Edge Awareness – A Dynamic Safety Perspective on Four Accidents/Incidents

Patrik Stensson[a] and Anders Jansson[b]

[a] Department of Informatics and Media
Uppsala University, Uppsala, Sweden

[b] Department of Information Technology
Uppsala University, Uppsala, Sweden

ABSTRACT

A framework focusing on the difference between situation awareness and edge awareness is presented. It consists in distinguishing system awareness from situation awareness, and introducing edge awareness as the candidate mental state to be used as a lodestar in design of resilient systems and to avoid future systems disasters. A case-study on four well known accidents/incidents is presented. The investigation reports are filtered through the new framework resulting in alternative interpretations of the causes of the accidents. It is concluded that the role of calculative models in systems disasters must be examined thoroughly, and that one way to counteract for such disasters is to design for edge awareness. Having edge awareness means being involved in and aware of how situations develop, how systems contribute and how these aspects combine into a joint and an emergent phenomenon. Edge awareness is the basis for responsible and autonomous decisions.

Keywords: Human Systems Interaction, Systems Engineering, Situation Awareness, Edge Awareness

INTRODUCTION

It does not matter if you like to keep a safe distance to every possible edge there is, if you get your kicks from 'living on the edge', or if you end up in a situation where you have to defeat an opponent by being the better at getting close to an edge. It is in any case of crucial importance to be thoroughly aware of the edge. Otherwise you may unintentionally slip over and fall helpless into whatever it means to be on the other side. Consequences from issues with human-systems interaction and lack of edge awareness are therefore of concern for everybody. In this paper, we propose a framework for different types of awareness, focusing on the difference between the contemporary interpretations of situation awareness and the complementary concept of edge awareness. First, a rationale for this approach is presented and we argue that emergent properties of hazardous situations need to be addressed properly if safety in terms of resilient systems is the ultimate goal, not only safety based on calculative models. Second, we present a case-study on two accidents with catastrophic consequences, and two incidents that ended without loss of lives, although, events causing a lot of harm and distrust. The cases are all well investigated and the reports are filtered through the new framework. We end by discussing the value of edge awareness in relation to the conclusions in the investigation reports and in relation to the contemporary understanding of situation awareness.

EDGE AWARENESS

While Edge Awareness (EA) obviously is a mental phenomenon, and thereby principally similar to Situation Awareness (SA), there is still a crucial difference (Stensson 2014). To explain the distinction it is first necessary to consider emergence, a somewhat controversial concept within philosophy of science. Emergence describes phenomena that are "neither predictable from, deducible from, nor reducible to the parts alone" (Goldstein 1999, p. 57) and it is a central concept to the stratified world-view of critical realism (e.g. Bhaskar 2008). Phenomena of higher strata may be dependent on (they are rooted in) phenomena of lower strata, but cannot be fully explained by the lower aspects, in particular they cannot be explained away as in reduced to phenomena of lower strata. For example, certain biological mechanisms are rooted in chemistry but still emergent biological phenomena irreducible to the mechanisms of chemistry (Collier 1994, pp. 107-111). Emmeche et al. (1997) suggests four primary levels of emergence: the physical, the biological, the psychological, and the social. Awareness of any kind is emergent at the psychological level but SA and EA are both concerning phenomena from the physical level, which is in accordance with the present context of human-systems interaction. Moreover, the intertwining of system 1 and system 2 mental processes (Stanovich and West 2000, Kahneman 2003, 2011) suggests that psychological phenomena via the intuitive system 1 are highly dependent on practical involvement of the body and the brain (the biological level), which is particularly true for edge awareness, we argue. The difference between EA and SA can be described as that they are mental states about phenomena from different strata.

The perhaps most important distinguishing aspect of edge awareness is its connection with dynamics and the representation of time. Mathematically it is not a problem to represent dynamics by having time progressing in infinitesimal steps implying discrete state transitions of modeled parameters. Essential dynamic aspects such as speed and acceleration are formally well-represented analytically by higher order derivatives of basic state functions (with time as the independent variable). However, for system operators real-life implications of several such higher order aspects in conjunction are poorly represented as state data, no matter how many formally correct parameters that are used. Getting 'the hang' of the momentum of a vehicle traveling through a certain environment is to become aware of one emergent phenomenon, if seen from the involved perspective of the driver. Formally, the phenomenon is a performance relation between one or several physical properties of the technology and one or several physical properties of the environment. Essentially, the phenomenon is an emergent aspect within higher strata than that in which the basic parameters reside. Maintaining steerage-way speed of a vessel is describable but not understandable in terms of situation and system parameters, understanding requires being involved in the dynamic progress of the overall situation. Edge awareness is about such compound dynamic phenomena, it is about phenomena that perhaps are describable from a detached perspective but not understandable. The distinguishing characteristics of edge awareness is that it is about phenomena that are emergent within a situation as a whole, it is about phenomena that makes no or little sense when considered from a lower stratum such as that of analytical physics merely speaking mathematics. Edge awareness is not reducible to a discrete representation of time. This is similar to how strategies in dynamic decision making tasks (Brehmer 1992) cannot be reduced to single snap-shot judgments and choices.

Means for involved and situated (i.e. in-the-loop) system control are essential for edge awareness, for rich contextual interpretations of system effects, and for local judgments of values. The local nature of a system is obscured without situated controllability implying that a lack of contextual relevance for effects will remain unknown, which for model-based usefulness is a non-existing issue as this aspect is not part of the equation. Out-of-the-loop performance problems are associated with several complex issues such as vigilance decrements, complacency and over-trust in automation, as well as control skill decay (Endsley and Kiris 1995, Kaber and Endsley 1997, Endsley and Kaber 1999). In addition, lack of edge awareness obstructs the developing of incentives for consciously diverging from predetermined routes because without it options and consequences become difficult to discern. To consciously diverge from a predefined route is analogous to rejecting a proposal or withstand persuasion, an essential aspect of having a free will. Edge awareness is therefore crucial for human emancipation and autonomy because to adopt and accept externally defined values and behaviors implies heteronomy (Kant 1785, Stensson and Jansson in press).

