Proceedings of the 12th IFAC/IFIP/IFORS/IEA Symposium Analysis, Design, and Evaluation of Human-Machine Systems,
Las Vegas, Nevada, USA. — August 11-15, 2013.

Dealing with the Unexpected in our Complex Socio-Technical World

Guy A. Boy
Human Centered Design Institute, Florida Institute of Technology, 150 W. University Blvd. Melbourne, FL 32901, USA
(Tel: 321-506-5073; e-mail: gboy@fit.edu)

Abstract: This paper presents and discusses the imperative necessity to use complexity science principles and approaches to deal with the open world where we live in. During the 20th century, we have developed theories, methods and tools based on linear approaches to engineering systems that consider unexpected and rare events as exceptions, instead of including them in the flow of everyday events, handled by well-trained and experienced experts in specific domains. Consequently, regulations, clumsy automation and operational procedures are still accumulated in the short term instead of integrating long-term experience feedback. This results in the concept of quality assurance and human-machine interfaces (HMI) instead of focusing on human-system integration. Quality assurance promoted standardization; HMI promoted corrective ergonomics, instead of human-centered design from the early stages of product life cycle. It is time to depart from this linear approach based on standardization and procedures to investigate our non-linear dynamic world based on expertise and flexibility. We promote human-centered processes such as creativity, adaptability and problem solving. We then need to be better acquainted with risk taking, preparation, maturity management, complacency emerging from routine operations, and educated common sense. These fundamental assets are presented using examples from various life-critical domains.

Keywords: Unexpected events, complexity, non-linear systems, human-system integration, creativity, problem solving, procedures, automation, experience, expertise, risk taking, control, management, regulations, life-critical systems, human-centered design.

1. INTRODUCTION

Sectors dealing with life-critical systems (LCS), such as aerospace, nuclear energy and medicine, have developed safety cultures that attempt to frame operations within *acceptable domains of risk*. They have improved their systems engineering approaches, developed more appropriate *regulations, operational procedures and training programs. System reliability* has been extensively studied and related methods have been developed to improve safety (Nilsen et al., 2003). *Human reliability* is a more difficult endeavor; human factors specialists developed approaches based on human error analysis and management (Hollnagel, 1998). Despite this heavy framing work, we still have to face unexpected situations that people have to manage in order to *minimize consequences***.** This paper presents and discusses the imperative necessity to use complexity science principles and approaches to deal with the open socio-technical world where we live in.

First, understand and deal with indetermination. Quantitative risk assessments are typically based on the (event-probability multiplied by consequence-magnitude) numerical product. This formula does not work when we deal with *small probabilities and huge consequences*; it is mathematically *undetermined*. The misconception that the unexpected is exceptional comes from this probabilistic approach of operations and more generally standardized life. In contrast, *LCS human operators deal with the unexpected all the time in their various activities*, and with possibilities and necessities instead of probabilities (Dubois & Prade, 2001).

Second, understand and deal with context and variations. During the twentieth century, we developed methods and tools based on *a linear*[1] approach of human-machine systems (HMS). We developed user *interfaces and operational procedures based on experience feedback* (IAEA, 2006). We have accumulated a giant amount of operational knowledge. In other words, we tried to close a world that is still open. As a result, anytime human operators deviate from the (linear) norm, we talk about noise, or even about the unexpected. Consequently, this model of the world tends to consider the *unexpected as an exception.* This could be explained by the fact that engineering was developed having the normal distribution in mind supported by the Gaussian function, and any event that deviates beyond a (small) given standard deviation could be ignored. This simplification does not take into account that *context* may change, and simplification assumptions made may turn to be wrong when context changes. Therefore, when a bigger *variation* occurs, it is considered as rare and unexpected. In other words, once such simplification is made we should be aware of its limitations instead of being surprised. Context-dependent systems are fundamentally dynamic and non-linear.

[1] Linearity can be understood in three ways: proportionality, single-causality or chronological order such as reading a paper-based book or document. Non-linearity does not satisfy these conditions, i.e., can be understood as non-proportionality, multiple-causality or out of chronological order such as browsing the Web. The use of procedures and standards leads to often-rigid linear processes and behaviors. Managing unexpected situation and problem solving requires flexible non-linear processes and behaviors.

