Is Smartness Risky? A Framework to Evaluate Smartness in Cyber-Physical Systems

Chronopoulos, Christos; Carreras Guzman, Nelson Humberto

Published in:
Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

Is Smartness Risky? A Framework to Evaluate Smartness in Cyber-Physical Systems

Christos Chronopoulos

Department of Technology, Management and Economics, Technical University of Denmark (DTU).
E-mail: christos.chronopoulos@gmail.com

Nelson Humberto Carreras Guzman

Department of Technology, Management and Economics, Technical University of Denmark (DTU),
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU)
E-mail: nelca@dtu.dk

New technologies have become a significant part of peoples' everyday lives. Smart systems that integrate information and communication technologies (ICTs) and ubiquitous computing interact with humans and the physical environment, providing in return some utility. Many of those systems can be classified as cyber-physical systems (CPSs), from smart objects and autonomous vehicles to smart cities and industrial applications, transportation systems and healthcare. These new technologies come with new vulnerabilities and risks that are not fully studied yet, exposing the safety and security of smart systems. Moreover, the increasing complexity that comes together with smartness hinders the identification of the crucial features that characterize smartness and how they affect the systems' attributes relevant for risk. Therefore, we propose a framework of smartness in CPSs with four dimensions, namely i) degree of integration, ii) real-time feedback control, iii) level of automation and iv) degree of cooperative control. Moreover, this paper illustrates a case study of the recent aviation accidents of Boeing 737 MAX, related to the erroneous operation of an autonomous flight control system. We analyze the accidents' reported root causes with regard to our framework of smartness and, subsequently, we identify the interactions within the smart system that remained undetected during the risk analyses.

Keywords: Smartness, cyber-physical systems (CPSs), risk, framework, aviation, accidents.

1. Introduction

Nowadays, applications of new technologies are ubiquitous and affect all aspects of peoples everyday lives by increasing the smartness of systems to provide useful and intelligent functions. Smart buildings can monitor the indoor climate conditions and other variables to increase comfort and safety while minimizing the energy consumption (Arditi et al. 2015). In industrial systems, production processes are integrated with information and communication technologies (ICTs) towards fully autonomous systems that are able to gather production data in order to predict future conditions and adapt to them in real-time (Sabella 2018). The transportation sector has also been evolved rapidly. On one hand, in the automotive industry, numerous companies are developing fully- and semi-autonomous vehicles with advanced systems (e.g. lane-following, collision warning, navigation) to augment and aid the drivers, and eventually achieve driving with no human intervention (Endsley 2017). On the other hand, in the aviation industry, the degree of automation has been higher compared to vehicles for at least two decades. In the 1970s, Boeing started to develop the flight management computer (FMC) by combining the performance management computer and navigation computer into a single unit. The FMC was capable of automatic navigation and real-time performance predictions based on data inputs from several systems of the aircraft (Miller 2009).

However, these new technologies increase the complexity of smart systems and create new vulnerabilities and risks, which are greater than the accumulated risks of the individual components (Axelrod 2013). Marchese and Linkov (2017) posed the question whether a system can be smart and resilient at the same time, despite the attributes' conflicting nature. Several major accidents due to deliberate security attacks or unintentional failures have occurred in the last decade, stressing the significance of dealing with the emerging vulnerabilities and risks. One example, is the Stuxnet malware that targeted the supervisory control and data acquisition systems of nuclear facilities in Iran in 2010, causing substantial damage to the infrastructure (Kushner 2013). Another example is the fatal crash of a Tesla vehicle in 2018 while driving in "autopilot" mode (Levin 2018). Recently, the two fatal aviation accidents in 2018 and 2019, involving the Boeing 737 MAX aircraft, have both been linked to the malfunction of an autonomous flight control system due to erroneous sensor data (Leggett 2019; Boeing 2019c). The systems become increasingly dependent on software "that's all too

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN/DOI: TBA

easy to manipulate" (Travis 2019). The human factor, despite its fundamental role in aircraft systems engineering is often disregarded as potential causal factor in risk identification and hazard assessment (Pickthall 2014).

