How does this relate to uncertainty management? Whenever we need to decide in an uncertain world, we need to project ourselves into the future and anticipate what would happen if we took the currently foreseen appropriate action. In other words, we either implicitly simulate possible futures in our head or implement a prototype and test it using a HITLS approach, enabling us to observe the system at work (i.e., observe activity). A better sense of activity generated in possible futures is a great way to manage uncertainty.

Managing the unexpected is what retains people over systems. The necessary operational glue maintains the overall stability and integrity of human-machine systems. People need to understand what is going on, make their judgments, and act appropriately. Creativity is key. These abilities do not come without extensive training over a long period of time. Unfortunately, creativity and procedure following are contradictory concepts. This is why we need to focus more on creativity to handle our everyday unexpected situations instead of continuing to believe only that regulations, standards, and procedures will support safety with a fallacious expectation of zero risk.

This chance-and-necessity philosophical claim requires we consider a tangible systemic ontology (i.e., a systemic approach and framework) that will support the appropriate description of situation awareness, decision-making, and action-taking. Indeed, uncertainty management requires us to understand the systemic framework that can support it correctly.

4 From linearized short-term models to complexity management

Twentieth-century engineers were educated and trained to simplify complex problems to match the requirements of affordable engineering techniques. They were taught to focus on problem-solving methods rather than the art of stating dirty, complex problems. Simplification is often a matter of developing a quasi-linear model that can be handled effectively using well-known engineering methods. In other words, we learned how to state problems to fit problem-solving methods. In some cases, we had to invent new methods, of course, but we rapidly came back to things that were, and still are, manageable, especially financially and in the short term. Unsurprisingly, we often come up with situations that are difficult to manage today because their tremendous complexity (i.e., COVID-19) increases the difficulty of uncertainty management.

Life-critical situations force complexity management. Complexity mostly results from the large number of factors involved. For example, a typical aviation situation results from a dynamic and nonlinear combination of the psychological and physiological states of the aircrew, the way the given airline manages operations, aircraft state, air traffic control state, weather, ground infrastructure, commercial situation, airspace state (in terms of density and capacity), current regulations, political situation, and so on. The number of these factors and their states can vary unexpectedly. Their possible combinations are quite large, if not infinite.

This inevitably creates complexity. Pilots always have the expected aviation situation patterns in mind, built from experience, and what happens in practice is not always what they anticipate. However, the variation between the expected situation and the available situation is most of the time modest and handled very smoothly. In some cases, such variation can be much bigger. Apollo 13's successful accident is an excellent example of a very well-orchestrated complex operation, where the flight director managed uncertainty by developing a solution on the ground and sent an engineered procedure developed in real-time to the astronauts on board, who successfully implemented it and returned safely to Earth.

Small variations have been considered for a long time as noise, and engineering practice tends to filter them. However, the **variability** of complex nonlinear systems does not always fit the mold, and deviations from the expected can be much bigger. Regular automation no longer works and leaves end-users responsible for handling such nonlinearities. This happened during the COVID-19 problem-solving experience when medical doctors had acute workload stress. Preparation means seeking appropriate medication and having enough resources for hospitals and medical personnel. We see here that uncertainty management, in the sense of risk management, is about stability, sustainability, and flexibility. Stability deals with redundancy and resilience (Boy, 2016). Sustainability deals with the continuity of "normal" life and business and lasting quality. Flexibility deals with the ease of solving problems when uncertain (e.g., off-nominal situations).

The extreme cases already presented are the tip of the iceberg of nonlinear system dynamics variations where *problem-solving* necessarily replaces procedure following. It is, therefore, useful to better understand complexity theories, such as catastrophe theory, bifurcation theory, and chaos theory, instead of conventional reductionism. In catastrophe theory, for example, we observe patterns that are inevitable catastrophes (Thom, 1989). In bifurcation theory, we observe that for a small change in a "bifurcation" parameter value of a system, a sudden "qualitative" or topological change (Poincaré, 1885) occurs in its behavior (e.g., a small change in temperature and pressure may suddenly change steam into ice). In chaos theory (Thuan, 1998), we observe small variations potentially leading to uncontrollable behavior of the overall system and persistent patterns, called attractors, that can be identified and managed. This nonlinearity needs to be understood and appropriated in various contexts by human operators who deal with life-critical systems. In particular, these human operators need to understand that some parameters directly influence the qualitative nature of the system behavior.