Third, understand and deal with human-system integration. The twenty-first century started with the Fukushima nuclear tragedy (Ramana, 2011), which highlighted the fact that our linear/local approaches to engineering must be revised, and even drastically changed, emphasizing our world in a *non-linear and holistic* manner. This is not possible without addressing complexity in depth. *Nature is complex.* People are part of nature, therefore human-machine systems (HMS) are necessarily complex; even if machines could be very simple, people create complexity once they start interacting with these machines. Therefore, when talking about safety, reliability and performance, people are the most central element. Instead of developing user interfaces once systems are fully developed as it is still commonly done today (the linear local approach to HMS), it is urgent to integrate people and technology from the very beginning of design processes. This is why *human-system integration* (HSI) is now a better terminology than human-machine systems or human-computer interaction. The term "system" in HSI denotes both *hardware* (machine in mechanical engineering terms) and *software* (the most salient part of contemporary computers). In addition, integration remains a key issue that requires us to take into account technology, organizations and people at the same time (Boy, 2013a).

Forth, understand and deal with the dilemma between standardization and creativity. The necessary shift from linear/local to non-linear/holistic has tremendous repercussions on the way technology is designed. The engineering community rationalized design and manufacturing, and produced very rigid standards to the point that it is now very difficult to design a new LCS without being constantly constrained and forbidden from any purposeful innovation. To a certain extent, *standardization* is a successful linearization of highly rationalized domains. In aviation, even human factors have been standardized (EASA, 2004). However, we tend to forget that *people* still have fundamental assets that machines or standardization systems do not and will never have, they *are creative, adaptable and can solve problems that are not known in advance.* These assets should be better used both in design and operations. Standard operational procedures are good socio-cognitive support in complex operations, but competence, knowledge and adaptability are always the basis for solving hard problems. For that matter, both non-linear/holistic and linear/local approaches should be used, and in that order. They should be combined putting non-linear/holistic at the top (the design part) and linear/local at the bottom (the implementation part). In other words *human-centered design* should oversee technology-centered engineering, like an architect would oversee builders (Boy, 2013a).

It is time to (re-)*learn how to deal with the unexpected using a non-linear approach,* where *experience and expertise* are key assets. LCS operations require knowledge and competence in complex systems design and management, the domain at stake (e.g., aerospace, nuclear), *teamwork* and *risk taking.* Dealing with the unexpected requires *accurate and effective situation awareness, synthetic mind, decision-making capability, self-control, multi-tasking, stress management and cooperation* (team spirit). This paper presents a synthesis using examples in the aviation domain compiled from a conference organized in 2011 by the Air and Space Academy on the subject (ASA, to appear).

2. FROM MECHANICS TO SOFTWARE TO COMPUTER NETWORKS

Our socio-technical world drastically changes. When I was at school, I learned to simplify hard problems in order to solve them using methods and techniques derived from linear algebra, for example. This is a very simplified view of what my generation learned but it represents a good image of the 20th century engineering background. We developed very sophisticated applied mathematics and physics approaches to build cars, aircraft, spacecraft and nuclear power plants for example. Indeed, everything that engineers learned and used was very much linear by nature. Any *variability* was typically considered as noise, which needed to be filtered. We managed to build very efficient machines that not only extended our capabilities, but also enabled us to do things that were not naturally possible before.

The 20th century was the era of mechanics more than anything else, conceptually and technologically speaking. Then a new era came supported by the development of modern computers where software took a major role. Software introduced a totally different way of thinking because machines were able to perform more elaborate tasks by themselves. We moved from manipulation of mechanical devices to interaction with software agents. We moved *from control to management.* In aeronautics, the first glass cockpits and fly-by-wire technology drastically changed the way pilots were flying. Information technology and systems invaded cockpits and intensively support pilots' activities. New problems arose when systems fail and manual reversion is necessary. In other words, nowadays pilots not only need to master the art of flying, but they also need to know how to manage systems. Even if these systems have become more reliable and robust, they do not remove the art of flying. We always need to remember that flying is not a natural capability of people, it is a cognitive ability that needs to be learned and embodied by extensive and long training.