As described above, EA is different from the contemporary approach to SA. Endsley's (1995) information processing-based three-level model of SA is divided into perception, comprehension and projection. EA is not possible to divide into lower levels of strata, that is, reduced to the mental states it is rooted in. EA is different from distributed situation awareness (Stanton et al 2006) because it cannot be reduced to the sum of the understanding of situation (environment) and system. Finally, measurement of EA cannot be approached in the same manner as measurement of SA (Fracker 1991). Any attempt to measure EA would run into the problem of poor representation. Figure 1 below shows the relation between EA and SA/SysA.

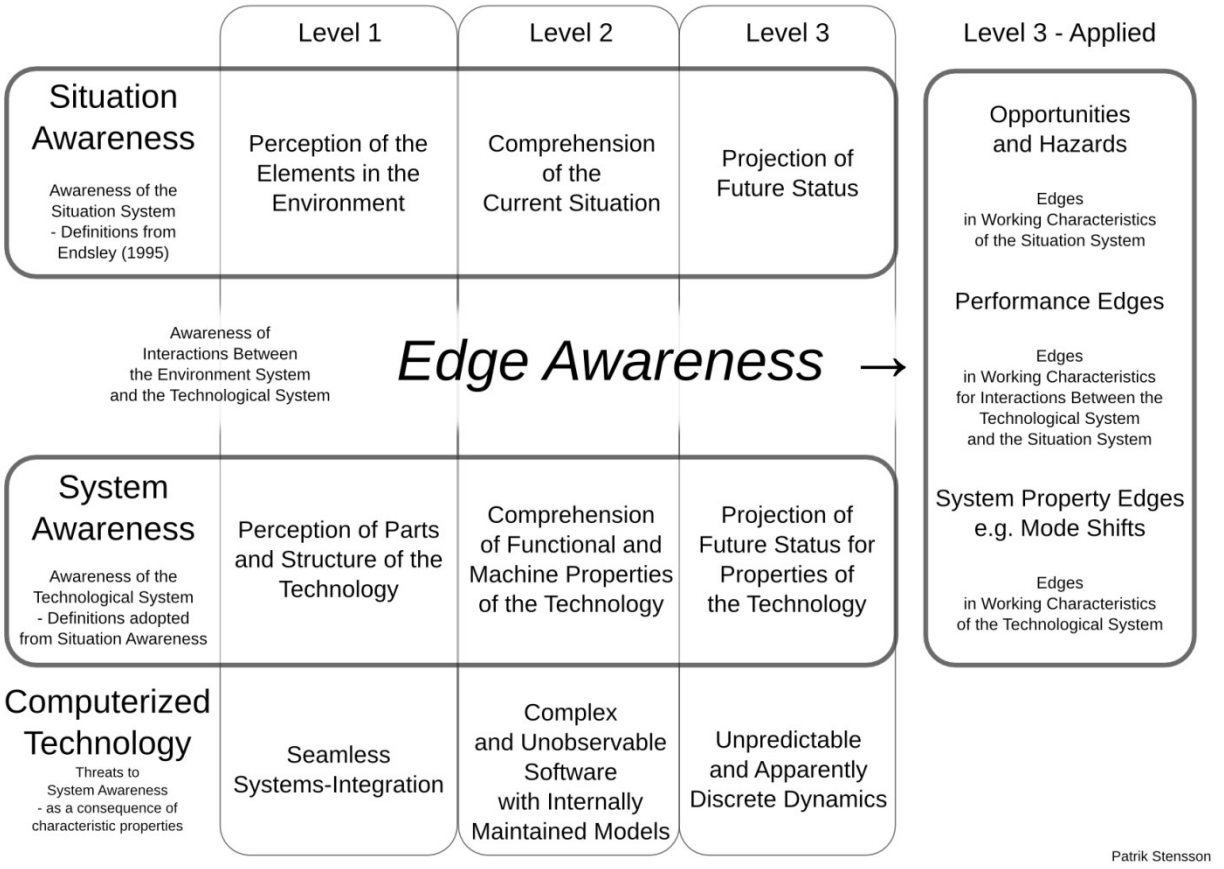

Figure 1 The relation between Edge Awareness and Situation/System Awareness.

Modern interpretations of SA as well as straightforward interpretations of SysA are, apparently, more about conditions for knowing what goes on– i.e., detached facts concerning what goes on – than about what goes on! Therefore, EA mainly concerning emergent dynamic aspects of a physical situation as a whole, is believed to better capture the original meaning of SA, it concerns knowledge about what actually is going on, dynamically and situated within the actual situation at hand. When effects are evaluated and values are defined from a detached perspective (e.g. before-the-fact), the richness and meanings of the involved perspective is lost (Dreyfus and Dreyfus 1988). Detached findings might be specific and rigorous, thereby appearing thoroughly convincing, but still have no meaning because they lack real-life relevance (Boulding 1956, Davenport and Markus 1999), a situation leading to ethical dilemmas when designing and implementing persuasive technologies (Fogg 2003, chap. 9).

Below, we make use of the framework and the concept of edge awareness presented above. Four cases, two from aviation and two from the nuclear power industry are analyzed in order to see whether the framework contributes with new insights compared to SA, and to the conclusions in the investigation reports. In all the studied cases, it is evident that performance edges were crossed with loss of control as a consequence. For understanding the role of the crew/team, the interesting questions remaining are:

- Did the crew/team see the performance edge coming?
- Did they have situated controllability, that is, did they have means to intervene?