Our study focuses on the assessment of smartness in CPSs to support and enhance risk identification towards comprehensive safety and security analyses. Section 2 presents in detail our conceptual framework of smartness and provides the definition of CPSs. Section 3 introduces the case study of the recent Boeing 737 MAX accidents and briefly explains the technical aspects of the flight control system that failed. Section 4 discusses the factors that are relevant to this study, that contributed to the aviation accidents as presented in the accident reports, and analyzes them with our framework of smartness dimensions and characteristics. Finally, Section 5 concludes.

2. Smartness conceptual framework

The framework of smartness dimensions and characteristics facilitates the assessment of a system's overall level of smartness in the context of CPSs. This can further support the identification of the links between smartness and robustness, towards balancing those two attributes. Furthermore, it can enhance the safety and security risk analyses, especially in safety-critical CPSs. In this section, we describe what we conceive as CPSs and illustrate the conceptual framework of smartness, its dimensions and characteristics.

2.1 *Cyber-Physical Systems (CPSs)*

The U.S. National Institute of Standards and Technology (NIST) describes CPSs as smart systems consisting of engineered interacting networks of physical and computational components (NIST 2017). Similarly, in Alur (2015) interconnected computing devices interact with the physical world through sensors and actuators in a feedback loop.

Our framework is based upon the definition of CPSs proposed by Carreras Guzman et al. (2019), that is, engineered systems which integrate information technologies, real-time control subsystems, physical components and human operators to influence physical processes by means of cooperative and (semi)automated control functions. This definition encompasses the key features of CPSs, which provided the "guidelines" in our search of smartness dimensions and characteristics. That is (i) the real-time feedback control of physical processes through sensors and actuators, (ii) the cooperative control among networked subsystems and, (iii) a threshold of automation level where computers close the feedback control loops.

2.2 *Framework of smartness in CPSs*

The proposed framework of smartness dimensions and characteristics was developed using the aforementioned definition. In that sense, we defined four dimensions of smartness:

(i) Degree of integration
(ii) Real-time feedback control
(iii) Level of automation
(iv) Degree of cooperative control

Those four dimensions were further divided in groups of characteristics, which have been identified through a comprehensive literature review of the term "smartness" in the two major digital scientific libraries, namely Scopus and Web of Science (Chronopoulos et al., n.d.). In that previous study, we identified and analyzed several definitions of smart systems. Additionally, we extracted a set of 52 attributes of smartness described implicitly or explicitly in the reviewed literature. The identified attributes were further classified in groups of characteristics under the four dimensions of smartness. Fig. 1 illustrates our framework of smartness dimensions and groups of characteristics. The individual characteristics within the three subgroups of the level of automation are depicted in Table 1, whereas a detailed description of each individual characteristic within all four dimensions of our smartness conceptual framework can be found online at the online resource "Dimensions and Characteristics of Smartness in Cyber-Physical Systems — DTU Research Database" (2019).

Table 1. Level of automation dimension, groups and characteristics of smartness (adapted from Chronopoulos et al., n.d.)

Level of automation	Characteristics
Information acquisition and analysis	Information collection
	Information processing and interpretation
	Knowledge creation
	Self-learning
	Self-awareness
	Sensing and Context-awareness
Decision and action selection	Reasoning
	Anticipation
	Decision-making
Action implementation	Actuating
	Self-regulation
	Adaptability
	Personalization
	Self-configuration
	Self-protection

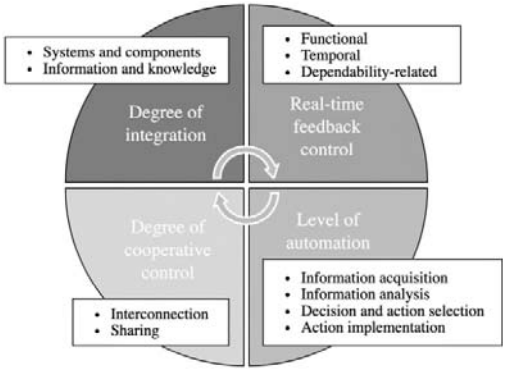

Fig. 1. The four dimensions of smartness in CPSs and the respective groups of characteristics in boxes (Chronopoulos et al., n.d.).

3. Case study: Boeing 737-8 (MAX)

The aviation industry has been a pioneer in advanced control systems. Information and communication technologies are integrated with aircraft control systems increasing the level of automation in flight operations. Yet, the technology is not mature enough for full automation and hence, it is still the pilots who have complete authority over the aircraft's function. Boeing is determined that "the pilots will continue to always have the ability to override (the autonomous systems) and manually control the airplane" (Boeing 2019a).