This brings to the front the difficult issue of *tools versus prostheses.* We never stopped automating technology. Automation can be seen as a natural extension of human capabilities. That is a simple transfer of cognitive and physical functions from people to machines; a very mechanical view of automation. Rasmussen's model is an excellent example of a mechanistic model of human behavior that contributed to the development of cognitive engineering (Rasmussen, 1986). In reality, building an aircraft for example is not a function transfer because people do not naturally fly; we are handicapped compared to birds, and therefore an aircraft is a prosthesis that enables us to fly. In a sense, the aircraft is a cognitive entity that was built using methods and tools developed by mechanical engineers and now information technology specialists.

During the nineties, many research efforts were carried out in human factors on ironies of automation (Bainbridge, 1983), clumsy automation (Wiener, 1989), and automation surprises (Sarter et al., 1997). Engineers automated what was easy to automate, leaving the responsibility of complex things to human operators, such as abnormal conditions. What was called automation surprises is actually related to the topic of this paper on the unexpected. However, none of these research efforts did take into account *technology maturity and maturity of practice* (Boy, 2013a). People take time to become mature and learn. It is the same for technology and its usages. It takes many surprises to learn. Maturity is related to autonomy. Autonomy differs from automation in the sense that the former relates to problem solving and learning, as the latter relates to procedures following whether for machines or people. Indeed, without appropriate understanding, embodiment and critical thinking, procedure following is a kind of people behavior automation (Boy, 2013a). Machines can be automated but are still far from being autonomous like people can be. Consequently, technological automation also requires appropriate understanding, embodiment and critical thinking at operations time.

Today, things are getting more difficult when we continue to use mechanistic cognitive models because our socio-technical world becomes more *interconnected*. Instead of mechanical devices, we have many pieces of software highly interconnected. Instead of complicated devices that we could deconstruct and repair, like the old mechanical clocks, we have layers of software that are difficult, and most of time impossible, to humanly diagnose when they fail, e.g., modern cars are comprised of electronics and software, and only sophisticated diagnostic systems enable troubleshooting. The level of technology and related-usages complexity drastically changed with the introduction of software. It is now even more complex as computer networks are not only local (e.g., in the car), but also more global (e.g., among cars and other cars with collision avoidance systems). How do we deal with the unexpected, and more generally variability, in such highly interconnected world?

3. HANDLING COMPLEXITY: LOOKING FOR NEW MODELS

Here are four examples of so-called "successful accidents": the aborted Apollo 13 mission after an oxygen tank exploded on April 13, 1970; the DHL A300 landing in Bagdad shot by a missile on November 22, 2003; the US Airways A320 landing on the Hudson River after loosing both engines on January 15, 2009; the Qantas A380 recovery around Singapore after the explosion of an engine on November 4, 2010 (ASA, to appear). These examples are described in more details in section 4 of this paper. They show that people can handle very complex and life-critical situations successfully when they have enough time (Boy, 2013b) and are equipped with the right functions, whether in the form of training and experience, or appropriate technology; in addition, these functions should be handled in concert. Consequences are about life and death. We can see that problem solving and cooperative work are major ingredients of such successful stories. The main question here is to maintain a good balance between automation that provides precision, flawless routine operations and relief in case of high-pressure situations, and flexibility required by human problem solving. Obviously, conflicts may occur between automation rigidity and people's flexibility. Let's analyze this dilemma.

Automation will continue to develop taking into account more tasks that pilots use to perform. It is also clear that, at least for commercial passenger transportation, pilots will be needed to handle unexpected situations for a long time. There will be surprises that will require appropriate reactions involving good situation awareness time-wise (Boy, 2013b) and content-wise, decision-making, self control, stress management and cooperation with the other actors involved. Dealing with the unexpected is not really a new skill that pilots should have, but instead of being frightened by the evolving complexity of our socio-technical world, we should better understand and use this complexity. For example, since the airspace capacity will continue to increase, it is better to use its *hyper-redundancy* to improve safety and constant management of unexpected situations, i.e., small and bigger variations of it.

Automation rigidifies operations. Operational procedures also rigidify operations, since they tend to automate human operator's behavior. Therefore, both automation and procedures need to be used with a critical spirit, competence and knowledge. Human operators dealing with highly automated life-critical systems need to deeply know and understand the technology they are using, especially when this technology is not fully mature. Automation is good when it is designed and developed by considering its users, and when it has reached an acceptable level of maturity (Boy, 2013a). There are even situations where people may switch to automation to improve safety. This requires competence, situation awareness and great decision-making skills.

