How do Systems Fail?

Conference Paper · January 2020

DOI: 10.1109/RAMS48030.2020.9153715

CITATIONS
3

READS
931

2 authors:

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **937** CITATIONS

SEE PROFILE

Bryan O'Halloran
Naval Postgraduate School
64 PUBLICATIONS **476** CITATIONS

SEE PROFILE

How Do Systems Fail?

Bryan O'Halloran, Ph. D., Naval Postgraduate School
Douglas L. Van Bossuyt, Ph. D., Naval Postgraduate School

Key Words: Failure Analysis, Failure, Risk Analysis, Systems Engineering

SUMMARY & CONCLUSIONS

Modern systems are changing quickly and becoming more complex through increased connectivity, smaller packaging, higher performance requirements, more components, the inclusion of complex software and Artificial Intelligence (AI), and much more. The following are high-level challenges that arise in many modern systems. The first is the distribution of the system, which are both physical (e.g., power grids) and digital (e.g., air traffic control, transportation networks). With highly distributed system, the vulnerability from the environment becomes significant. The second challenge is the implementation of new technology where examples include driverless vehicles and Boeing's 787 Dreamliner. Occasionally implementing new technology doesn't lend well to their intended purpose as observed by the Supersonic Transport (SST) aircrafts for commercial flights such as Concorde [1] and the Tupolev Tu-144 [2]. This industry suffered a major crash, Air France Flight 4590, that killed 109 passengers and crew and led to the ultimate demise of the industry [3]. The result of these design challenges is the need for improved methods to identify, assess, and mitigate off-nominal behavior.

While all industries seek to create safe and reliability systems, their failures continue to splash across the news with surprising regularity. The examples are nearly endless. Across 63 years (1957-2019) there have been 402 mission failures in the spaceflight industry including satellites, manned spacecrafts, rockets, etc. As a subset of these missions, the manned spaceflight industry has seen 118 failures with a total of 262 deaths [4]; there have been 5 manned flight incidents where 19 astronauts died, 8 training or testing incidents where 11 astronauts died, 35 incidents where a total of 232 non-astronauts died (e.g., civilians, employees, etc.), and 70 incidents (35 flight and 35 training or testing) where no deaths occurred. Beyond the 402 mission failures, there have also been 118 Satellite launch failures [4]. Since the introduction of the commercial airline industry in 1918, there have been a reported 154,984 deaths [3]. Since 1970, there have been 11,634 accidents. Even more alarming is that the annual death rate hasn't decreased much with time. The death rate per year between 1970-2018 is 1722 and between 1990-2018 is 1337. While this has reduced, a large number of accidents continue to cause a large number of deaths in this industry. According to [5], there have been 25 major dam failures, 16 of which have occurred in the last 50 years. The nuclear power industry has observed over 100 failures, several of which have resulted mitigations exceeding a billion US dollars. It is important to note that systems fail with regularity regardless of the system's type, purpose, or age, the industry that the system belongs, or the era in which it was designed and built. The continued increase in what we demand from our systems has always trumped the practitioner's ability to assess and mitigate off-nominal behavior.

These facts show that failure has always been imminent. Until significant improvements are made to the way that we assess and mitigate failures, it is unreasonable to consider the outcome to change. As such, one element of assessment is to understand the variety of causes that involve the failures we observe. As such, this paper seeks to characterize failures by their cause. This is done by surveying a large number of failures from several different relevant industries, then deriving categories of failure cause.

Seven categories of failures are identified including: development failures, induced failures, common cause failures, propagated failures, interaction failures, malicious failures, and management, customer, and misuse failures. By understanding the different classes of failures potentially present in complex systems, engineers can better choose which failure, risk, and reliability analysis tools are most appropriate to use with specific systems. This in turn may lead to more reliable systems that are less prone to failure throughout the system lifecycle.