As long as humans are involved in the loop, the manufacturers have to implement human-centered design principles in their processes. Murman and Allen (2003) stress the significance of assessing the complex interrelationships between the aircraft technical components and humans throughout their entire lifecycle in aircraft systems engineering. The Avionics Handbook describes two human-centered flight deck design objectives with regard to automation. First, the automation must act predictably in a way that is well understood by the flight crew. Second, that its function must directly support flight crew in performing their tasks. If the automation fails to meet those two objectives, this might inhibit the controllability and supervision of the flight control system, potentially leading to confusion of the crew, automation surprizes and unintended aircraft responses (Spitzer 2001).

This was the case for the Lion Air flight LNI610 in 29th of October 2018 and the Ethiopian Airlines flight ET302 in 10th of March 2019, where erroneous data from the Angle of Attack (AOA) sensor of the Boeing 737-8 MAX caused the uncommanded operation of an automatic flight control system, known as Maneuvering Characteristics Augmentation System (MCAS). Unfortunately, a series of failure conditions and contributing factors, led to the crash of both aircrafts with a total of 346 casualties.

3.1 *What is MCAS?*

The MCAS function is an automatic flight control system that moves the horizontal stabilizer up to 2.5 degrees in 10 seconds during manual flight, flaps-up (i.e. retracted), high AOA maneuvers to reduce the pitch up tendency of the aircraft (Boeing 2019a). MCAS function is contained in each of the two Flight Control Computers (FCCs). However, at aircraft power-up the default master FCC is the left, on Captain's side.

The Air Data Inertia Reference Units (ADIRUs) are devices that provide inertial position and track data, as well as attitude, altitude and airspeed data to the FCC. The ADIRUs process data measured by several sensors including the AOA sensors, the pitot probe, and internal gyros and accelerometers (KNKT 2018).

In Boeing 737-8 MAX, the left and right horizontal stabilizers located at the rear of the fuselage provide pitch control (i.e. movement on the lateral axis). The horizontal stabilizers pivot up and down, causing trim of the aircraft to nose down (AND) and nose up (ANU) position respectively. The movement is provided either by a single stabilizer trim motor, or mechanically through cables and pulleys. The flight crew can manually control the motor through either the yoke electric trim switches located on each control column, or the manual stabilizer trim wheel located on each side of the control stand. Additionally, trim can be provided automatically through the autopilot and MCAS function, which actuate the motor accordingly. The stabilizer trim cut-out switches, when positioned to CUTOUT, remove the power from the stabilizer trim motor and therefore, no electric trim can be provided either manually or automatically, while the trim wheels remain functional. An illustration of MCAS including the functional components and the respective data flows is depicted in Fig. 2.

The MCAS software function was added to the 737 MAX to counteract the negative maneuvering stability effects due to the integration of a new engine (i.e. CFM LEAP-1B), with larger fan diameter and engine nacelle. The new engine could provide better fuel efficiency according to the manufacturer, but it required structural aerodynamic changes. For example, the engines had to be positioned higher and forward compared to the previous Boeing 737 models, causing a tendency to stall at higher AOA. Another reason that MCAS was added is "to make the Boeing 737-8 (MAX) handling characteristics so similar to the NG versions that no simulator training was needed for type rating" (KNKT 2018), which is the certification of pilots to fly a certain type of aircraft.