Automation shifted the human operator's role from basic control to supervisory control and management (Sheridan, 1984). Instead of directly manipulating handles and levers, human operators push buttons in order to manage systems. These systems are often qualified of agents (Boy, 1998). Therefore, this new work environment involves human agents and artificial agents. We talk about humans and systems as a multi-agent environment, and ultimately human-system integration. This shift from control to management involves new *emergent properties* that need to be clearly identified. People in charge of such multi-agent environments need to know and understand these emergent properties. For example, it is now known that automation increase complacency in the long term, especially when it works very well. More generally, the best way to face the unexpected is to move *from task training to skill training*, such as astronaut training where they learn humility, time-constrained situations that require simple and effective solutions, and the most appropriate use of technology (considered as a tool and not as a remedy).

For example, the airspace is evolving everyday toward more aircraft in the sky, especially in terminal areas. In 2011, the Federal Aviation Administration (FAA) anticipated that U.S. air transportation would double over the next two decades (Huerta, 2011). EUROCONTROL anticipated similar air traffic growth over the same period of time in Europe (Gregorova, 2010). This growth tremendously changes the way air traffic control will be performed during future decades. In particular, the increasing number of aircraft and their interconnections will cause new complexity issues and emergences of new unexpected properties that we will need to identify and manage. Air traffic control will progressively evolve toward air traffic management. Air traffic controllers will become air traffic managers. During the PAUSA project, we identified various changes in authority sharing and a new model that we called the *Orchestra* model (Boy, 2013a; Boy, 2009).

Until now, air traffic control (ATC) had authority on aircraft. We took the metaphor of the military where the general has authority on the chain of command down to the soldier. Within the Military model, information flows are hierarchical, linear and sequential. In contrast, in the Orchestra model, soldiers have become musicians (i.e., more specialized, cooperative and autonomous). The conductor replaces the general who coordinates the various information flows that have become more non-linear and parallelized. In addition, the composer generates scores (prescribed tasks) that musicians follow to perform (effective task or activity). The composer coordinates these scores before delivering the symphony. We observed this very interesting change in the shift from ATC to air traffic management (ATM), where scores are contracts (Boy, 2009). Today, we need to better define the function (jobs) of composers, conductors and musicians, as well as the overall organization of the Orchestra.

Until now, air traffic controllers had a reasonable number of aircraft to control. They knew where aircraft were located using radar technology. Their job consisted in ensuring a fluid traffic flow with no conflicts leading to collision. A new type of complexity emerges from traffic over saturation in final areas. In the future, instead of controlling they will need to manage like a conductor would manage an orchestra. Conductor's situation awareness has to be perfect from beginning to end of play. They need to deal with various personalities. They are managers in the sense of authority, effectiveness and professionalism. They are self-confident and have a good sense of humor. A good conductor knows about emerging patterns that an orchestra produces. He or she needs to identify these patterns in order to have the required authority.

The management of life-critical systems is always based on a model, whether the Military or the Orchestra models for examples, which needs to be further elicited. We already argued that if we use the traditional linear model, where operational procedures could support most kinds of situations, the unexpected is typically considered as an exception to the rule or procedure. However, if we are in the non-linear model of life, where problem solving is the major resource, the unexpected is an everyday issue that deals with care, concentration and discipline.

4. RISK TAKING: DEALING WITH NON-LINEAR DYNAMIC SYSTEMS

What do successful risk takers do? They prepare everything in detail before starting their activity. They usually detect all possible recovery situations where they can end up safe when everything goes wrong. They need to know and embody these kinds of things; "depending on their feeling of the situation, then they do not go." They also need to know their limitations, which need to be compatible with the risk they will take. Preparation and risk assessment are key. They also need to accept that it takes a long time to learn these skills.

Taking a risk involves a logical *abduction* process (Boy & Brachet, 2010). Abduction is one of the three inference mechanisms with deduction and induction. Abduction is about postulating a possible future and demonstrating that we can manage to reach it. John F. Kennedy abducted that Americans will go to the Moon and get back safe to Earth; NASA demonstrated that to be true in less than a decade. This is typically what great visionaries do. Abduction requires competence, knowledge and understanding of the world, not necessarily to have a good idea, but to make sure that it is reachable. Abduction deals with *goal-driven behavior*, characterizing people's intentions and actions. It is generally opposed to event-driven behavior, characterizing people's reactions to events. In fact, people constantly switch from one to the other using an opportunistic behavior. In aviation, pilots learn how to "think ahead" (this is a kind of abduction) and constantly shift from goal-driven to event-driven behaviors.