1 RELATED RESEARCH

Research has observed a variety of failures classifications for electromechanical systems. For many years, work has been done to classify failures by failure mechanisms. A variety of research exists here [6-8] that is primarily concerned with the modeling of such failures. Collins observes many of these failures models and created a strategy for defining all types of failure mechanisms [9]. His work is for mechanical and material failures, which he defines as the physical process that combines effects to produce a failure. As such, his approach can produce all known failure mechanisms by choosing a value from each of three categories; manifestation of failures, failures inducing agents, and the location of the failure. Uder extends this work by developing the electrical failure mechanisms into a taxonomy [10]. This work was further extended into a hierarchical failure modes and mechanisms taxonomy [11]. This group of research is concerned with the categorization of failure mechanisms, which are highly specific with respect to

the cause and does not include many failure causes identified in modern systems. In contrast, this research is seeking to categorize the cause at a broader level.

Other work has been done to classify failures that are not as specific and also not focused on electromechanical systems. Bondavalli and Simoncini classify failure modes in computing systems [12]. Wiegmann and Shappell define a classification for humans with the goal to mitigate the propagation of the error throughout the system [13]. Vaidyanathan and Trivedi develop a classification for software faults. They classify these into permanent, intermittent, and age-related faults [14]. Jouini et al., present a classification of security threats to information systems [15]. Their classification is extensive and includes the threat's source, agents, motivation, intention, and impact. Similarly, Pawar and Anuradha describe types of attacks on network systems [16]. Historically Hollnegal [17] and Rouse and Rouse [18] have developed a taxonomy of error types. Subsequent work by Sutcliffe and Rugg proposes a taxonomy that is relevant in failure analysis and risk assessment for human-computer systems [19]. Their classification types are broad such as cognitive, social, and organizational. These authors have developed classifications for several types of failures; however, they are not developed across several industries or to span multiple disciplines. As a result, they are only applicable within their industry.

While existing research has had the similar intent of classifying failures and other types of off-nominal behavior, it typically exists under the guise of one particular industry or discipline. We remove the semantic barriers (e.g., failure, hazard, error, etc.) that are defined by the disciplines, and instead focus on how the cause of the off-nominal behavior can be characterized. Further, we observer off-nominal behavior from several industries to inform the proposed classification.

2 DISCUSSION AND ASSESSMENT OF HISTORICAL FAILURES

This paper suggests ways to understand the cause of a system failure. The term failure is primarily used within reliability engineering, whereas its analogy in systems safety is a combination of hazard and mishap, and often the term error is used in a variety of industries. This paper uses the term failure more generically than its standard definition. Failing can be defined as anything off-nominal or unexpected, which significantly broadens the typical use of failure.

To ensure that the failure categories, presented later in this paper, are as comprehensive as possible, a variety of industries have been reviewed. This approach primarily ensured that the historical failures are not specific to one industry. The challenge was to define the boundary for which industries should be included. This was decided based on several factors including (1) the industry must produce systems, (2) the systems must be used by large populations of people (e.g., our society or the military), (3) the system must be definable and well-understood (e.g., the "internet" does not meet the criteria), and (4) a substantial amount of failure information must have been available. As a result, the following industries were reviewed: spaceflight, transportation (e.g., trains, planes, ships, and vehicles), oil and gas, defense, telecommunications, and industrial plants (power plants and manufacturing plants).

In addition to an industry being reviewed, we recognize that some industries have too many failures to assess, as noted previously in this paper. Due to the volume of failures, we have taken a sampling approach for many industries. When possible, specific criteria are used to direct this sampling. For dams, we review all cases later than 1970 to prove relevance toward modern systems. For nuclear power, we use all cases where the International Nuclear and Radiological Event Scale (INES) value is 5 or greater. The INES scale is a logarithmic scale, similar to the magnitude of earthquakes, and is used to characterize the consequence of an incident [20]. For the commercial aerospace industry, the seven cases with the most fatalities are used.

The failures were reviewed in two ways including general statistics and specific failure incident review. In the first case, general statistics, causes are identified by finding general failures cause statistics for an industry, as was the case for the automotive industry. In this case, the causes are clearly stated and take little effort to understand how they fit into the classification presented in this paper. In the second case, specific failure incident, the approach was to find and specific failures reports and derive the cause from them. In this case, a significant amount of review was required to ensure that all potential causes were evaluated. A database of these failures has been developed. Due to the size of the database, examples have been extracted and presented here.