How can we train people to manage these variations between the expected and actual situations? The best answer to this question is to look for stability. *Stability* can be passive or active. Passive stability does not require any specific action to be applied to the system to return to a stable state, such as the pendulum. Active stability, conversely, requires a proactive attitude to maintain the system in a steady state, such as the inverted pendulum. In sociotechnical systems, we can experience both kinds of stability. Experience provides cases that can be categorized and further associated with appropriate behaviors related to passive or active stability. In cases where passive stability prevails, we must let go instead of counter-interacting with the system, especially when automation does the job for us. When active stability is at stake, proactive behavior is required.

5 From rigid automation to flexible autonomy

Taking into account Amalberti's categorization of life-critical systems (Amalberti et al., 2005), the main difference between very unsafe and ultrasafe systems is not only their rates of catastrophic accident exposure in terms of the number of deaths per exposure (e.g., 10^{-2}/hour for extreme mountaineering or cardiac surgery, and 10^{-6}/hour for commercial aviation) but also the level of subject matter expert involvement (e.g., expert mountaineers are extremely trained

and know how to solve problems efficiently in extreme situations, whereas commercial pilots are trained to follow procedures with little chance of solving problems in extreme situations). Experience feedback practice is well developed in ultrasafe systems, such as commercial aviation and nuclear energy. Both procedure following and automation are also highly developed in ultrasafe systems, whereas control remains "manual" in unsafe systems, such as mountaineering or surgery. Ultrasafe systems may fail and, in this case, bring people back to manual control, moving from rigid automation monitoring and procedure following to problem-solving that requires flexible autonomy (Figure 2).

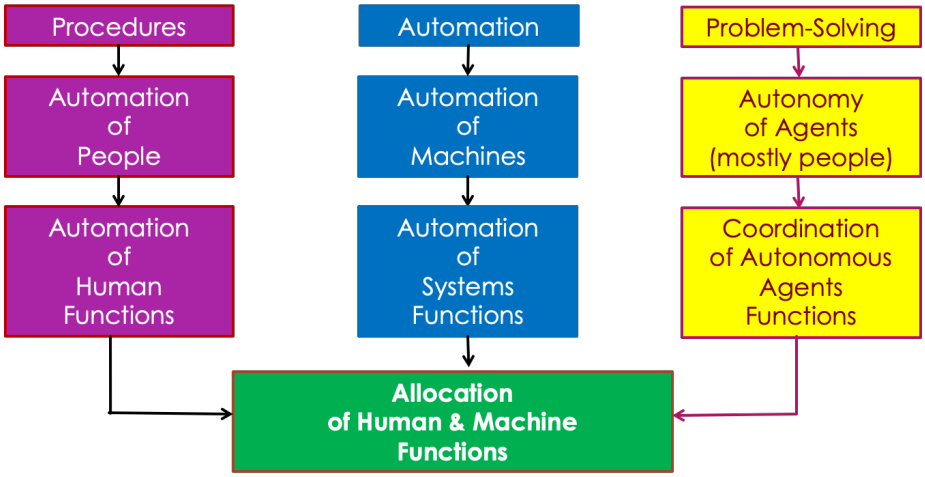

Figure 2. From rigid automation to flexible autonomy.

Uncertainty management in aviation has been handled through the incremental implementation of software layers based on experience, to the point that current aircraft are highly automated, providing a robust level of safety within a close-knit, familiar environment. If we have accumulated a lot of knowledge since the beginning of aviation, we do not know everything! Therefore, outside this close environment, automation rapidly induces rigidity, and pilots are the ultimate resources to solve unexpected problems onboard. In such situations, they must deal with the unexpected exceptionally, using their airmanship, not with operations procedures or automation, which provide rigidity (Pinet, 2015). If it is recognized that they require more autonomy and flexibility, they also should have appropriate tools, which are not necessarily available. In contrast, mountaineers must deal with the unexpected all the time. They are also extremely flexible in solving mountaineering problems. This distinction between rigid automation and flexible autonomy is illustrated in Figure 2, where autonomy involves multiagent problem solving (i.e., cooperation among human and machine agents) and, therefore, coordination among these agents.

It becomes clear that procedure following, automation, and problem-solving are three main functions useful in managing life-critical systems. If we have done much to support the first two, many efforts must be made to support the third one. A question is: What are the situations where people must solve problems that have not already been compiled into appropriate procedures and automata? We often discuss unexpected situations (Boy, 2013a; Pinet, 2019). In such situations, people in charge should have autonomous capabilities. Autonomous agents, be they humans or machines, need to be appropriately coordinated. Altogether, designing for systemic flexibility requires human and machine function allocation.