Risk taking deals with discipline, i.e., there are *safety margins* that cannot be overridden and experts know them, therefore they are very *disciplined* and respect these safety margins scrupulously. The main difficulty is to handle the complexity of a risky situation. Complexity comes from the large number of factors involved. For example, a typical aviation situation results from a dynamic and non-linear combination of aircrew psychological and physiological state, 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), actual 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 in mind expected aviation situation patterns built from experience, and in practice what happens is never what they anticipated. However, the variation between the expected situation and the actual situation is most of the time very little, and is handled very smoothly. In some cases, such variation can be much bigger (Fig. 1) such as in Apollo 13, which was an excellent example of a very well orchestrated operation.

In space programs, ground and board are very well coordinated both at design and operations times (i.e., astronauts as musicians are very well trained, responsible and autonomous; they know how to use the scores produced by a variety of engineers and scientists, as composers; flight director and control room officers are conductors). When the Apollo 13 explosion occurred and oxygen tank no. 2 in the service module broke, in three hours, they lost all oxygen stores, water, electrical power, and use of the propulsion system. The service module was no longer usable, and astronauts needed to use power and consumables of the lunar module that became the lifeboat for Apollo 13. An excellent teamwork started among the actors both onboard and on the ground. Ground mission control provided instructions (like a composer provides scores), and astronauts built a supplementary carbon dioxide removal system out of plastic bags, cardboard, parts from a lunar suit and a lot of tape! Even if the astronauts did not go to the Moon that time, they got back safe to Earth. In fact, they did their job!

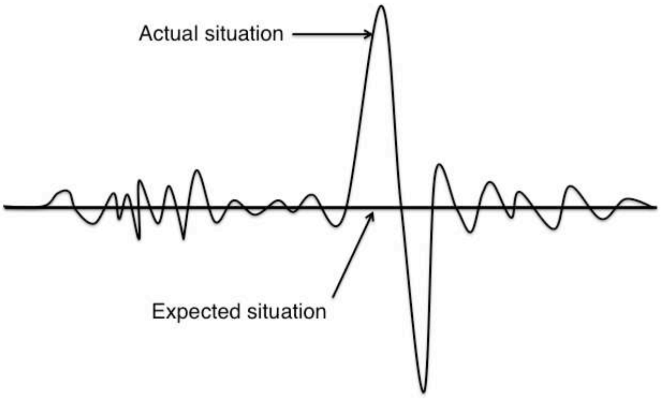

Fig. 1. Expected and actual situation showing small and bigger variations.

Shortly after takeoff from Baghdad airport, terrorists shot a DHL A300 cargo plane. The left wing tip was struck by a surface-to-air missile, which caused the loss of hydraulic flight control systems; the aircraft was uncontrollable in a classical way. 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., non-linear flight dynamics and mechanics first principles), and they did it successfully.

US Airways Flight 1549 suffered a double bird strike after takeoff from LaGuardia airport. No engine was available. Consequently, the aircrew had to fly the aircraft as a glider. This was a very challenging situation especially in a populated area such as the New York area. The captain had to make a decision that was not in the book! He had to solve a problem. Once he made his decision, he managed the situation until he successfully landed the Airbus A320 in the Hudson River (i.e., goal-driven behavior in a very constrained environment). Again, all crewmembers did their jobs.

One of the engines of the Qantas A380 Flight 32 exploded en route over Batam Island, Indonesia. Explosion damaged the fuel system causing leaks, disabled one hydraulic system and anti-block brakes, and caused engines 1 and 4 to go into a "degraded" mode, damaged landing flaps and the controls for the outer left engine 1. It took 50 minutes to complete this initial assessment, due to the interconnectivity and non-linearity of numerous operational procedures. No panic; all crewmembers made their jobs very professionally, behaving like in a simulator. They returned to Singapore and landed safely with four tires blown. They did their jobs, managing the actual situation (ASA, to appear).