Buffalo Creek Dam

- Date: 1972
- Description: Inspections were performed that were primarily unsatisfactory and led to decisions that were insufficient; one example was to add a 24-inch emergency spillway pipe, which ultimately was useless. Significant rainfall contributed to the possibility of dam overflow, for which the dam's management decided to add a second drainage pipe (in addition to the 24-inch pipe). This decision was made the day of the failure. Insufficient drainage appears to be one contributing factor toward the failure.
- Fatalities: 125 people
- Cost of incident: $50,000,000 (1972) or $306,391,148 (2019)

Google Self-driving Car

- Date: February 14, 2016
- Description: The autonomous vehicle encountered sandbags on the road and decided to stop before running over them. After waiting for several other vehicles to pass, the vehicle subsequently maneuvered around the sandbags. During the maneuver the autonomous vehicle struck the side of a bus. The autonomous vehicle was traveling at approximately 2 mph while the bus was traveling around 15 mph. As such, no injuries or significant damage was caused.
- Fatalities: 0 people
- Cost of incident: Not reported

Saudi Arabian Flight SV163

- Date: August 19, 1980
- Description: Shortly after takeoff, the crew noticed smoke rising from the cargo compartment. After confirming the smoke, the captain decided to turn the plane around and re-land. 5 minutes after radioing their plans back to the air-traffic control, the thrust level for engine 2 became jammed due to the fire burning through the operating cable. The captain shut the engine down the final approach to the airport. The aircraft made a successful landing and shortly thereafter came to a stop, however, due to their position they were located on the opposite end of the runway from the emergency team. The flight crew attempted to shut down engines, which the system required for evacuation, which ultimately took over 3 minutes. During this time communication with the crew was lost due to the fire continuing to spread. It took 23 minutes to get the first door open, during which time the rear inside of the plane was engulfed in flames. 3 minutes after opening the door, the remainder of the plane burst into flames and all members on the flight were lost. It was later determined that the likely cause of the fire was a personal stove being used by a passenger.
- Fatalities: 301 people
- Cost of incident: Not reported

Skylab Space Station

- Date: July 11, 1979
- Description: 63 seconds after launch, Skylab's micrometeoroid shield, intended to shield the system from space debris and function as a thermal blanket, opened unexpectedly. This resulted in the mounting of workshop solar array wing number 2 to fail and partially deploy. Subsequently the rocket motor thrust from stage two tore off the partially deployed solar array. The result of this was a communication issue with NASA, reduced power, and an overheated system. A partial recovery to the equipment was made by the crew, which successfully departed and made it back to earth safe; however, the system could not sustain its orbit over time and was ultimately put on a trajectory for destruction in the atmosphere. A math error led to debris landing in parts of Australia, but fortunately nobody was hurt.
- Fatalities: 0 people
- Cost of incident: Not reported

Mars Climate Orbiter

- Date: September 11, 1998
- Description: After a successful launch and 10-month travel toward Mars, the Mars Climate Orbiter was destroyed in flight. The cause was a set of data that was not converted during design, resulting in spurious data being used in the control of the system and causing an unexpected trajectory.
- Fatalities: 0 people
- Cost of incident: $125,000,000 (1998) or $196,428,680 (2019)

3 CLASSIFICATION OF HISTORICAL FAILURES

The purpose of this subsection is to present (1) the process for how the categories for a classification of historical failures were developed, (2) the specific categories for the classification of historical failures, and (3) example failures classified to demonstrate the classification categories.

3.1 Classification Category Development Process

We first began categorizing historical failures at a single level of fidelity. Next, we moved to hierarchical classification. This led us to identify that historical failures all relate to activities/actions in the system's lifecycle especially including the design phase of the system lifecycle. There are potentially an unlimited number of activities that could be involved in a failure event, and as such, we realized that there is a practical need to limit the total number of historical failure classification categories. If too many categories were allowed to exist, a lack of binning (i.e., one failure per category) may result which would not inform the user of the significance of the failure. This effort resulted in the failure classifications introduced and discussed in the following subsection.