What does it take to manage uncertainty in life-critical situations successfully? Mountain guides are a good example of risk-takers. They must face the reality of danger in extreme cold, falling stones, ice, avalanches, and the possibility of losing their bearings or suffering from

physical disorders caused by high altitude. Any error, however insignificant, can be fatal. Mountaineering goes back several centuries but acquired a higher profile at the beginning of the 19th century. It is a human paradox to seek certitude, safety, adventure, and risk. The notion of a "guide" is particularly interesting because guides must show the way: They are escorts, monitors, instructors, and service providers. As in all high-risk fields, mountain guides must take account of the human factor, combine information and rules, use flexible thinking, and be steeped in a culture of error. They endeavor to adapt scientific knowledge to field practice, optimize their know-how, cultivate an awareness of risk rather than a safety reflex, and train in guessing, judging, and anticipating. Three principles apply: (a) avoid needless risk, (b) limit the consequences of exposure to danger, and (c) optimize risk management with motivation and unknown factors and stakes. In the end, guides manage the unknown using both caution and daring: They use abduction.

Abduction is one of the three forms of logical inference, along with deduction and induction. It assumes that a consequence B will be verified and that we are starting at premise A; the logical inference (A → B) will be useful to prove B. The mental process of abduction and choosing the right hypothesis is intimately linked to intuition, expertise, and competence. Charles Peirce defined abduction as a process of constructing an explanatory hypothesis and argued that it is the only logical operation that introduces a new idea (Burks, 1958). For example, the designers of the Airbus fly-by-wire aircraft implemented an abduction process (i.e., they projected themselves into the future and attempted to demonstrate the validity of their hypotheses). The plan was to design computer-driven digital aircraft, also called fly-by-wire aircraft, which consisted of developing software-based systems that would automatically control surfaces on the wing and tail. Pilots would manage these embedded systems. The shift was from doing to thinking in terms of cognitive processes. Airbus then had to demonstrate that this solution was safe, efficient, and usable. This is a good example of how such a goal-driven abductive engineering approach caused a sociocognitive disruption. We went from control of mechanical aircraft devices to digital systems management. Uncertainty management at that time was mainly an unanticipated sociocognitive model that we needed to understand and incorporate into aviation training and culture.

5 Mastering system knowledge, design flexibility, and resource management

Industrial engineering typically consists of designing, developing, and manufacturing complex systems (e.g., aircraft, power plants) by using skills of subject matter expert teams that not only project themselves into the future but also can demonstrate that the structural and functional choices will lead to the best performance of the projected system. Such an abduction process involves both global and specific objectives. The following deduction processes involve analytical and experimental validation of these objectives. However, it will only be during physical tests (e.g., flight tests for aircraft) that the team, including experimental testers, will verify hypotheses and prove them. Successive modifications are incrementally made to end up with satisfactory solutions. Delivered products are also typically further refined during operations. Knowledge and expertise are essential assets. This is why three parameters should be considered to manage design uncertainty: system knowledge, design flexibility, and resource management. How can we optimize these three parameters to reduce uncertainty? An answer to this question can be provided by using current modeling and simulation digital technology.

Figure 3 shows the theoretical evolution of these three parameters during the whole life cycle of a system when a technology-centered approach is used (typically what we have done up to now). We can see that system knowledge increases slowly in the beginning and grows faster toward the end of the cycle. Design flexibility drops rapidly, leaving few alternatives for

changes because resource commitments were too drastic too early during design and development processes. The main goals are to increase the following three concepts sufficiently early: system knowledge, that is, knowing about systems at design, development, operations, and closeout times and how the overall system works and behaves, including people and machines; design flexibility, that is, keeping enough flexibility for systems changes later in development and during usage; and resource commitments, that is, keeping enough "money" for choosing adapted resources management during the whole life cycle of the overall system. Today, instead of accumulating software-based systems in bigger systems such as aircraft, it is time to consider a systemic approach that rationalizes how systems are designed and built using modeling and simulation as a major support.