Method

Four cases of two different kinds were studied with the purpose to explore the usefulness of the framework and answer the two questions. The cases are: two airliner incidents, one incident from the past (1991) that actually ended quite happily, and one present case (2009) that was fatal, and, two nuclear power plant incidents, one from the Computing, Software, and Systems Engineering (2018)

past (2006) that as a matter of fact also went by without any significant consequences, and one present (2011) that became a disaster still going on. The idea with this methodological approach is that aspects identified as relevant for explaining the role of the crew/team in relation to the level of automation can be compared between types of technology and between time frames. As such the structure becomes a kind of cross-case display with simultaneously case-ordered and time-ordered cases (Miles and Huberman 1994, pp. 187, 200). The investigation reports were studied and recapitulated, split into one description of the event and one description of the analysis made by the official report. This effort implied both data reduction and data display.

The four cases are all studied by reference of incident investigation reports, produced by independent and formally appointed investigation authorities. The SAS crash in Gottröra was investigated by the Swedish Board of Accident Investigations, the Air France crash was scrutinized by the French Bureau d'Enquètes et d'Analyses pour la sécurité de l'aviation civile, and Fukushima was investigated by The National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission. These organizations are by virtue of their official status considered trustworthy sources and their reports the most reliable information available about the studied cases. The exception to this rule of assumed trustworthiness is the Forsmark incident that was not considered severe enough to merit an independent accident investigation. The incident was instead investigated by the analysis group at the Swedish Nuclear Training and Security Center, self-proclaimed as being independent, but still part of an organization jointly owned by the Swedish nuclear power plant operators. As a consequence, the information available as of their brief reports is considered, possibly, slightly biased, which also is discussed in the presentation and analysis of the case.

SAS, SK 751, 1991

Friday morning at 08:51 local time on the 27th of December 1991, SAS flight SK 751 from Arlanda just north of Stockholm, bound for Copenhagen, lost both its engines and crashed outside the small village of Gottröra only four minutes and five seconds after takeoff. Miraculously, not a single one of the 129 people on board was killed in the crash, although some were injured for life and others suffer still today from post-traumatic stress. Nevertheless, since this was just after Christmas, this accident, which easily could have become a tragic disaster, is sometimes referred to as The Christmas Miracle in Gottröra.

Takeoff proceeded normally until rotation, which is where the aircraft has gained enough speed to lift its nose and take off, when a slight rumble was noticed, followed by an unidentified sound registered by the Cockpit Voice Recorder (CVR) as a weak humming. The de-icing had evidently not been satisfactory performed, and when the wings were slightly bent the stiff clear ice cracked and chunks of it flew off. Some of these loose pieces of ice got sucked into the engines located straight behind the wing roots. The crew noticed the first engine malfunction alright, the co-pilot also identified it correctly as compressor stall. They deduced from the instruments that it was the right engine, although the captain said later that he had problems reading the digital displays due to vibrations and quickly changing values. The captain reduced the right throttle slightly, however, not enough to stop the engine from pumping. The co-pilot said afterwards that it was not until both engines were out that he noticed the warnings on the engine instrument panel and that the exhaust temperatures were much too high.

Accident investigation findings

The report concludes that the accident was caused by insufficient instructions and procedures within SAS for ensuring that clear ice is removed from the wings before takeoff, in spite this being a well-known hazard. Thereby the aircraft came to take off with clear ice on the wings, ice that during rotation flew off and was sucked into the engines. The ice damaged the compressor stages of the engines, which resulted in compressor stall and pumping, enough severe to destroy both engines. The report states as contributing factors, insufficient training of pilots to identify and handle compressor stall and pumping, and, the Automatic Thrust Restoration (ATR) system, which, without pilot awareness, slowly increased the throttle settings and made the pumping worse.

Interpretations according to the framework

While the main cause of the accident was organizational according to the investigation report, the present analysis is not content with the argument that this accident would not have happened if regulations and procedures actually had

been followed. Focus for this analysis is on the fact that there were automated technologies that made the hazardous situation significantly worse and considers the situation as an emergency that might have occurred anyway. Jet engines can in fact get ice, or other foreign objects, into their inlets and have their compressor fan blades damaged, regardless the amount of precautions. Certain unfavorable environmental conditions may befall, or there may be other causes for a system breakdown. Let them be low-probability events, yet for them to occur is not impossible. Whatever the reason why such a hazardous situation might occur, it will be of crucial importance to have the ability to control the malfunctioning technological system (i.e., the engines) in a non-routinely but still insightful manner. What if there had been birds damaging the compressors instead of ice? Like for the astonishingly similar accident, accordingly nick-named The Miracle on the Hudson (National Transportation Safety Board 2010), where US Airways Flight 1549 on January 15th 2009 took off from La Guardia Airport in New York city, got some birds (allegedly several large birds) in the engines and made an emergency landing on the Hudson River completely without casualties. Can the presence of birds be blamed on flaws in organizational procedures? Probably not! Therefore a more constructive approach must be to consider the emergency with malfunctioning engines merely initiated by the presence of ice, and to consider the crash as caused by something else. Plausibly, the plane crashed because both engines were destroyed, which perhaps could have been avoided. From the report:

> Nothing indicates that the engines had any other damages when the pumping started besides the limited damages induced [by ice from the wings] when the aircraft took off. These damages were not more severe than that the pumping in the right engine probably would have stopped if the thrust setting had been reduced sufficiently much. Pumping would probably not have occurred in the left engine at all, if the initial thrust setting had been kept during climb. With a sufficiently reduced thrust setting for the right engine and a maintained thrust setting for the left engine, the engines would probably not have been destroyed. The aircraft should then have been able to return [to Arlanda] for landing (SHK 1993, pp.74-75, authors' translation, brackets added).