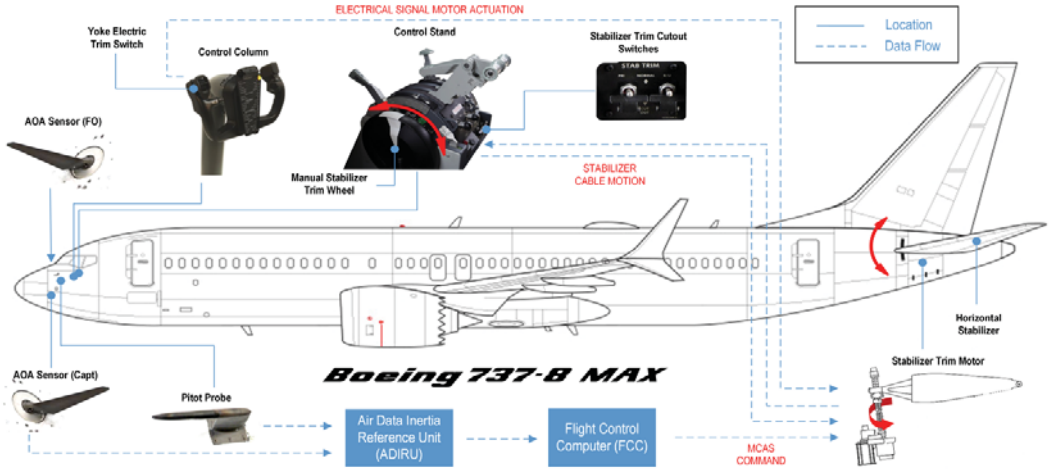

Fig. 2 Representation of the MCAS including the functional components and the respective data flows (authors' own elaboration, adapted from KNKT (2018) and norebbo.com)

3.2. *The accidents*

On October 29, 2018 a Lion Air Boeing 737-8 MAX, scheduled to depart from Jakarta, Indonesia to Depati Amir Airport, crashed in the Java Sea after approximately 11 minutes of flight, causing 189 casualties. The flight crew had reported "flight control problem" to the Air Traffic Controller (ATCo) but did not declare either urgency (i.e. PAN PAN) or emergency (i.e. MAYDAY) conditions. At the same time, the crew was getting several alarms and suffered the uncontrolled operation of the aircraft due to erroneous data from the left AOA sensor that activated MCAS under false conditions (KNKT 2018).

Similarly, on March 10, 2019 an Ethiopian Airlines Boeing 737-8 MAX took off from Addis Ababa Bole International Airport to Nairobi and crashed near Ejere village after approximately 6 minutes of flight, resulting in 157 casualties. The flight crew had experienced the uncommanded operation of MCAS caused by erroneous AOA sensor data and had reported flight control problem to the ATCo (AIB 2019).

3.3 *What went wrong?*

On April 5, 2019 Boeing acknowledged the "erroneous activation of the aircraft's MCAS function" as "common chain link" between the two aviation accidents (Boeing 2019c).

In the Lion Air LHI910 accident report, published by the Indonesian National Transportation Safety Committee (KNKT), 89 findings are documented. The findings indicate not only the causes and deficiencies that led to the accident, but also "the conditions that pre-existed the accident sequence" and contributed to its occurrence. The respective failures and errors can be divided in organizational and design-related ones. The organizational failures include issues with regard to "Incident and Faults Reporting and Documentation", "Flight Crew Training", and "Problems Handling and Maintenance", whereas the design-related include issues of the MCAS software function, "MCAS Functional Hazard Assessment", physical component failures and the human factor.

3.4 *What has been done?*

At the time when we wrote this paper, KNKT had already issued the final report of the Lion Air accident, whereas only a preliminary report for the Ethiopian Airlines accident had been published by the Aircraft Accident Investigation Bureau of Ethiopia (AIB). In the final report of the Lion Air accident, numerous safety actions are described, which were taken by the Airline Operator (i.e. Lion Air) with regard to Operations and Maintenance, as well as by the Boeing Company, the U.S. Federal Aviation Administration (FAA), the U.S. National Transportation Safety Board (NTSB) and the Directorate General of Civil Aviation of India. Additionally, several safety recommendations are proposed by the Investigation team to the aforementioned civil aviation operation and regulatory bodies.

Among the numerous safety actions, it is worth noting that on November 6, 2018, Boeing issued a bulletin in addition to the existing Flight Crew Operations Manual, to inform the airline operators about the AOA sensor failure and the subsequent uncommanded and repetitive AND trim. Additionally, the manufacturer provided operating instructions on how to handle and deactivate the system, without referring to MCAS in that document. Later, on March 11, 2019 and after the second accident, the FAA issued a Continued Airworthiness Notification to the International Community to inform the airline

operators about the ongoing and completed safety actions, mentioning that "external reports are drawing similarities" between the two accidents. Officially, the FAA commanded the grounding of all Boeing 737 MAX operated by U.S. airlines or in U.S. territory on March 13 (FAA 2019). The European Union Aviation Safety Agency (EASA) announced the suspension of operations in Europe on March 12 (EASA 2019). All Civil Aviation Authorities worldwide suspended the aircraft's operations until the 18th of March.