3.2 Failure Classification

In the subsection below, categories for types of failures are proposed. Each category is provided with an explanation as well as examples. It is useful to note that in some cases the examples are relevant to more than one category. Due to this, we acknowledge two separate approach to "categorizing" failure: 1) a taxonomy categorization, and 2) a tagging categorization. The taxonomy approach leads to one choice in the taxonomy, which can exist at any level. In comparison, the tagging approach can be tagged with as many aspects as possible. We chose to combine the two approaches to allow as many categories to be selected as is needed to fully categorize a failure.

Development Failures: The development category includes failures caused during design, testing, and building (e.g., tests (e.g., ESS or otherwise) that induce a failure, workmanship/infant mortality, etc.). In reliability engineering, the bathtub curve describes the rate of failure as a function of time. The bathtub curve includes three regions: infant mortality, random failure, and wear-out [21] (note that the "random" region fits into a separate category). The infant mortality and wear-out failures fit in this category.

Induced Failures: Induced failures occur when a functional flow passes the system boundary and causes a failure in the system. Environmental failures are a subset of this category and have the same definition. Examples include systems that are dropped during manufacturing or transportation and systems that are used outside the design envelope. The latter is often observed in a system of systems (SoS) environment where a system (e.g., missile systems) is featured on another system (e.g., aircraft). This is the case since the parent system is the design being used and therefore the featured systems may not have been appropriate design to fit that use case.

Any system can fail due to induced failures. Systems are not made to handle every possible input that travels across the system boundary; doing so would lead to extraneous costs and system complexity. Therefore, this category of failure begs the

following question: How much do we investigate external flows? Fukushima was not designed to handle the combination of a magnitude 9.0 earthquake as well as a tsunami. These inputs were outside the bounds of the design due to their low probability of occurrence.

The debate within many induced failures is that they aren't failures at all. The definition of reliability demonstrates that unexpected environment are not to be included within the reliability calculation. Unexpected flows from outside the system are not expected to be designed in, and therefore a failure of the system should be anticipated.

Common Cause Failures: Common cause failures are defined as a single failure (e.g., component failures, maintenance failures, etc.) causing multiple redundant systems to fail [22]. These types of failures are relevant to systems with significant redundancy. Nuclear power is an example industry that specifically designs in significant redundancy, especially at the subsystem level (e.g., cooling subsystems), with the goal to protect the reactor core. Note that many systems naturally have a low risk to this category due to having a minimal amount of redundancy. Aerospace systems are an example.

Propagated Failures: Propagated failures tend to be catalyzed by an initial failure; however, this is not a requirement. In such a case, a failure occurs in the system which then subsequently causes additional failures. The number of failures the follow define the length of the propagation path.

Interaction Failures: Interaction failures can be largely characterized as the relationship between two or more items, whereas an item can be a function, physical component, software component, firmware component, etc. This type of failure can be understood by considering an example where two component, which independently have very high reliability, interact in a way that induces a failure. For example, a micro-controller sends a signal pyrotechnic device earlier than expected. While the microcontroller sent a good signal, and the pyrotechnic device received it as expected, the system has failed due to the timing issue. Everything worked, just not the way it was intended.

Malicious Failures: These are a new kind of off-nominal behavior and are not well understood or protected against. The classic example is Stuxnet where centrifuges were failing at an increased rate [23]. It was later found that these failures were due to a digital virus planted on computers that controlled the centrifuges. This case is interesting because the virus directed its attack on the physical system, whereas more traditional cyber-failures do not have a noticeable effect on the physical system.

Management, Customer, and Misuse Failures: All systems are designed to be used for a specific purpose. This is typically characterized during the design process using the Concept of Operations (CONOPS), specifications (i.e., set of specific requirements), etc. Management, customer, and misuse failures have one of the following characteristics including being used in a way that the system wasn't designed for, "management" making poor decisions about the operation of the system (e.g., over-use, omitting important indicators of a failure, making unethical decisions (e.g., Ford Pinto), restrictions due to budget, etc.), and acts of omissions (e.g., poor maintenance or inspection).