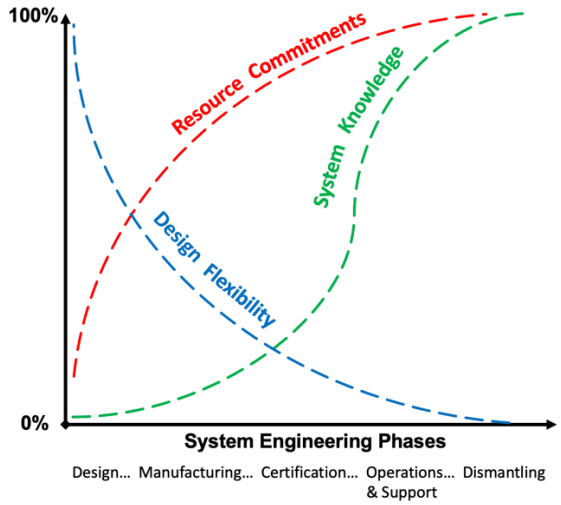

Figure 3. Technology-centered engineering: Late in life cycle[2].

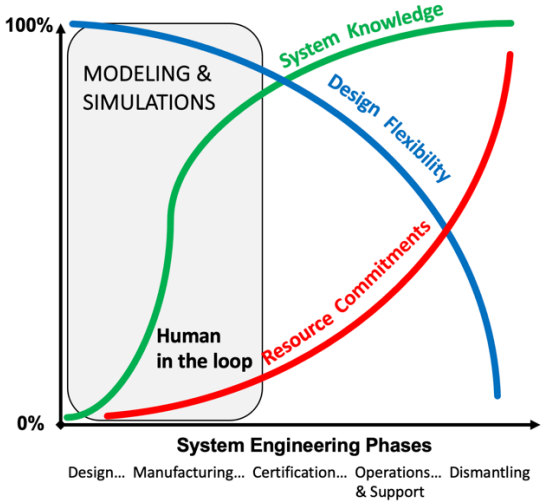

Figure 4. Human-centered design: What we really want!

In contrast, Figure 4 shows the evolution of these three parameters in a very different way. Instead of developing technology first, software models are used for the development and use of HITLS, which enables end-users' activity observation and analysis and, therefore, discovery of emergent properties and functions that can, in turn, be considered incrementally in design much earlier than before. This is a typical human-centered design (HCD) process. Consequently, system knowledge increases more rapidly in such agile design and development. At the same time, design flexibility decreases slowly, with an inverted concavity, enabling possible changes later during the life cycle. Software-based modeling and HITLS enable testing various configurations and scenarios, enabling softer resource commitments initially and leaving more space for appropriate changes.

Indeed, since the beginning of the twenty-first century, most projects have started on computers. First, ideas are generated using a PowerPoint slide deck; then, a computing model and visualizations are generated; and finally, a simulation is developed and used with end-users in the loop. For example, the Falcon 7X, developed by Dassault Aviation, was entirely built as a giant interconnected piece of software that led to a sophisticated computer game flown by test pilots. Instead of a classical task analysis for generating systems requirements, they produced requirements from an activity analysis. As a reminder, tasks are prescribed to be done, and activity is what is effectively done.

[2] Thanks to Mike Conroy for the work he supported when the author was at NASA Kennedy Space Center, as well as his involvement into INCOSE HSI Working Group.

6 Opening a discussion on uncertainty management approaches

At this point, let us open a discussion that could lead to a synthesis of what has been presented earlier by associating Amalberti's life-critical system categories, the situational model for uncertainty management (Figure 1); dealing with the unexpected, complexity management, and flexible autonomy (Figure 2); and system knowledge, design flexibility, and resource management (Figures 3 and 4). This synthesis will be made in terms of the management of trust in domain models for uncertainty management.

Various kinds of models and strategies

In life-critical systems, uncertainty management requires defining models of the system we want to study, design, evaluate, and/or operate. These models can be analogs (e.g., an electricity analog of a river flow) or ontology-based (i.e., we define the syntax and semantics of the system to elaborate its structural and functional components). The former will enable prediction; the latter will enable explanation. If we draw the evolution of a system in time, uncertainty in the future (i.e., that is essentially unknown) can be modeled by constant readjustments to reach the goal. Imagine drawing a straight line from point A to point B on a blank sheet. You may want to adopt two strategies: an event-driven and a goal-driven one. If we adopt the event-driven strategy, you must constantly monitor and control your pencil in the short term (i.e., point by point). The result is very likely to be a noisy line. Conversely, if you look at the goal (i.e., point B) constantly, you will adopt a goal-driven strategy**,** and without looking at your pencil, the result will likely be a straight line.