If that is true, that the engines could have been saved by an appropriate handling of the thrust settings (the throttles) and thereby allowed the aircraft to return safely for landing at the airport. Then this must obviously mean, contrary to what the report itself states, that the accident in fact was not caused by the presence of ice, but by whatever made the engines brake down after they were damaged. The interesting question therefore becomes, why were the pilots unable to keep the engines running? The answer is arguably (in part) also there in the report, but listed among contributing factors. Table 1 below summarizes the analysis of the SK 751-accident as well as the other three cases.

The report lists two contributing factors to the accident (SHK 1993, p. 86). The first is that the pilots were insufficiently trained to identify and remedy compressor stall and pumping. The second is the ATR system, at the time unknown to SAS, which became activated and increased the throttles without the pilots being aware of it. Both these issues are about controlling the specific aircraft subsystem consisting of the two jet engines.

So, why did the pilots not stop the pumping that destroyed the engines? One plausible explanation is that they were not sufficiently aware of neither the fact that the engines actually were pumping, nor the severity of the situation. The pilots were for evaluation of the situation confined to actively consult instruments only capable of conveying feedback explicitly designed to convey, which usually concerns only information relevant for normal operation. In addition, the fact that airliners normally operate within safe limits and thus constitute a low-risk environment might eventually create a false sense of security. Combined with a lack of training for identifying and counteracting compressor stall and pumping, this might imply a contextual and emotional distance as well. The appearance of the situation to the pilots, endorsed by a lack of up-to-date skills to handle such situations together with a lack of experience to identify and have confidence in the ability to handle such situation, did not trigger the will to actively make use of available controls to control the system until it stopped pumping. In addition, there was this ATR system, adding to the difficulties for the pilots. The ATR is an example where at least two of three characteristic properties of computerized technological systems imply undesired consequences (Stensson & Jansson in press).

The edge awareness chart can be used to summarize all this. The pilots kept (with help from the assisting pilot!) sufficient situation awareness throughout the event. However, they did not have sufficient system awareness as the function of the ATR was unknown to them. What seems to be overlooked is the generative consequence of the combination of moderate situation awareness and insufficient system awareness. This made the pilots also lack sufficient edge awareness. They evidently fell over the operational edge for the engines resulting in a complete breakdown of both. Apparently they did not see the performance edge coming. They slipped, so to speak, on the ice that flew off the wings, ended up closer to the edge than before without realizing this. Because of the ATR they did

not have appropriate awareness about the performance relation between throttle settings and engine workings, resulting in several damaged compressor fan blades. Lack of engine performance edge awareness made them unable to get away from the edge. This is arguably what caused the accident that was triggered by the presence of ice.

Table 1 Summary of results from analyses of the four cases

Awareness Types	The Four Cases			
	SK751	**Forsmark**	**AF447**	**Fukushima**
SA Level 1	Yes	Yes	Yes	Yes
SA Level 2	Yes	Yes	No	Yes
SA Level 3	Yes	No	No	No
SA – Summarized	They kept (with help from the assisting pilot) their awareness about the situation throughout the event	They noticed the loss of external power and understood its consequences, but could not anticipate – caused by an external mistake	They noticed that the situation was unfavorable, but they were, at least not until it was too late, aware of that they were stalling	They new about tsunamis and about the possible impact on the power plant, but ignored the situation because the risk was judged insignificant
SysA Level 1	Not really	Yes	Yes	Yes
SysA Level 2	No	No	No	Yes?
SysA Level 3	No	No	No	Perhaps?
SysA – Summarized:	They did not understand the engine regulator sub-system and were therefore not aware of the slowly increasing thrust settings	They knew about the UPS units, but did not comprehend how they really worked and could therefore not anticipate the failure to connect	They knew about the flight-control automation systems, but they did not understand system limits and could not anticipate mode-shifts	System awareness is largely irrelevant for this case as it was overwhelming situational aspects that led to loss of control
EA – Did they see the performance edge coming?	No, the engines started pumping and there was no (sufficient) control input to stop it	No, the UPS automation failed silently	No, not the stall edge, nor the flight-control mode-shifts	No, they worked under the assumption that it would not happen
EA – Did they have situated controllability?	Yes, the automation could be overridden by simply shifting the thrust levers by force	Not intentionally, but there were additional means of manual control that were utilized	Yes, in principal, the aircraft was in manual mode but the pilots were not trained to use it	No, required means for control under such conditions did not exist
EA – Summarized: **Action Regulation, based on SA+SysA+EA**	Out of the loop, they were unaware of the existence of the thrust regulation automation, thereby never really within the engine thrust control loop	Out of the loop initially, but later they regained control	Out of the loop, by being content with the idea that the aircraft could not stall the pilots willingly remained out of the loop – unable to gain control	Initially in the loop, until the situation escalated beyond control
Conclusions	Human contribution in airframe maneuvering (and luck) saved the situation. However, better EA for engine performance would	Human contribution and sufficient controllability when finally realizing (from long time experience of working at the plant) the	False safety depending on calculative models. An exaggerated belief in automated control implied inadequate practical means for	False safety depending on calculative models. The kind of situation that in fact occurred was considered ignorable

	probably have allowed for a normal landing with reduced engine power	necessity to switch in the power generators manually saved the situation.	situated control (inappropriate system design and training)	

FORSMARK, 2006

The incident began at 13:20 on the 25th of July 2006, when the Swedish national grid (SVK), the state-owned electricity distribution organization, was about to do some work at the 400kV switchyard outside the Forsmark nuclear power station. Forsmark power station consists of three boiling water reactors (BWR), where reactor F1 and F2 are connected to the switchyard in question, while reactor F3 is connected to a different one. F2 was shut down for maintenance, while F1 was in full operation. In the switchyard to which the running F1 was connected, a high-voltage dis-connector was opened such that an arc appeared. This caused a two-phase short-circuit that in turn created severe fluctuations in voltage within the power station.