These extreme cases are the top of the iceberg of non-linear system dynamics variations. It is useful to better understand *complexity theories*, such as catastrophe theory, bifurcation theory and chaos theory, as opposed to conventional reductionism. In the catastrophe theory for example, we can learn that there are patterns that are inevitable catastrophes (Thom, 1989). In the bifurcation theory, we learn that for a small light change on a "bifurcation" parameter value of a system, a sudden "qualitative" or topological change occurs in its behavior (Poincaré, 1885), e.g., a small change in temperature and pressure, may suddenly change steam into ice. In chaos theory (Thuan, 1998), we can learn that for very small variation in some variables, the behavior of the overall system may become incontrollable after a while, but generates persistent patterns, called attractors, which can be identified and therefore managed. This non-linearity needs to be understood and appropriated in various contexts by human operators who deal with life-critical systems. In particular, they need to understand that some parameters have a direct influence on the qualitative nature of the system behavior.

Managing the unexpected is what remains to people over systems. It is the necessary operational glue that maintains the overall stability and integrity of human-machine systems. These people need to be able to understand what is going on, make their own 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 only believe that regulations, standards and procedures will support safety with this fallacious expectation of zero risk.

Now, how can we train people to manage these variations between the expected situation and the actual situation? 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 apply on 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 socio-technical systems, we can experience both kinds of stability. Experience provides cases that can be categorized and further associated with appropriate behaviors related to either passive or active stability. In cases where passive stability prevails, we need to let go instead of counter-interact with the system, especially when automation does the job for us. When active stability is at stake, a proactive behavior is required.

LCS human operators require very important *skills* such as creativity, familiarity, availability, adaptability (or flexibility), dependability and boldness. Indeed, any actor who needs to face unexpected situations is required to be:

- creative and foreseeing possible futures; for example, when Captain Sullenberger decided to land his Airbus 320 on the Hudson river on January 15, 2009, he was creative and, for sure, investigated all other possibilities before taking the risk (NTSB, 2010);
- familiar with the environment where they work; for example, flying skills in various atmospheric situations and aircraft configurations;
- familiar with the various tasks that they have to perform; for example, normal and abnormal tasks experienced in a flying simulator;
- familiar with personal capabilities and limitations; for example, reduced perception of night situations while driving or working memory cognitive limitations;
- familiar with organizational constraints and possibilities; for example, responsibility and accountability related to a job in an organization;
- familiar with technological constraints and possibilities; for example, automation limitations and advantages in a large variety of situations;
- available anytime anywhere during duty time; for example, management of complacency in case of routine activities and maintenance of proactive behavior;
- adaptable (or flexible) to any operational situation; for example, facing an unexpected event such as wind shear, pilots will fit their behavior with respect to changes in their environment; they know the various contextual responses to wind shear (Skybrary Aero);
- dependable in life-critical situations; for example, a mountain guide is typically trustworthy in dangerous situation with his or her clients;
- bold in risk taking; for example, facing an unexpected life-critical situation a human operator should have the courage to take an appropriate action that may put his or her life in danger.

All these skills should be learned form *experience* (learning by doing). The use of simulators enables human operators to experience various kinds of situations and configurations, which would never be possible to experience in the real world because they would be too dangerous. These skills are not only individual, but also collective. They should be intelligently articulated during operations. This articulation process is another skill that needs to be learned. Therefore, trust is an important quality to be developed by team members who are likely to deal with life-critical systems and, for that matter, face unexpected life-critical situations.

5. DISCUSSION

Dealing with the unexpected triggers various kinds of human factors such as time pressure and workload management, multi-tasking and complexity management. This is why anything that can be performed by technology should be continuously understood both statically and dynamically. Let's take an example.

2011 Fukushima Daiichi nuclear disaster is certainly one of the most unexpected events of that type in the nuclear industry. Let's analyze what "unexpected" means in this case. Taking into account the exceptionally low probability of occurrence of an earthquake (9.0 magnitude on the Richter scale) followed by a tsunami (40 meter waves, but the plant was designed to resist to 5.7 meter waves and the plant was struck by 10 meter waves), and the extreme magnitude of the consequences, the formula (event-probability * consequence-magnitude) leads to indetermination. Therefore, the conventional technological reliability approach does not work here. Once an unexpected event occurs, people in charge have to make decisions. A domino effect started and led to the fact that there were not enough generators to cool the plant to a complete safe shutdown phase (Schmitt, 2012). It was concluded that automation in this situation was insufficient for the events that occurred, and passive and fully automated systems would have significantly modified the outcome of the catastrophe.