More generally, in adopting an event-driven strategy, actors have to make a new decision almost at each critical point in time and act accordingly. This induces constant short-term readjustments. In contrast, in adopting a goal-driven strategy, actors have a global goal and optimize their intermediary subgoals, which are most of the time defined in advance (i.e., these subgoals are defined from a backward chaining process, or retro-planning, from the ultimate goal that is the possible future). Anticipation of possible futures is risky and typically relies on abductive reasoning (i.e., we set a goal and manage to develop resources to reach it). In this latter case, uncertainty management will be based on subgoals necessary to reach the goal. The level of risk to reach each goal depends on our situational and organizational models. This is why risk-takers (i.e., decision-makers and actual actors) develop and use the right heuristics at the right time to abduct the right outcomes.

In their prospect theory, Tversky and Kahneman demonstrated that context, expressed in gains or losses, matters in people's attitudes toward risks (Tversky & Kahneman, 1992). They talked about risk aversion and risk seeking. In the former case, for example, people would choose a gain of $1,000 if it is certain (e.g., 100% chance), compared to gaining $2,500 if it is uncertain (e.g., 50% chance). In the latter case, for example, if the same people are confronted with a loss of $1,000 versus a 50% chance of no loss or a $2,500 loss, they often choose the risky alternative.

In addition, risk-takers do not act the same when facing life-critical situations. Llewellyn showed three types of mountain climber orientations related to risk-taking: **risk avoiders, risk reducers,** and **risk optimizers** (Llewellyn, 2003, p. 27). These categories are related to self-confidence. Risk optimizer behavior is consistent with Tversky and Kahneman's empirical results. Much is to be learned regarding Llewellyn's risk-taker categories, specifically obtaining more evidence on the relationships between these categories and other categories, such as novice, occasional, and expert risk-takers.

Risk takers need to manage uncertainty using appropriate representations and models to handle situations, in the sense of the various interconnected human-centered meanings of the situation concept presented in Figure 1, and available resources. Resources can be cognitive

and/or physical. They can also be internal or external to each agent. Internal resources lead to self-confidence (i.e., trust in personal knowledge and experience). External resources lead to trust in another agent, whether human or machine. Uncertainty models that we typically use are based on probability theory. We talk about the probability of an event occurring. Such a mathematical model can also be used to handle trust in resources. Note that these mathematical models have their limitations. Let us turn to an example.

Safety engineering handles uncertainty by modeling risk (R) as the mathematical product of the probability (P_E) of the occurrence of an event by the seriousness of consequences of this event (S_C): $R = P_E$ x S_C. However, when P_E is very small (e.g., the probability of occurrence of an earthquake followed by a tsunami of the magnitude of Fukushima's disaster was very small and known as 6 in 3 millennia and is S_C very big (e.g., a dramatic nuclear disaster in Fukushima in 2011), the product of a very small number (close to zero) and a very big number (close to infinity) is undetermined in mathematics (i.e., zero multiplied by infinity is undetermined). Therefore, probability theory does not work in this case. It would be better to take the possibility theory (Dubois & Prade, 2001), which considers two numbers, the possibility and necessity of an event to occur, instead of one probability. In the Fukushima case, an event like the one in 2011 was possible (i.e., $Pos_E = 1$; $Nec_E = 0$). The gap between possibility and necessity is the ignorance we have on the occurrence of the event (i.e., $I_E = 1$). Using possibility theory instead of probability theory in such an exceptional situation would have given the conclusion that the event's seriousness of consequences is the only parameter that counts. We can see here that uncertainty management can be very different when choosing a risk-taking theory.

Such uncertainty models should be developed for available, expected, perceived, desired, meaningful, and projected situations (Figure 1). We see that unexpected situations should be identified with ignorance and, simultaneously, degrees of possibility and necessity. Expected, desired, and background situations have degrees of ignorance, possibility, and necessity, impacting respective degrees for perceived, meaningful, and projected situations. Unexpected situations can be known or unknown. When known, they cause additional stress but can be handled using a rule-based behavior, in Rasmussen's sense (Rasmussen, 1986). However, when they are unknown, they require creative problem-solving using available resources, which can be handled using knowledge-based behavior, in Rasmussen's sense.