It is crucial for a nuclear power station to have access to electrical power, as it is required for maintaining control of the heat producing nuclear reaction process. Thus, ironically for an electrical power plant, it is availability of electrical power that constitutes its weak spot. The power station at Forsmark have several sources of electrical power to guard this weakness, one external 400kV power grid, one external 70kV power grid, and in-house electrical power production. Furthermore, there are four independent internal power distribution subsystems, called subs, labeled A-D, where each one is fitted with a battery secured Uninterruptible Power Supply (UPS) system, designed to provide the station with electrical power for two hours, and one diesel driven generator per sub for prolonged emergency power. The battery system is connected to the sub between a rectifier and an inverter (because, batteries provide direct current and the power grid require alternating current). It is sufficient for two subs to function in order to provide the power station with necessary internal power. Electrical power is required for equipment measuring water level and steam pressure within the reactor, as well as for control room instrumentation. Since not all subs were working and different equipment was connected to the different subs, some control room systems were not working, and the staff had to control the nuclear reactor in partial blindness. When twenty two minutes had passed, there was a successful manual restoration of power from sub A and B diesel generators, resulting in all four subs having power again. The surveillance systems in the control room came back on providing indication of all the rods being in place. Water pumping capacity increased again and normal levels could be maintained. Forty five minutes from the beginning of the event, after extensive checks had been made, the staff was able to note in the log that “The reactor is safely sub-critical and operational status is stable” (KSU 2007, p.4).

Incident report findings

The switchyard short-circuit was apparently caused by a misjudgment by the external power grid organization, about the need to interlock an earth fault protection. Had this been done properly then there had been a much shorter short-circuit and much less fluctuations in voltage. If this had been the case, the disturbances had probably not affected the internal power production of the power station at all. However, the generator circuit breakers for both main generators did not work properly. They should have opened on under-frequency when the generators were stopped, which they did not. In 2005, new under-frequency generator protection systems had been installed. These systems were unknowingly working differently than the replaced ones. The old protector systems were independent of phase sequence in the three-phase grid, and the new ones were not. Lacking knowledge about this made also the testing after the installation fail to identify the error. If the circuit breakers had worked as they were supposed to, then the power supply for switching in the diesel generators would also have worked. The diesel generators were automatically started, all four of them, but only two could be connected to their respective subs. Two of them failed because they required power from non-working UPS:es to establish the connections. The report concludes that this shows two things, the vital function of the UPS:es, and the fact that there were functional relations between the different systems, relations that made it possible for them to fail by a common cause. Regarding the control room the report does not say much. It highlights that the staff successfully carried out emergency procedures according to how similar incidents had been handled during simulator training, and, that despite a confusing situation with failing displays and a lack of information the staff managed to carry out “their work in accordance with their instructions in a particularly effective manner” (KSU 2007, p. 5). The report concludes also that training of operators in simulators

proved valuable and kept control room staff work rational in the stressing situation.

Interpretations according to the framework

The calculative approach to safety is highly evident throughout the analysis, but perhaps especially in the conclusions sections, where the reasoning focuses on measures that will make the power station be safe if similar incidents would occur in the future. It is indicated, for example, by the focus on simulator training. Simulators are great for some purposes. But one of their major flaws is inherent in their very nature. They can only be used in training for predicted events because for valid training the simulators must behave reasonably similar to how the real systems would behave, which is possible only if the event can be analyzed in advance such that relevant system properties can be implemented in the simulator. This very incident was an unpredicted event, as most incidents leading to accidents appear to be. It could not have been trained for in simulators because before the accident the common knowledge was that the UPS:es worked as they should, which means that the simulators would have been programmed such. If the malfunctioning had been predicted, the UPS:es would either have been modified or the staff would have been prepared to do the manual reconnection of the diesels directly when it occurred. This is the core paradox of calculative safety. By focusing on preventing undesired events from ever happening, that is, by considering the establishing of safe-guards for predictable events sufficient, the safety becomes brittle because of an increased unpreparedness for unpredictable events, which in turn makes an unpredictable event more likely to cause a disaster. The report tries also to give the impression that the safety has been increased after the accident because this kind of event has now been implemented in the simulators, while this in reality only means that the safe-guard perhaps has become stronger, but probably also more brittle. It is evident from the investigation report that the team had basic situation awareness, but initially they were unable to anticipate a potentially hazardous situation due to lack of system awareness. This lack of awareness kept the operators out of the loop initially and they did not see the performance edge coming. However, based on experience and knowledge about alternative manual control possibilities, after a while it was possible to regain control of the situation.

AIR FRANCE AF447, 2009

Late Sunday night the 31st of May 2009 the Airbus A330-203 registered as F-GZCP was scheduled to leave Rio de Janeiro Galeão for Paris Charles de Gaulle, and it took off at 22:29 UTC. About three hours later, around 01:35, early on the 1st of June, at FL350 (about 10700 meters), the co-pilot adjusted the level of detail on his navigation display and noted “So we've got a thing straight ahead”. The Cockpit Voice Recorder (CVR) system was running and conversations as well as radio traffic was continuously captured. This “thing” the co-pilot referred to was a bit of bad weather related to the Intertropical Convergence Zone (ITCZ). The Captain confirmed the statement and they discussed the fact that they still had a very heavy aircraft and that the comparatively high temperature inhibited them from climbing to FL370 (about 11300 meters) for an attempt to get above the bad weather. They dimmed the internal lights to be able to see better out through the cockpit windshield and the co-pilot observed that they were entering the cloud layer. Turbulence started shortly after.