Recently, Boeing released a Return-to-Service update to inform the public regarding the status of the safety actions taken by the manufacturer towards getting the aircraft's airworthiness reapproved. The update includes among others, company actions, training and software updates. Especially, with regard to the software, MCAS update developed with additional layers of protection in the case of erroneous AOA sensors data. Specifically, the system will compare inputs from both AOA sensors, instead of using a single sensor, and will not activate MCAS in case of input disagreement of more than 5.5 degrees, while indicating it on the flight deck. Furthermore, MCAS when activated in non-normal conditions will provide only one input for each high AOA event, contrary to the repetitive trim inputs of the previous software version (Boeing 2019a).

Regardless of the actions taken, Boeing eventually announced that the production of the 737 MAX will be temporarily discontinued from January 2020. The manufacturer had only reduced the production of the aircraft despite the worldwide grounding.

4. Discussion: Analyzing the accident using the framework of smartness

This section focuses on the design failures that contributed to the fatal accidents involving the Boeing 737-8 MAX aircraft. Particularly, we examine and analyze the ones related to the automated flight control software function, called MCAS. We base our analysis on the published final Lion Air and the preliminary Ethiopian Airlines accident reports. We apply the conceptual framework of smartness of CPSs, described in Section 2.

The MCAS is an engineered system that integrates several of the aircraft's flight computing systems (e.g. ADIRU and FCC), the AOA sensors and the flight crew (i.e. human operators), to influence the (non-normal) flight characteristics by actuating the horizontal stabilizer in automated, cooperative and real-time manner. Therefore, the MCAS can be classified as a CPS under the notion of CPSs by Carreras Guzman et al. (2019).

We base our analysis on the published final Lion Air and the preliminary Ethiopian Airlines accident reports. We apply the conceptual framework of smartness of CPSs, described in Section 2.

In hindsight, it is not possible to claim that using the smartness framework would have prevented these accidents. Nevertheless, the analysis of these accidents serve to illustrate an application of the smartness framework into these particular scenarios.

In the next paragraphs, we analyse the design-related failures into types of failures and subsequently, we relate them with the framework of smartness dimensions and characteristics.

4.1 *Flight Displays, Alerts and Controls*

The AOA DISAGREE alert on both Primary Flight Displays, which is a standard feature in all Boeing aircrafts, was falsely linked to the optional and paid AOA Indicator (Boeing 2019b). This means that the airline operators that did not acquire the optional paid AOA indicator also did not have the standard AOA DISAGREE alert. In addition to that deficiency, during the accident flight, erroneous inputs from the AOA sensor resulted in several fault messages and alerts (e.g. IAS DISAGREE, ALT DISAGREE), and eventually in the uncommanded activation of MCAS. Moreover, the stick shaker, which is a tangible alert mechanism that intensively vibrates both control columns, was activated almost immediately after take-off due to the erroneous AOA sensor data, creating significant noise in the cockpit. All those conditions might have affected the flight crew's understanding and awareness of the situation. The flight crew, not being able to identify the problem, did not declare an urgency or emergency condition to the ATCo, and hence the flight crew was provided several heading instructions that further increased their workload.

Analyzing those failures from the perspective of the smartness dimension called **degree of integration**, the several fault messages and alerts – including the stick shaker that appeared during the accident flight – can be linked to *efficiency and optimization* issues, signifying non-optimal operation of the system's integrated resources.

Within the **real-time feedback control** dimension, we identify the absent AOA DISAGREE alert and the several fault alerts and messages as a *data visualization* issue. That is, the system's inability to present data in an understandable manner, and to prevent confusion. The system should also be able to identify the erroneous sensor data and report them timely (i.e. *identification*), whereas the physical sensor component should have minimal failure rates (i.e. *safety*). Additionally, the uncommanded MCAS activation signifies *interaction* and *usability*

issues. Interaction as a smartness characteristic is the ability of the user to interact with the system and to resolve occurring malfunctions, whereas usability is related to the easiness of that interaction. Both characteristics are omitted or depreciated in the analyzed system.