Associating uncertainty and trust

According to French et al. (2018), interest in trust most often appears in situations of uncertainty and vulnerability. Trust is necessary when an element of risk arises from the possibility that the trustee will fail to complete the task (Harding, 2006). Note that today, such trustees can be humans or machines. Therefore, trust maintenance is directly related to uncertainty management and risk-taking. Trust is a very rich topic that has been explored for a long time in many fields, such as psychology, sociology, human factors, philosophy, economics, and political science. In a multiagent environment, trust is intimately related to cooperation and collaboration. Consequently, the focus is systemic and organizational (Castelfranchi & Falcone, 2000; Mayer et al., 1995). Trust may vary concerning the evolution of context. For example, we may trust a human or a machine based on reputation and suddenly realize that this agent does not fit what we expected; consequently, we may no longer trust this agent or system.

Working on trust in human-machine systems, where machines are increasingly autonomous, Atkinson (2012) insisted on the fact that autonomous agents are not tools but partners that have the following properties: appropriate reliance and interdependency; delegation of authority; initiative (taking and relinquishing); social interaction and personalization; agent self-motivated behavior; and ethical behavior by and with agents. Atkinson (2012, p. 4) claimed, "our trust in automation today is based on confidence built over

many years in developing highly reliable, very complex systems." Examples of complex systems are spacecraft, airplanes, planet-wide information systems, and so on. This categorization is based on the fact that we have many tools and techniques to verify, validate, test, and evaluate complex systems. These tools are not perfect, but usually they are good enough. Consequently, we increasingly rely on complex, automated systems, but only in proportion to our trust in them (optimal utility requires "appropriate" reliance). This all means that trust in complex systems relies on *familiarity*. How long does it take to become familiar with an autonomous system? Learning is a matter of working together enough to ensure that teamwork reflects the identity of the other partner. This is a matter of maturity of practice, which translates into solid intersubjectivity.

Trust is thus about competence, predictability, and transparency; reputation (stable signals and behaviors); and reliability (enabling anticipation, guidance, and teamwork). Trust has to do with stable interaction among agents, minimal conflicts among agents, and predictability of interactions. This is what it takes to manage uncertainty in the design and operations of complex systems. Let us take flight operations as an example. Uncertainty can be reduced and better managed when information feedback is correctly provided. For example, when the pilot enters the value of a parameter into the machine on the flight-deck user interface, the machine should immediately inform the pilot that the entered information has been well received and considered for treatment; similarly, when the pilot requests the copilot to do something, the copilot should acknowledge the request and inform the pilot when done.

This is a matter of control. For example, a pilot will trust an embedded system when they know which agent should be in charge, whether the pilot or the embedded system, in a given context. Trust is also a matter of the reliability of the system. People tend to distrust a system when they experience too many failures and, therefore, need to manage uncertainty. This is a general rule; that is, systems can be scored concerning successes and failures—in the same way, communities of people score several web systems. This is the same for human errors. People who commit too many embedded errors tend to distrust the system. This could be caused by their level of proficiency with the system or the quality of the system itself. This relation between trust and reliability fosters more research efforts on physical tangibility (i.e., trust at the human hand level—the ability to grasp physical objects) and figurative tangibility (i.e., trust at the human mind level—the ability to grasp abstractions and concepts).

Considering the situational model for uncertainty management (Figure 1), trust or distrust may occur from uncertainty at various situational levels. Imperfect external sensors may cause this, failing human perception for various kinds of reasons (e.g., high workload, low vigilance, distraction), failing abductive inference and/or interpretation, and incomplete projection due to internal and external factors (e.g., time pressure, human error, complacency). Trust management is a matter of belief maintenance processes. In human-machine systems, trust management is strongly influenced by the quality of collaboration of the human–machine team. How this team is organized is crucial and depends on various human factors, including personality, intersubjectivity, delegation management, authority sharing, respect, feeling of freedom, acceptance of mandatory constraints, and so on. People would be reluctant to take risks if they do not trust themselves, the others involved, and their environment. Therefore, risk-taking relies on trust, and trust relies on uncertainty management.

Conclusion and perspectives

This chapter introduced concepts and approaches that enable the investigation of uncertainty management in life-critical systems. The proposed situational framework provides a language for handling uncertainty and risk and relationships between several meanings of situations and their interrelations.

We now understand that dealing with the unexpected strongly requires departing from the philosophy based on a linear approach that "filters" small variations from the start and equips human operators with procedures and automated machines, leaving them the responsibility to "discover" and handle unexpected events or surprises (Bainbridge, 1983). Unexpected events or surprises are mostly related to the nonlinearities that the filtering process and automation did not take into account. Instead, a new philosophy based on a nonlinear approach that acknowledges real-time systemic variations should lead to systems that consider technology, organizations, and people from the start, and structures and functions are incrementally developed in concert.