At 02h:09m:40s there was a change in the background noise, later identified as the sound of ice-crystals hitting the aircraft. After twenty-five seconds, first the autopilot then the auto-thrust systems disconnected and the pilot-flying (PF) called out “I have the controls”. The aircraft began to roll rather quickly to the right and the PF made a distinct nose-up and left input, followed by two left-right inputs to the stop positions. Supposedly the excessive control inputs came from being surprised by the quick initial right roll combined with an unfamiliarity with and unawareness about the change into alternate flight control law. The roll angle fluctuated between 11° right and 6° left and the pitch attitude increased to 11° in ten seconds. The indicated speed on the left Primary Flight Display (PFD) made a sharp fall from about 275kt to 60kt and shortly later on the Integrated Standby Instrument System (ISIS) as well, and there were two brief stall-warnings. The Flight Director (FD) indications on the PFD disappeared without the crew explicitly disconnecting them, indicating the loss of normal flight control protections.

The two pilots continued struggling with the controls. Just after the PF had concluded “We're there we're there we're passing level one hundred” (10000ft, ~3000m), the pilot-not-flying (PNF) said at 02h:13m:20s, “Wait me I have I have the controls eh”, but he seems to have let go and asked instead “Try to find out what you can do with your controls up there”. The PNF had after all apparently still not fully understood the situation, because when the PF at

02h:13m:36s called out “Nine thousand feet” he responded with “Climb climb climb”. Then the PF said what probably made both the Captain and the PNF realize what was going on. At 02h:13m:41s the PF said “But I've been at maxi nose-up for a while”. The Captain responded “no no no don't climb” and the PNF “so go down”, “So give me the controls the controls to me controls to me”, and the PF acknowledged “Go ahead you have the controls we are still in TOGA eh”, and the Captain continued “(so wait) AP OFF” meaning to shut off any remaining autopilot involvement. However, it was already too late. The PNF side-stick was positioned nose-down for 15 consecutive seconds, supposedly in a futile attempt to make a stall recovery maneuver, although the DUAL INPUT parameter in the FDR was activated five times. Then the ground collision warning system triggered with a voice repeating “pull up”, “pull up”. At 02h:14m:21s the PF takes control priority and says “(!) we're going to crash”, “This can't be true”, and finally he uttered a last expression of confusion, “But what's happening”. The PNF side-stick is positioned nose-down, the PF nose-up to the stop. Then the recording stopped, at 02h:14m:28s.

Accident investigation findings

Just as for the SAS SK751 incident, this accident was triggered by the presence of ice, in a situation where ice was known to exist and for which there were procedures and regulations in effect. While the ice in the SK751 case actually damaged the aircraft in a way that led to the destruction of both engines, the ice-crystals hitting AF447 caused nothing but a temporary loss of airspeed, which would have been completely insignificant and harmless for the aircraft if not the situation had evolved as it did. This means that the crucial question is why this, in some sense trivial malfunction evolved into a fully developed stall right into the ocean. The report begins with the fact that the crew became completely surprised by what happened and that they seem never have understood fully the situation they ended up in. For this confusion there may have been several reasons. To begin with, when cruising at high altitudes on long-haul flights the main concern for the crew is usually to avoid turbulence, for comfort reasons (BEA, 2012, p. 168). This task involves selection of alternative flight paths and flight levels weighted against extra fuel consumption and prolonged flight time and it is performed on a rather high level of abstraction mainly by adjusting autopilot settings. The step to begin existential maneuvering of the aircraft by use of direct control input to keep it flying is thereby quite long, thus requiring significant insight for actually taking the step mentally. The problems associated with identifying the situation correctly is thus the main focus of the report.

The crucial moment of the event was the exit of the flight envelope, up until which appropriate control input probably would have regained safe flight rather quickly. This exit happened around the time when the aircraft peaked in altitude at about 38000ft (~11600m). After exiting the flight envelope only very deliberate and consistent control input from a resourceful crew could have saved the situation. Because, the only way out from the fully developed stall would have been to reduce the angle of attack significantly and gain speed by making the aircraft enter into a steep dive. For everyone not familiar with advanced aircraft handling and aerobatics (for which an airliner is not built) this would perhaps appear as worsening the situation, yet it is what had to be done for any chance of getting back within the flight envelope. However, this maneuver would obviously require quite a nerve and a total insight by the crew of being in stall, together with sufficient altitude, which they actually had, although not for long. Hence, the fundamental problem seems to have been a lack of situation insight. The report concludes that the accident was caused by a series of events, beginning with the obstruction of the pitot probes by ice crystals. This obstruction caused a total loss of airspeed and the autopilot to disconnect, and a reconfiguration of flight mode to alternate law. The crew failed to link the loss of airspeed to appropriate procedures and to identify in time the deviation from the flight path and the approach to stall (i.e., they failed to comprehend the effects of next statement). Inappropriate control inputs made the aircraft exit its flight envelope and enter into a fully developed stall, which continued until even such inputs that could have made it possible to recover into safe flight were too late.

Interpretations according to the framework

The conclusion of the report focuses on finding a causal chain of events beginning with the ice obstructing the pitot tubes followed by automation degradation. It is a conclusion focusing on concrete actions and courses of events, while forgetting to consider what caused the conditions to be what they were. This focus is arguably a too narrow perspective implicitly demanding responsibility from people not given proper means to shoulder those demands. The report provides explanations that touch upon other matters. For example, the identification of a culture that made it impossible for people involved to address the implications of technological insufficiencies, such as the consequences of a total loss of air speed, by use of further technological solutions. This culture is also present in the conclusion that pilot training in basic aircraft handling (at high altitudes) and stall recovery was insufficient. However, it is possible to view the matter from another position. The explanations, and especially the calculative culture, had

created technological conditions in the form of system designs that made the situation evolve as it did, which thus must be concluded as the cause of the accident. The series of events stated as the cause is here argued better considered an explanation of how the accident evolved. The calculative culture identified within the airline operations community seems unfortunately to extend to and also prevail in the airliner constructors community, resulting in aircraft designs with such abstracted control that it effectively inhibits the pilots to do what they are supposed to do, namely to fly the plane. It is possible to state that the approach during aircraft design and the resulting character of controllability led to insufficient system awareness, indicated by surprise, confusion, and excessive control inputs. The aircraft design led also to insufficient situation awareness, indicated by the failure to identify the stall and apply appropriate control input for recovery. Consequently, the aircraft design led also to insufficient edge awareness, proved by the fact that they fell over the stall edge and exited the flight envelope. The vicious circle culture (Stensson & Jansson in press), considering predictable behavior sufficient enough to be enforced by abstracted control models, had made the pilots adopt too much the role of being automation supervisors, at the expense of skilled system handling on the more fundamental level of aircraft aerodynamics.