This section also include "random" failures. It is recognized that regardless of how well an item is designed, it still retains some chance of failing at any point in time. While this category is important, we recognize that every "random" failure has a cause, it is just unknown. Whether that cause was related to contamination during manufacturing, or a misunderstanding of the component (often the case when new technology is being integrated into a system), randomness is only the "best" way to describe it. As such, this category represents a lack of knowledge.

3.3 Example Failures Classified to Demonstrate the Classification Categories

Buffalo Creek Dam

- Failure categorization: (1) Induced failures, (2) Management, customer, and misuse failures, (3) Development failures
- Failure categorization reasoning: A significant storm initiated the failure, which was exacerbated by poor inspection/maintenance. Further, drainage pipe design led to insufficient drainage.

Google Self-driving Car

- Failure categorization: (1) Development failures, (2) Management, customer, and misuse failures
- Failure categorization reasoning: The vehicle stopped on the side of the road, putting the passenger in danger. During the re-entry onto the road, the driver did not take control as the bus approached.

Saudi Arabian Flight SV163

- Failure categorization: (1) Induced failures, (2) Propagated failures
- Failure categorization reasoning: A passenger started the fire with a person device, then the failure propagated throughout the aircraft.

Skylab Space Station

- Failure categorization: (1) Development failures, (2) Propagated failures
- Failure categorization reasoning: The failure was initiated by a failing component (i.e., Skylab's micrometeoroid shield inadvertently opened), then the failure propagated to the workshop solar array wing number 2, which ultimately was destroyed by the rocket motor thrust.

Mars Climate Orbiter

- Failure categorization: (1) Development failures
- Failure categorization reasoning: Errors in data processing were made during the design process.

4 APPLICATION OF FAILURE CATEGORIZATION

A system can be analyzed for similarities to existing systems that have experienced historical failures. For instance, a startup company designing a new space launch vehicle may find it useful to review past accident and mishap reports. An established company that has a product line with long history may have analyzed their own products' past mishaps to understand potential failure categorization. The use of a Failure,

Reporting, Analysis, and Corrective Action System (FRACAS) is another useful source of historical failures. However, looking across industries, as the work presented in this paper has done, can lead to new insights. In our own professional practices, we have encountered many instances where the reliability and failure analyses performed by a specific company or division of the company are chosen only because that is what they have historically done or that is all that is required by a regulatory agency. We have seen multiple instances where failures continue to happen because the wrong analyses are done or because the failure categorizations are not well understood.

In light of this, to make the best use of the failure categorizations presented above, a practitioner must assess the system of interest for potential failures and also in parallel must examine historical failure information from a wide range of systems beyond their specific industry or product. This may provide the insights necessary to realize that a potential for failures exist in the system that otherwise was not identified previously. As an example, in 2013 when Boeing released the 787 Dreamliner, it became evident that the lithium ion battery had issues. As a result of this battery issue, the 787 Dreamliner aircraft fleet was grounded worldwide. This was the first full grounding of an aircraft in 34 years, which demonstrates that it was a severe issue for Boeing as a company as well as their engineering capability [24]. The fundamental issue is that the lithium ion battery has caused many failures historically across a variety of industries [25]. Regardless, the issue was missed by Boeing during design of the 787 Dreamliner aircraft. As it relates to practitioners, this example highlights the value presented in this paper. Specifically, practitioners should observe failures that have occurred historically, either in adjacent industries or in their own, and use that information as an input when designing a new system. This can be done for any type of analysis that assess off-nominal behavior, and is ideally done as early in design as possible [26-34]. The failure categories presented in this paper have consolidated historically observed failures into a few categories allowing the practitioners to focus more on their assessment and less on identifying historical failure. These failure categories are specifically those that were not mitigated during design, regardless of whether they were assessed, which highlights an important point for practitioners. By nature these failures have shown to be evasive. As such, the rigor applied to these during an assessment should be significant.

In future work, we will develop a method to down-select what risk and failure analysis methods to use. This will allow practitioners to double-check that they are using appropriate analysis techniques to minimize the potential for missing or downplaying the importance of specific potential failure risks. While the work presented above helps to move practitioners toward the ability to easily look across domains to determine if they are thinking about all the potential ways their system of interest can fail, currently no one method has proven to be effective across multiple projects and industries, as evidenced by the use of different methods at different companies and in different industries.