However, even if technology is well designed to ensure safety, people may become too confident and/or may not have received training to handle specific situations; these factors are likely to induce unrecoverable situations. This is the case of the Air France 447 accident over the Atlantic on June 1, 2009. The final report (BEA, 2012) stated that "the accident resulted from a succession of events: temporary inconsistency between the airspeed measurements, probably following an obstruction of the Pitot tubes by ice crystals, that caused the autopilot to disconnect; inappropriate control inputs that destabilized the flight path and led to a stall; and pilot misunderstanding of the situation leading to a lack of control inputs that would have made it possible to recover." In reality, these are contributing factors, and we need to consider that the captain left the cockpit to rest "in accordance to common practice", and delegated the flight task to the least experienced co-pilot on-board; he re-entered the cockpit when it was too late. The co-pilot flying the aircraft made "nose-up inputs despite stall warnings, causing a fatal loss of airspeed and a sharp descent." Stall warning sounded for 54 seconds, which is a long time. The problem is that pilots had not received specific training in "manual airplane handling of approach to stall and stall recovery at high altitude"; this was not a standard training requirement at the time of the accident. None of the pilots understood what was happening. This is a typical case where appropriate training and airmanship could have greatly contributed to avoid the accident. In addition, the absence of expert leadership redundancy and involvement was critical.

In these two examples, function allocation between people and automation was a major issue. What should we automate? What should be the role of people in charge of life-critical systems? In all cases, it is crucial to determine the various roles (and authority) of people and technology, but also the way people and systems are organized. Roles should be associated to relevant contexts and appropriate resources. Of course, resources should be available in the various operational contexts. The three attributes (role, context, resources) correspond to the definition of cognitive functions (Boy, 1998). Therefore, cognitive function analysis is a good approach to anticipate appropriate function allocation among human and system agents.

Finally, *time* is critical to manage failures, incidents and accidents. Time can be analyzed at various levels such as operational and maturity levels. At the operational level, an equation relates the required time (TR) to the available time (TA) to do something (Boy, 2013b). The more the ratio TR/TA is close to one and get bigger than one, the more it is difficult for human operators to handle the situation at stake. Obviously, even in very dangerous situations, human operators are able to handle safety margins because this ratio is less than one. At the maturity level, criteria such as safety, efficiency and comfort are constantly optimized, and we end up with a maturity period already explained elsewhere (Boy, 2011).

6. CONCLUSION

This paper introduced concepts and approaches that enable the investigation of unexpected events and deal with them in our complex socio-technical world. We saw that it is a question of Technology, Organizations and People (the *TOP model)*. Technology can greatly help time pressure and complex situation management by supporting humans in case of excessive workload. Of course, such highly automated technology should be reliable, dependable and mature. It should also be understood by the human operators involved in the control and management of the life-critical system at stake. Organization is another support for handling unexpected events. Communication, cooperation and coordination are important processes that need to be developed to ensure good collective situation awareness. Team spirit and trust are crucial assets. People involved, whether designers or users, must be competent, creative and familiar with all aspects of the situation, available, dependable, and bold. This takes extensive training and operational experience, motivation and enthusiasm.

We now understand that dealing with the unexpected strongly requires a *new philosophy* of operations departing from a linear approach that removes small variations from the start and "discovers" unexpected events to a non-linear approach that takes care of these variations in real-time. We need to 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, 2013a). This does not mean that operational procedures have to be removed. They are very useful in normal and abnormal operations, but actors have to learn how to override them to adapt to fluctuating situations. Risk taking and complexity management are major skills to develop. This is an *education* issue (Boy, 2013c). Finally, dealing with the unexpected is not limited to LCS; it is important in any scenario where people interact within complex socio-technical environments.

7. ACKNOWLEDGEMENTS

The author thanks Wafa Almukadi, Sharon Chinoy, Jarrett Clark, Ondrej Doule, Patrick Millot and Jean Pinet for their very insightful comments that contributed to improve the quality of this paper. This research is part of the French-American Project "Risk Management in Life Critical Systems" funded by the Partner University Fund.

8. REFERENCES

ASA (to appear). *Dossier on Air transport pilot facing the unexpected*. Air and Space Academy. Paris, France. http://www.academie-air-espace.com/event/newdetail.php?varCat=14&varId=216

Bainbridge, L. (1983). Ironies of Automation. *Automatica*, Vol. 19, No. 6, pp. 775-779.