Most of the failures can also be related to the dimension of smartness called **level of automation**. Specifically, the erroneous AOA sensor data indicate inability of the system to gather meaningful information (i.e. *information collection*), and sense and understand the condition of its own components, what we call *self-awareness*. Moreover, the simultaneous activation of several alerts and fault messages suggests that the autonomous system is not capable of managing its operation (i.e. *self-regulation*) and adapt it to unforeseen situations (i.e. *adaptability*). The uncommanded MCAS activation with regard to the level of automation, signifies inability of the system to make logical inferences (i.e. *reasoning*) and select among alternatives based on various criteria (i.e. *decision-making*). The autonomous flight control system was not successful in understanding its own environment and identifying the erroneous data (i.e. *sensing and context-awareness*), which were falsely pushing to an AND position and caused the crashes.

Regarding the smartness dimension called **degree of cooperative control**, there is a *co-regulation* issue because the AOA DISAGREE feature is falsely affected by the operation of another interconnected software component, in that case, the AOA Indicator. MCAS presented *communication* and sharing control issues. Specifically, the system was not able to interact with the human operators and function safely, lacking *social readiness*. The flight crew's attempts to bypass MCAS were unsuccessful. In other words, the system was designed to operate in such way that inhibited the crew's commands, indicating also *co-regulation* issues. The software design failures are further analyzed in the next section. The classification of each failure in relation to the framework of smartness dimensions and characteristics is illustrated in Fig. 4.

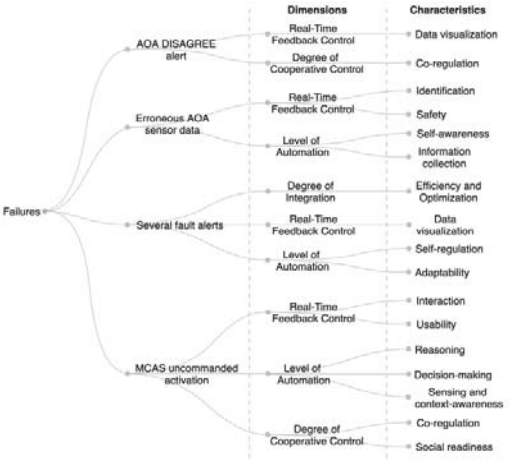

Fig. 3 The Flight Displays, Alerts and Controls failures linked to the framework of smartness dimensions and characteristics.

4.2 *Software design*

The following section discusses failures that are specifically related to the software design of the autonomous flight control system, known as MCAS. During the development process, MCAS was given increased authority to command high rate stabilizer movement up to 2.5 units within 10 seconds. Its operation was also expanded to low Mach numbers (i.e. at low speeds). MCAS commands can be counteracted by manual electric trim inputs from the flight crew. However, it resets after 5 seconds when manual electric trim inputs are performed. In the accident flight, the crew performed numerous manual electric trim inputs to correct the uncommanded MCAS activation. This resulted to several resets of that system and hence, to its repetitive and uncommanded activation. Surprisingly, MCAS function has limited redundancy by using input from a single AOA sensor only. This is because of the assumptions made during the Functional Hazard Assessment (FHA), which resulted in classifying the associated failure conditions as "major" (i.e. not hazardous or catastrophic), with a remote probability of occurrence. Therefore, that redundancy was not required by the regulations. Moreover, pulling back the control column normally interrupts any automatic electric stabilizer command to AND position. In the 737 MAX when the MCAS is operating, this cutout function is disabled, meaning that the flight crew commands cannot override the system's autonomous operation.

We identify an issue of the effective utilization of resources (i.e. *self-optimization)* in the **degree of integration** smartness dimension, due to the reliance of the system to a single-sensor input. This is despite the existence of several and redundant sensors that provide inertial position and track data, including attitude, altitude and airspeed.

With regard to the **real-time feedback control** dimension, the 5 second reset interval and the single-sensor input indicate design flaws that contribute to the inability of the system to identify emerging errors (i.e. *identification*), to regulate its *real-time* operation accordingly and preserve the *safety* of the system. Additionally, this non-redundant design inhibits the ability of the system to prevent failures (i.e. *prevention*) and reduces its

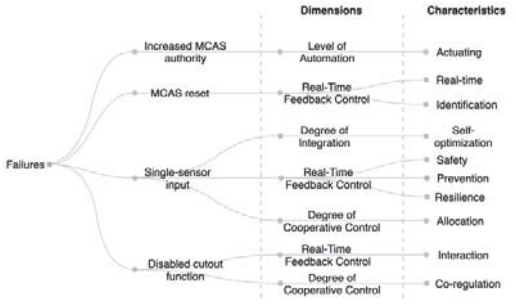

Fig. 4 The MCAS Software Design failures linked to the framework of smartness dimensions and characteristics.

capacity to recover when the failure occurs (i.e. *resilience)*. Moreover, the disabled cutout function signifies limited *interaction* between the flight crew and the system.