Looking across domains to better understand failure and the inherent risk assessment biases that an industry or a practitioner has is similar in concept to the idea of the "anthropological lens" perspective and aligns with a new concept we refer to as the "assessment lens" approach to examining a system from multiple perspectives and with internal and external biases taken into consideration. Acknowledging and embracing the potential for biases and blind spots in failure and risk analysis gives practitioners a better opportunity to spot potential issues that otherwise would go unanalyzed. Making smart choices about which failure and risk analysis approaches to implement ensures the process is "right sized" to sufficiently analyze the system while not investing resources unnecessarily.

REFERENCES

[1] Sebastien Candel. Concorde and the future of supersonic transport. Journal of propulsion and power, 20(1):59-68, 2004.

[2] US Umesh Siddarth, Anuradha Das, and Bathinda MRSPTU. A review study on supersonic flight.

[3] The Bureau of Aircraft Accidents Archives (B3A). Statistics. Technical report, 2019. URL http://www.baaa-acro.com/statistics.

[4] Gary E Musgrave, Axel Larsen, and Tommaso Sgobba. Safety design for space systems. Butterworth-Heinemann, 2009.

[5] Association of State Dam Safety Officials. Lessons learned from dam incidents and failures, case studies. Technical report, 239 S. Limestone Street Lexington, KY 40508. URL https://damfailures.org/case-study/?posts per page=-1.

[6] Abhijit Dasgupta and Jun Ming Hu. Failure-mechanism models for excessive elastic deformation. IEEE Transactions on Reliability, 41(1):149-154, March 1992 1992.

[7] Junhui Li and Abhijit Dasgupta. Failure-mechanism models for creep and creep rupture. IEEE Transactions on Reliability, 42(3):339-353, September 1993 1993.

[8] Abhijit Dasgupta and Jun Ming Hu. Failure mechanism models for plastic deformation. IEEE Transactions on Reliability, 41(2):168-174, June 1992 1992.

[9] J.A. Collins. Failure of Materials in Mechanical Design. John Wiley & Sons, New York, NY U.S.A., 1993. ISBN 0-471-55891-5.

[10] S. J. Uder, R. B. Stone, and I. Y. Tumer. Failure analysis in subsystem design for space missions, 2004.

[11] Bryan M O'Halloran, Robert B Stone, and Irem Y Tumer. A failure modes and mechanisms naming taxonomy. In Reliability and Maintainability Symposium (RAMS), 2012 Proceedings-Annual, pages 1-6. IEEE, 2012.

[12] Andera Bondavalli and Luca Simoncini. Failure classification with respect to detection. In [1990] Proceedings. Second IEEE Workshop on Future Trends of Distributed Computing Systems, pages 47-53. IEEE, 1990.

[13] Douglas A Wiegmann and Scott A Shappell. A human error approach to aviation accident analysis: The human factors analysis and classification system. Routledge,