BEA (2012). On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris. Final Report. Bureau d'Enquêtes et d'Analyses, Paris, France.

Boy, G.A. (1998). *Cognitive Function Analysis*. Ablex / Greenwood Publishers, Westport, CT, USA. ISBN 9781567503777.

Boy, G.A. (2009). The Orchestra: A Conceptual Model for Function Allocation and Scenario-based Engineering in Multi-Agent Safety-Critical Systems. *Proceedings of the European Conference on Cognitive Ergonomics*, Otaniemi, Helsinki area, Finland; 30 September-2 October.

Boy, G.A. & Brachet, G (2010), Risk Taking. Dossier of the Air and Space Academy, Toulouse, France, ISBN 2-913331-47-5.

Boy, G.A. (2011). Conclusion of the *Handbook of Human-Machine Interaction: A Human-Centered Design Approach*. Ashgate, U.K.

Boy, G.A. (2013a). *Orchestrating Human-Centered Design*. Springer, U.K.

Boy, G.A. (2013b). Time in life-critical human-computer interaction. *Workshop on Changing Perspectives of Time in HCI. ACM CHI'13*. Paris. France.

Boy, G.A. (2013c). From STEM to STEAM: Toward a Human-Centered Education. Proceedings of the *European Conference on Cognitive Ergonomics*, Toulouse, France. Also available from the ACM Digital Library.

Dubois, D. & Prade, H. (2001). Possibility Theory, Probability Theory and Multiple-valued Logics: A Clarification. *Annals of Mathematics and Artificial Intelligence,* 32, pp. 35-66.

EASA (2004). www.easa.eu.int/doc/rulemaking/nPa/nPa_15_2004.pdf.

Gregorova, M. (2010). *EUROCONTROL Long-Term Forecast: Flight Movements 2010 – 2030.* CND/STATFOR Doc415. Eurocontrol, 96 Rue de la Fusée, B-1130 Brussels.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method: CREAM*. Oxford: Elsevier Science.

Huerta, M.P. (2011). *FAA Aerospace Forecast: Fiscal Years 2012-2032*. U.S. Department of Transportation, Federal Aviation Administration, Aviation Policy and Plans. http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/2012%20FAA%20Aerospace%20Forecast.pdf.

IAEA (2006). *A system for the feedback of experience from events in nuclear installations*. Safety Guide no. NS-G-2.11. IAEA Safety Standards. International Atomic Energy Agency, Vienna, ISBN 92-0-101406-6.

Nilsen, T. & Aven, T. (2003). Models and Model Uncertainty in the Context of Risk Analysis. *Reliability Engineering & System Safety*, 79, pp. 309-317.

NTSB (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.

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

Ramana, M. V. (2011). Beyond our imagination: Fukushima and the problem of assessing risk. *Bulletin of the Atomic Scientists.*http://thebulletin.org/web-edition/features/beyond-our-imagination-fukushima-and-the-problem-of-assessing-risk.

Rasmussen, J. (1986). *Information Processing and Human-Machine Interaction*. Amsterdam: Elsevier.

Sarter, N.B., Woods, D. D. & Billings, C.E. (1997). Automation Surprises. In G. Salvendy (Ed.), *Handbook of Human Factors & Ergonomics*, second edition, Wiley.

Schmitt, K.A. (2012). Automations influence on nuclear power plants: A look at three accidents and how automation played a role. *Proceedings of the 2012 IEA World Congress*, Recife, Brazil. IOS Press. Work 41, DOI 10.3233/WOR-2012-0035-4545.

Sheridan, T.B. (1984). Supervisory control of remote manipulators, vehicles and dynamic processes: experiment in command and display aiding. In *Advances in Man Machine Systems Research*, Vol. 1, pp. 49-137.

SkybraryAero http://www.skybrary.aero/index.php/Low_Level_Wind_Shear

Thom, R. (1989). *Structural Stability and Morphogenesis: An Outline of a General Theory of Models*. Reading, MA: Addison-Wesley, 1989. ISBN 0-201-09419-3.

Thuan, T.X. (1998). *Le Chaos et l'harmonie – La fabrication du réel.* Folio Essais, Gallimard, Paris.

Wiener, E.L. (1989). *Human factors of advanced technology ('glass cockpit') transport aircraft.* Technical Report 117528. Moffett Field, CA: NASA Ames Research Center.