Analyzing the software design failures from the **level of automation** dimension of smartness, we identify two issues related to the *actuating* characteristic of the system. That is, the increased authority of MCAS in terms of the maximum command limit and the extended operation at lower speeds.

The design failures generated sharing control issues. The sharing characteristics are classified under the smartness dimension **degree of cooperative control**. For example, the single-sensor input indicates systems resources *allocation* deficiency, despite the existence of several and redundant sensors that provide crucial flight data. Furthermore, the disabled cutout function when MCAS is activated is an unnecessary feature related to the *co-regulation* characteristic of smartness in the degree of cooperative control. Fig. 5 depicts all the aforementioned failures related to the software design and how they are classified under the framework of smartness dimensions and characteristics in CPSs.

4.3 *MCAS Functional Hazard Assessment*

During the development process of safety-critical systems in aviation, the aircraft manufacturers perform safety assessments not only for the aircraft but also for the individual systems. FHA is performed on all those systems that are considered by the assessment to be required for safe flight and landing, in order to identify and classify failure conditions. The classification categories are typically "minor", "major", "hazardous" and "catastrophic" in accordance to the FAA System Design and Analysis requirements for airworthiness AC 25.1309-1.

Boeing identified and classified two hazards associated with uncommanded MCAS activation as "major". This classification did not require further analyses, such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA), which are performed for "catastrophic" and "hazardous" failure conditions. Those analyses, according to KNKT, would have been able to identify the potential single and combined failures. Moreover, a redundant software design that relies on both AOA sensors was not required by the regulations for that classification. Boeing did not consider in FHA the failure modes that could lead to uncommanded MCAS activation, such as the AOA sensor erroneous data. MCAS maximum authority limit of 2.5 units was not among the testing scenarios in simulations. The repetitive uncommanded activation of MCAS was evaluated no worse than single, and hence was not considered either.

The flight crew behavior assumptions that were made in the FHA, even though in agreement with the FAA regulations, differed from the crew reactions during the accident flight. This has happened because the combined effects of the failures and in-cockpit conditions – "the interactions of the pilots and the flight deck" that Spitzer (2001) emphasizes – were not properly considered and evaluated in the safety assessment.

Software updates are effortlessly pushed to products already on the market, creating a design culture that depreciates safety in the false impression that software "bugs" can be corrected afterwards (Travis 2019). However, this mentality can be hazardous, especially in safety-critical CPSs. The increasing complexity of smart CPSs due to the integration of modern ICTs requires improvements of the design and evaluation processes to include both software and human aspects (Axelrod 2013).

5. Conclusion

In this paper, we provided a conceptual framework to assess the increasingly complex smartness of CPSs. Our framework can be used as a guide when assessing the smartness dimensions and characteristics of a system against the potential failures and subsequent hazards. As a case study, the two recent fatal Boeing 737-8 MAX accidents have been a baleful but awakening alarm to the aviation industry. The shift from hardware to software reliance creates new vulnerabilities and risks that is critical we understand and are able to identify. In this regard, we applied the smartness framework to the aviation accidents and assessed the system design-related failures and errors according to the smartness dimensions and characteristics. In further work, we recommend an extension of the smartness framework to analyze the conceptual design of CPSs and suggest a balance between the smartness of the system and its robustness against failures and hazardous events.

References

AIB. (2019). "Aircraft Accident Investigation Preliminary Report No. AI-01/19."

Alur, R. (2015). *Principles of Cyber-Physical Systems*. MIT Press.

Arditi, D., G. Mangano, and A. De Marco. (2015). "Assessing the Smartness of Buildings." *Facilities* 33 (9–10): 553–72. https://doi.org/10.1108/F-10-2013-0076.