We must move from the now-conventional procedural approach where human operators are obedient soldiers (metaphor of the military) to a collaborative problem-solving approach where the actors are more autonomous musicians (metaphor of the orchestra; Boy, 2009, 2013a). This does not mean that operational procedures are not needed. They are useful in normal and most abnormal operations, but actors must learn how to override them to adapt to fluctuating situations. Risk-taking and complexity management are major skills that need to be developed. This is an educational and cultural issue (Boy, 2013b). Finally, dealing with the unexpected is not limited to life-critical systems; it is important in any scenario where people interact within complex sociotechnical environments.

Uncertainty management is at the core of system design (Grote, 2004). In fact, uncertainty is both in design and development and in operations. We saw that HITLS is needed during the whole life cycle of a human-machine system. HITLS allows for improving function allocation at design time and contributes to decreasing uncertainty by gaining system knowledge. In digital twins, HITLS enables one to observe and assess situation awareness, problem-solving, and action-taking during operations and maintenance. More specifically, modeling and HITLS help in uncertainty management during the whole life cycle of a human-machine system, as well as in discovering the system's emergent properties, structures, and functions. The more emergent properties are discovered and understood, the more the system's maturity is increased. HITLS of a complex human-machine system enables the people involved to become familiar with the various complexities of that system and helps detect inconsistencies, which are causes of uncertainty. Therefore, HITLS supports training and operational experience, especially when life is at stake.

We are at a crossroads of epistemological changes in how research, science, and practice are currently conducted. When I was offered to write this chapter on uncertainty management in work organizations, I immediately thought about uncertainty metrics, considering issues of noisy signals, incomplete information, and/or loosely articulated knowledge. Science is based on data, very well-designed institutionalized protocols, and methods for data crunching, aren't they? However, when we need to deal with abnormal, emergency, and sometimes unexpected situations in practice, where uncertainty is high, we need to act and take risks to reach goals, survive, and/or generally satisfy life-critical requirements. Abduction is then the cognitive process that enables risk-taking. It concerns situation awareness, preparation, deep knowledge, fine expertise, and courage to make evidence-based decisions. You may think that this is an oxymoron, but we need to be bold and humble at the same time. In other words, trust and collaboration are essential when facing a dangerous life-critical situation.

Hopefully, this chapter will pave the way to a new interdisciplinary approach that emerges from putting together clinical actions, creativity, team spirit, experience, and professionalism. We are at the heart of epistemology, where complexity science on the thinking side and risk-taking and creativity on the doing side should be intimately combined.

References

Amalberti, R., (2001). The paradoxes of almost totally safe transportations systems. *Safety Science*, *37*, 109–126.

Amalberti, R., Aroy, Y., Barach, P., & Berwick, D. M. (2005). Five system barriers to achieving ultrasafe health care. *Annals of Internal Medicine*, *142*(9), 756–764.

Amalberti, R., & Deblon, F. (1992). Cognitive modeling of fighter aircraft process control: A step towards an intelligent on-board assistance system. *International Journal of Man-Machine Studies*, *36*, 639–671.

Atkinson, D. (2012, November 4). *Human-machine trust* [PowerPoint slide presentation]. Presentation at the IHMC seminar, Pensacola, FL.

Bainbridge, L. (1983). Ironies of automation. *Automatica*, *19*(6), 775–779.

Barnes, J. (1982). *The presocratic philosophers* (rev. ed.). Routledge.

Berryman, S. (2016). Democritus. *Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/entries/democritus.

Boy, G. A. (2009, September 30–October 2). The orchestra: A conceptual model for function allocation and scenario-based engineering in multi-agent safety-critical systems. In *European Conference on Cognitive Ergonomics Proceedings*, edited by L. Norros, H. Koskinen, L. Salo & P. Savioja, published by VTT,1-7. SBN 978-951-38-6339-5.

Boy, G. A. (2013a). Dealing with the unexpected in our complex socio-technical world. In *Proceedings of the 12th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems*.

Boy, G. A. (2013b). From STEM to STEAM: Toward a human-centered education. In *Proceedings of the European Conference on Cognitive Ergonomic*. (Also available from the ACM Digital Library).

Boy, G. A. (2016). *Tangible interactive systems*. Springer, London, UK.

Boy, G. A., & Brachet, G. (2010). *Risk taking* (Dossier). Air and Space Academy.

Burks, A. W. (Ed.). (1958). *Collected papers of Charles Sanders Peirce, Vols. VII and VIII: Science and philosophy and reviews, correspondence and bibliography.* Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674138032.