2017.
[14] Kalyanaraman Vaidyanathan and Kishor S Trivedi. Extended classification of software faults based on aging. In Fast Abstract, Int. Symp. Software Reliability Eng., Hong Kong. Citeseer, 2001.
[15] Mouna Jouini, Latifa Ben Arfa Rabai, and Anis Ben Aissa. Classification of security threats in information systems. Procedia Computer Science, 32:489-496, 2014.
[16] Mohan V Pawar and J Anuradha. Network security and types of attacks in network. Procedia Computer Science, 48:503-506, 2015.
[17] Erik Hollnagel. Human reliability analysis: Context and control, volume 145. Academic press London, 1993.
[18] William B Rouse and Sandra H Rouse. Analysis and classication of human error. IEEE Transactions on Systems, Man, and Cybernetics, (4):539-549, 1983.
[19] Alistair Sutclie and Gordon Rugg. A taxonomy of error types for failure analysis and risk assessment. International Journal of Human-Computer Interaction, 10(4):381-405, 1998.
[20] Canadian Nuclear Safety Commission et al. International nuclear and radiological event scale. 2014.
[21] Patrick O'Connor and Andre Kleyner. Practical reliability engineering. John Wiley & Sons, 2012.
[22] Seppo Sierla, Bryan M O'Halloran, Tommi Karhela, Nikolaos Papakonstantinou, and Irem Y Tumer. Common cause failure analysis of cyber-physical systems situated in constructed environments. Research in Engineering Design, 24(4):375-394, 2013.
[23] Thomas M Chen and Saeed Abu-Nimeh. Lessons from stuxnet. Computer, 44(4):91-93, 2011.
[24] Wingfield-Hayes, Rupert. Dreamliners: Boeing 787 Planes Grounded on Safety Fears. BBC News. British Broadcasting Corporation 17, 2013.
[25] Hendricks, Christopher, Nick Williard, Sony Mathew, and Michael Pecht. A failure modes, mechanisms, and effects analysis (FMMEA) of lithium-ion batteries. Journal of Power Sources 297:113-120. 2015.
[26] Bryan M O'Halloran, Nikolaos Papakonstantinou, Kristin Giammarco, and Douglas L Van Bossuyt. A graph theory approach to functional failure propagation in early complex cyber-physical systems (ccpss). In INCOSE International Symposium, volume 27, pages 1734–1748. Wiley Online Library, 2017.
[27] Seppo Sierla, Bryan M O'Halloran, Heikki Nikula, Nikolaos Papakonstantinou, and Irem Y Tumer. Safety analysis of mechatronic product lines. Mechatronics, 24(3):231–240, 2014.
[28] Bryan M O'Halloran, Brandon Haley, David C Jensen, Ryan Arlitt, Irem Y Tumer, and Robert B Stone. The early implementation of failure modes into existing component model libraries. Research in Engineering Design, 25(3):203–221, 2014.
[29] Heikki Nikula, Seppo Sierla, Bryan O'Halloran, and Tommi Karhela. Capturing deviations from design intent in building simulation models for risk assessment. Journal of Computing and Information Science in Engineering, 15(4):041011, 2015.
[30] Guillaume L'her, Douglas L. Van Bossuyt, and Bryan M. O'halloran. Prognostic systems representation in a function-based bayesian model during engineering design. International Journal of Prognostics and Health Management, 8(2):23, 2017.
[31] Bryan M O'Halloran, Christopher Hoyle, Irem Y Tumer, and Robert B Stone. The early design reliability prediction method. Research in Engineering Design, pages 1–20.
[32] Nikolaos Papakonstantinou, Scott Proper, Douglas L Van Bossuyt, Bryan O'Halloran, and Irem Y Tumer. A functional modelling based methodology for testing the predictions of fault detection and identification systems. In ASME 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, pages V01BT02A015–V01BT02A015. American Society of Mechanical Engineers, 2016.
[33] Douglas L Van Bossuyt and Bryan M O'Halloran. A method to choose between automation and human operators for recovery actions during a cyber-attack. Procedia Computer Science, 153:352–360, 2019.
[34] Douglas L Van Bossuyt, Bryan M O'Halloran, and Ryan M Arlitt. Irrational system behavior in a system of systems. In 2018 13th Annual Conference on System of Systems Engineering (SoSE), pages 343–349. IEEE, 2018

BIOGRAPHIES

Bryan O'Halloran, Ph.D.
Naval Postgraduate School
833 Dyer Road, Bullard Hall 218, Monterey, CA 93943, USA

e-mail: bmohallo@nps.edu

Dr. Bryan M. O'Halloran is currently an Assistant Professor in the Systems Engineering department at the Naval Postgraduate School (NPS). His research interests include risk, reliability, safety, and failure modeling in the early design of complex systems.

Douglas L. Van Bossuyt, Ph.D.
Naval Postgraduate School

833 Dyer Road, Bullard Hall 218, Monterey, CA 93943, USA
e-mail: douglas.vanbossuyt@nps.edu

Dr. Douglas L. Van Bossuyt is currently an assistant professor at NPS in the Systems Engineering Department. His area of research focuses on risk and failure-informed conceptual design and trade-off study philosophies for complex systems.