Axelrod, C. W. (2013). "Managing the Risks of Cyber-Physical Systems." In *2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–6. IEEE. https://doi.org/10.1109/LISAT.2013.6578215.

Boeing. (2019a). "737 MAX Software Update." 2019. https://www.boeing.com/commercial/737max/737-max-software-updates.page. (accessed October 22, 2019).

Boeing. (2019b). "Boeing Statement on AOA Disagree Alert." Boeing. 2019. https://boeing.mediaroom.com/news-releases-statements?item=130431.

Boeing. (2019c). "Statement from Boeing CEO Dennis Muilenburg: We Own Safety - 737 MAX Software, Production and Process Update." 2019. https://boeing.mediaroom.com/2019-04-05-Statement-from-Boeing-CEO-Dennis-Muilenburg-We-Own-Safety-737-MAX-Software-Production-and-Process-Update. (accessed September 10, 2019).

Carreras Guzman, N. H., M. Wied, I. Kozine, and M. A. Lundteigen. (2019). "Conceptualizing the Key Features of Cyber-Physical Systems in a Multi-Layered Representation for Safety and Security Analysis." *Systems Engineering*, 1–22. https://doi.org/10.1002/sys.21509.

Chronopoulos, C., N. H. Carreras Guzman, and I. Kozine. n.d. "Conceptualizing Smartness in Cyber-Physical Systems." *Working Paper*. Technical University of Denmark.

"Dimensions and Characteristics of Smartness in Cyber-Physical Systems — DTU Research Database." (2019). 2019. https://orbit.dtu.dk/en/activities/dimensions-and-characteristics-of-smartness-in-cyber-physical-sys. (accessed January 2, 2020).

EASA. (2019). "Boeing 737-8 MAX and 737-9 MAX - Suspension of Flight Operations (SD-2019-01)."

Endsley, M. R. (2017). "Autonomous Driving Systems: A Preliminary Naturalistic Study of the Tesla Model S." *Journal of Cognitive Engineering and Decision Making* 11 (3): 225–38. https://doi.org/10.1177/1555343417695197.

FAA. (2019). "Continued Airworthiness Notification to the International Community (CAN-2019-03)." Des Moines, WA.

KNKT. (2018). "Final Aircraft Accident Investigation Report KNKT.18.10.35.04." Jakarta.

Kushner, D. (2013). "The Real Story of Stuxnet." IEEE Spectrum. 2013.

Leggett, T. (2019). "'What Went Wrong inside Boeing's Cockpit?'" BBC. 2019. https://www.bbc.co.uk/news/resources/idt-sh/boeing_two_deadly_crashes. (accessed May 17, 2019).

Levin, S. (2018). "Tesla Fatal Crash: 'autopilot' Mode Sped up Car before Driver Killed, Report Finds." The Guardian. 2018. https://www.theguardian.com/technology/2018/jun/07/tesla-fatal-crash-silicon-valley-autopilot-mode-report. (accessed September 12, 2018).

Marchese, D., and I. Linkov. (2017). "Can You Be Smart and Resilient at the Same Time?" *Environmental Science and Technology* 51 (11): 5867–68. https://doi.org/10.1021/acs.est.7b01912.

Miller, S. (2009). "Contribution of Flight Systems to PErformance-Based Navigation." *AERO Magazine*, 2009.

Murman, E. M., and T. J. Allen. (2003). "Engineering Systems: An Aircraft Perspective."

NIST. (2017). "Framework for Cyber-Physical Systems: Volume 1, Overview." Vol. 1. https://doi.org/10.6028/NIST.SP.1500-201.

Pickthall, N. (2014). "The Contribution of Maintenance Human Factors to No Fault Founds on Aircraft Systems Engineering." In *Procedia CIRP*, 22:59–64. https://doi.org/10.1016/j.procir.2014.07.013.

Sabella, R. (2018). "Cyber Physical Systems for Industry 4.0." Ericsson. 2018. https://www.ericsson.com/en/blog/2018/10/cyber-physical-systems-for-industry-4.0. (accessed August 19, 2019).

Spitzer, C. R., ed. (2001). *The Aviation Handbook*. Boca Raton, CRC Press LLC.

Travis, G. (2019). "How the Boeing 737 Max Disaster Looks to a Software Developer." IEEE Spectrum. 2019.