Castelfranchi, C., & Falcone, R. (2000). Trust is much more than subjective probability: Mental components and sources of trust. In *Proceedings of the 33rd Hawaii International Conference on System Sciences,* Ralph H. Sprague (Ed.) (pp. 1–10), ISBN: 0-7695-0493-0.

Dain, S. (2002). Normal accidents: Human error and medical equipment design. *Heart Surgery*, *5*(3), 254–257.

Dubois, D., & Prade, H. (2001). Possibility theory, probability theory and multiple-valued logics: A clarification. *Annals of Mathematics and Artificial Intelligence, 32*, 35–66.

Endsley, M. R. (1995). "Toward a theory of situation awareness in dynamic systems." Human Factors: The Journal of the Human Factors and Ergonomics Society*,* 37(1), 32-64.

French, B., Duenser, A., & Heathcote, A. (2018). *Trust in automation – A literature review* (CSIRO Report EP184082). CSIRO, Australia.

Goldstein, J. (1999). Emergence as a construct: History and issues. *Emergence*, *1*(1), 49–62.

Grote, G. (2004). Uncertainty management at the core of system design. *Annual Reviews in Control, 28*, 267–274.

Grote, G. (2018). Managing uncertainty in work organizations. In R. A. Scott, M. Buchmann, & S. Kosslyn (Eds.), *Emerging trends in the social and behavioral sciences.* John Wiley & Sons, pp. 1-14.

Hardin, R. (2006). Trust. Cambridge, Polity, U.K.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts.* Ashgate Publishing.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal and coping*. Springer.

Lichtenstein, B. B. (2016). Complexity science at a crossroads: Exploring a science of emergence. *Academy of Management Annual Meeting Proceedings*, (ol 1), 12259. doi:10.5465/AMBPP.2016.38.

Llewellyn, D. J. (2003). *The psychology of risk-taking behavior* [PhD thesis]. University of Strathclyde.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*, 709.

Monod, J. (1970). *Le Hasard et la Nécessité: Essai sur la philosophie naturelle de la biologie moderne*. Éditions du Seuil.

National Transportation Safety Board. (2010). *Loss of thrust in both engines after encountering a flock of birds and subsequent ditching on the Hudson River US Airways Flight 1549 Airbus A320-214, N106US, Weehawken, New Jersey, January 15, 2009* (Accident Report NTSB/AAR-10/03 PB2010-910403).

Nilsen, T., & Aven, T. (2003). Models and model uncertainty in the context of risk analysis. *Reliability Engineering & System Safety*, *79*, 309–317.

Norman, M. D., Koehler, M. T. K., & Pitsko, R. (2018). Applied complexity science: Enabling emergence through heuristics and simulations. In S. Mittal, S. Diallo, & A. Tolk (Eds.), *Emergent behavior in complex systems engineering: A modeling and simulation approach*. Wiley. https://doi.org/10.1002/9781119378952.ch10, pp. 201-226.

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Piaget, J. (1952). *The origins of intelligence in children*. Norton.

Piaget, J. (1954). *The construction of reality in the child*. Ballantine.

Piaget, J. (1971). Examen critique de la thèse de Jacques Monod. Hasard et dialectique en épistémologie biologique. *Sciences*. Revue de la Civilisation Scientifique (71), 29–36.

Pinet, J. (2015). *Facing the unexpected in flight – Human limitations and interaction with technology in the cockpit*. CRC Press, Taylor & Francis.

Pinet, J. (2019). *Dysfunctions of complex systems: A time-wise method for the analysis of non-linear problems in HSI – Role of expertise and experience.* [Conference presentation] INCOSE HSI2019 International Conference on Human Systems Integration, Biarritz, France.

Pinet, J., & Bück, J. C. (2013). *Dealing with unforeseen situations in flight – Improving aviation safety* (Dossier 37). Air and Space Academy. http://www.academie-air-espace.com/upload/doc/ressources/Doss37_eng.pdf

Poincaré, H. (1885). L'Équilibre d'une masse fluide animée d'un mouvement de rotation. *Acta Mathematica*, *7*, 259–380.

Rasmussen, J. (1986). *Information processing and human-machine interaction.* Elsevier.

Thom, R. (1989). *Structural stability and morphogenesis: An outline of a general theory of models.* Addison-Wesley.

Thuan, T. X. (1998). *Le Chaos et l'harmonie.* Folio Essais, Gallimard.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*, 297–323.