FUKUSHIMA, 2011

On March the 11th 2011 at 14:46 the Great Eastern Earthquake occurred, immediately triggering the emergency shutdown feature on unit 1, 2, and 3 of the Fukushima Daiichi Nuclear Power Plant. Units 4 to 6 were already shut down due to periodical inspections. However, the seismic tremors had damaged the electric transmission to the power plant, with a total loss of off-site electricity as the result. Also the secondary back-up line was unusable due to mismatched sockets. The tsunami that followed from the earthquake had its peak at 15:37. It destroyed the emergency diesel generators, the seawater cooling pumps, electrical wiring, and the DC power supply for units 1, 2, and 4. There was no electrical power available, except from an air-cooled emergency diesel generator at unit 6. Unit 3 had initially some DC power that ended before dawn of March the 13th. On March the 13th at 02:42 all means of water injection was lost at unit 3. At 04:15 the core started to be uncovered and, presumably, a massive amount of hydrogen developed. Workers dodged the extreme heat and went to vent the reactor, a considerable challenge that actually succeeded. Batteries were successfully connected to the safety-release (SR) valves allowing the pressure to lower enough to resume water injection. However, the unit ran out of water at 12:20. At unit 2 the operators started to prepare for a depressurization to allow for water injection by fire trucks because they estimated problems.

On March the 14th unit 3 boiled dry and at 04:30 the core had become completely uncovered. Fire trucks were preparing to assist with water injection when the building exploded at 11:01. Seven workers were injured, wreckage was thrown hundreds of meters high, and falling debris ripped a huge hole in the turbine building roof. Seawater injection could not be resumed until after more than five hours. The explosion interrupted once again the work at unit 2. Hoses and fire trucks were damaged and the workers had to start from scratch again. At 13:25 it was estimated that the reactor core at unit 2 would start to be uncovered by 16:30. Repeated aftershocks made the work be suspended until 16:00, and by 18:22 the core became fully uncovered. The fire trucks ran out of gas and the reactor continued to boil dry. More SR valves were opened facilitating more low pressure injection of water that succeeded in keeping some water level in the reactor, but not in covering it. At 06:00 on March the 15th the reactor building of unit 4 exploded and a large noise was heard inside the torus room of unit 2, supposedly indicating a leak. Workers were removed and the monitoring of unit 2 stopped.

Accident investigation findings

> The Commission recognizes that the fundamental cause of the Fukushima nuclear accident originated from “the collapse of nuclear safety monitoring and supervising functions stemming from the reversal of the relationship between the regulators and regulated” among the successive regulatory authorities and TEPCO. Considering that there had been many opportunities for both sides to undertake safety measures beforehand, we regard that this accident was not a “natural disaster” but clearly “man-made.” (introduction to: NAIIC 2012, p. 12).

The accident investigation commission states that the root causes of the Fukushima disaster were the organizational and regulatory systems that supported faulty rationales for decisions and actions. Because, the regulating authorities and TEPCO were since 2006 well aware of the risk for a total loss of electrical power if a tsunami would reach high enough, and the Nuclear and Industrial Safety Agency (NISA) was aware of that TEPCO had not taken any measures to remedy this risk. NISA had in spite of this knowledge refrained from issuing specific instructions to

meet these threats to public safety. In fact, the investigation commission found evidence that the relationship between the operators (TEPCO) and the regulators, in this case NISA and the Nuclear Safety Commission of Japan (NSC), was reversed . The regulating authorities regularly asked explicitly for the operators intentions when new regulations were to be implemented. As an explicit example the report states that NSC informed the operators that the possibility for a station blackout (SBO), meaning a complete loss of electrical power, which precisely was what happened on the 11th of March 2011, was negligible and therefore possible to disregard. NSC then asked the operators for a report providing the rationale why the risk for SBO could be considered negligible. In addition there was a negative attitude towards importing overseas advances in knowledge and technologies, which is one reason why the commission chose to label this disaster as "Made in Japan".

Interpretations according to the framework

The Fukushima Daiichi Nuclear Power Plant operated by Tokyo Electric Power Company (TEPCO) was severely damaged by the Great Eastern Earthquake and the following tsunami. These natural disasters triggered a man-made nuclear accident that is still happening, because, consequences are not restored and people are still suffering from exposure of radiation. The accident was man-made because it could and should have been foreseen and prevented. In fact, it was principally foreseen, but identified necessary measures were either ignored or postponed, and apparently this was mainly because of the Japanese management culture. Kiyoshi Kurokawa, the chairman of the National Independent Investigation Commission (NAIIC), put forth in the beginning of the report that:

> What must be admitted – very painfully – is that this was a disaster "Made in Japan." Its fundamental causes are to be found in the ingrained conventions of Japanese culture: our reflexive obedience; our reluctance to question authority; our devotion to 'sticking with the program'; our groupism; and our insularity. (executive summary of: NAIIC 2012, p. 9)

It seems as that the severity of consequences associated with losing control of nuclear power plants is of such magnitude that this must never happen. It is treated as inconceivable and practically impossible, yet it happened three times (Harrisburg, Chernobyl, and Fukushima). The important criteria for judging the entitlement for existence of nuclear reactors then becomes that the possibility for anything unpredictable to happen that might lead to a loss of control is negligible. This is where the question of responsibility returns. It seems that neither operators nor the regulating authorities are especially keen on taking the responsibility for the vast consequences of losing control of their nuclear power plants, and the only way to justify their own existence becomes therefore to make sure that the possibility for this to happen is negligible and that the residual risk can be blamed on the inherently unpredictable thus being the responsibility of someone or something else. As a consequence of the above, it appears as that in the nuclear power production business there is a high readiness for things to go wrong, but only for things that go wrong in known ways and extents. The safety management model becomes thereby to prepare for known events until the unknown appears righteously possible to consider as negligible.

CONCLUSIONS

By filtering the investigation reports through the new framework, this study has shown that calculative models and insufficient system awareness sometimes make it difficult or impossible for teams/crews to realize the performance edges coming. In some cases, they also seem to suffer from insufficient situated controllability, that is, they lack means to intervene. While crews/teams may have good situation awareness, automation tend, often ironically (Bainbridge 1983), to imply bad system awareness. Without appropriate system awareness, situated system-environment interaction characteristics cannot be sufficiently comprehended and bad (performance-) edge awareness becomes a consequence, and situation awareness of lower significance. Aiming for design of technological systems with situated controllability implies a quest for edge awareness. We therefore propose edge awareness to be the candidate mental state to be used as a lodestar in design of resilient systems and to avoid future systems disasters. Edge awareness is the basis for responsible and autonomous decisions.

REFERENCES

Bainbridge, L. (1983). Ironies of automation. *Automatica*, *19*(6), 775–779. doi:10.1016/0005-1098(83)90046-8

BEA, Bureau d'Enquètes et d'Analyses pour la sécurité de l'aviation civile. (2012). *Final Report, 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.* Retrieved from http://www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf

Bhaskar, R. (2008). *A realist theory of science* (New ed.). London: Verso.

Boulding, K. E. (1956). General Systems Theory - The Skeleton of Science. *Management Science*, *2*(3), 197–208.

Brehmer, B. (1992). Dynamic decision making: Human control of complex systems. *Acta Psychologica*, *81*, 211-241.

Collier, A. (1994*). Critical Realism, An Introduction to Roy Bhaskar's Philosophy.* London: Verso.

Davenport, T. H., & Markus, M. L. (1999). Rigor Vs. Relevance Revisited: Response to Benbasat and Zmud. *MIS Quarterly*, *23*(1), 19–23.

Dreyfus, H. L., & Dreyfus, S. E. (1988*). Mind Over Machine* (Reprint.). New York: Free Press.

Emmeche, C., Køppe, S., & Stjernfelt, F. (1997). Explaining Emergence: Towards an Ontology of Levels. *Journal for General Philosophy of Science / Zeitschrift Für Allgemeine Wissenschaftstheorie*, *28*(1), 83–119. doi:10.2307/25171082

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, *37*(1), 32–64.

Endsley, M. R., & Kaber, D. B. (1999). Level of automation effects on performance, situation awareness and workload in a dynamic control task. *Ergonomics*, *42*(3), 462–492. doi:10.1080/001401399185595

Endsley, M. R., & Kiris, E. O. (1995). The Out-of-the-Loop Performance Problem and Level of Control in Automation. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(2), 381–394. doi:10.1518/001872095779064555

Fogg, B. J. (2003). *Persuasive computing: technologies designed to change attitudes and behaviors.* San Francisco, Calif.; Oxford: Morgan Kaufmann ; Elsevier Science.

Fracker, M. L. (1991). Measures of Situation Awareness: Review and Future Directions (Final Report January 1990-January 1991 No. AL-TR-1991-0128). Wright-Patterson AFB, OH: Human Engineering Division, Armstrong Laboratory

Goldstein, J. (1999). Emergence as a Construct: History and Issues. *Emergence*, *1*(1), 49–72.

Kaber, D. B., & Endsley, M. R. (1997). Out-of-the-loop performance problems and the use of intermediate levels of automation for improved control system functioning and safety. *Process Safety Progress*, *16*(3), 126–131. doi:10.1002/prs.680160304

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, *58*(9), 697–720. doi:10.1037/0003-066X.58.9.697

Kahneman, D. (2011). *Thinking, Fast and Slow* (Reprint.). New York: Farrar, Straus and Giroux.

Kant. I. (1785). *Fundamental principles of the metaphysic of morals* [e-text]. Retrieved May 6, 2013, from http://www.gutenberg.org/etext/5682

KSU. (2007, February). The Forsmark incident 25th July 2006. Bakgrund, 20(1). Retrieved from http://www.analys.se/publicerBakgrund.htm

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). SAGE Publications, Inc.

NAIIC. (2012). *The official report of The Fukushima Nuclear Accident Independent Investigation Commission*. The National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission. Retrieved from http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/

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* (No. Aircraft Accident Report NTSB/AAR-10 /03). Washington DC.

SHK, Swedish Board of Accident Investigations. (1993). *Luftfartshändelse den 27 december 1991 i Gottröra, AB län* (No. C 1993:57).

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, *23*(05), 645–665.

Stanton, N. A., Stewart, R., Harris, D., Houghton, R. J., Baber, C., McMaster, R. Green, D. (2006). Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. *Ergonomics*, *49*(12-13), 1288–1311. doi:10.1080/00140130600612762

Stensson, P. (2014). *Edge awareness: Lessons not yet learned, PhD thesis on practical and situated usefulness of advanced technological systems among inescapable uncertainties and competing interests in the real world.* Unpublished manuscript, Uppsala university, Sweden

Stensson, P., & Jansson, A. (in press). Autonomous technology – sources of confusion: a model for explanation and prediction of conceptual shifts. *Ergonomics*,. doi:10.1080/00140139.2013.858777