Journal of System Safety

Assuring the Future of System Safety

Volume 58 No. 1
Winter 2023

A publication of the International System Safety Society -
Professionals dedicated to the safety of systems, products, and services

e-ISSN 2832-305X

Journal of System Safety

Editorial Team

For more information please visit our Editorial Team page

Editor-in-Chief

Dr. Charles Muniak
Syracuse Safety Research, USA
Email: editor@jsystemsafety.com

Associate Editors

Dr. Rod Simmons
Independent Consultant, USA

Stephen Thomas
NVIDIA Corporation, USA

Dr. Rami Debouk
General Motors, USA

Editorial Board

International System Safety Society

For more information please visit the Society Home page

Officers

Pam Alte, *ISSS President*
Dave West, *ISSS Executive Vice President*
Pam Kniess, *ISSS Treasurer*
Dr. Rami Debouk, *ISSS Executive Secretary*
Russ Mitchell, *ISSS Immediate Past President*

Directors

Dr. Rodney Simmons, *Education & Professional Dev.*
Donna DiFiglia, *Chapters & International Outreach*
Don Swallom, *Publicity and Media*
Rita Turner, *Member Services*
Yawa Adonsou, *Government & Inter-society Services*
Mike McKelvey, *Conferences*

Connect on Social Media

Society Corporate Partners

A-P-T RESEARCH, INC. AN EMPLOYEE-OWNED COMPANY

base2 solutions a Belcan company

DSTA Defence Science & Technology Agency

FIRSTMERIT Solutions

Parvati Consulting

An official publication of the International System Safety Society, Inc., a non-profit corporation incorporated in the District of Columbia.

Journal of System Safety is published three times a year by the International System Safety Society for the transmission of technical material and news of topical interest to those associated with the practice of system and product safety. Information, recommendations, statements and opinions expressed herein are those of the individual authors and advertisers and do not necessarily represent those of the International System Safety Society. Certain material is published for the purpose of stimulating independent thought on controversial matters or on problems of vital concern to safety professionals. Although caution is taken to ensure accuracy, the publishers or editors cannot accept responsibility for correctness or accuracy of the information presented.

ARTICLE SUBMISSION
Journal of System Safety welcomes article submissions from its readers. Technical manuscripts and news items of interest should be submitted at jsystemsafety.com or sent to Dr. Chuck Muniak, JSS Technical Editor, at journaleditor@system-safety.org. Authors should include the following: (1) one printed copy of the manuscript, double spaced; (2) electronic file in Microsoft® Word™, Adobe® InDesign® or ASCII format; (3) a statement of copyright ownership; (4) a short (one paragraph) author profile; (5) the author's name, address, daytime phone and fax number, email address, affiliation and professional status. For more information on submissions, please see our author guidelines or email journaleditor@system-safety.org. All submissions are subject to peer review.
If authors wish to have their materials returned, they should send a specific request along with a self-addressed, stamped envelope.

ADVERTISING POLICY
Journal of System Safety welcomes advertising compatible with the objectives of the International System Safety Society, subject to the approval of the Technical Editor. The acceptance of advertising does not imply endorsement by the Society or Journal of System Safety.
For more information on advertising, call 651-265-7856 or contact systemsafety@system-safety.org.

MEMBERSHIP INFORMATION
For information on subscription rates and membership, contact the International System Safety Society, 1000 Westgate Dr. Suite 252 Saint Paul, MN, 55114, USA. Tel: 651-265-7856; email: systemsafety@system-safety.org; Web site: www.system-safety.org.

EDITORIAL DISCLAIMER
The views expressed in the editorials and columns in Journal of System Safety are those of the individual writers and do not necessarily reflect the views of the International System Safety Society.
(e-ISSN 2832-305X)

Table of Contents

In The Spotlight

Features

From the Editor's Desk

JSS Technical Editor
C. G. Muniak P.hD.

Significance of Significance

I was recently discussing some research papers with a colleague who placed a lot of weight on the "significance" aspects of some statistical conclusions. I was reminded of one of my statistics professors from 40 years ago warning us about p values. A p value of less than 0.05 is often considered to be the "gold standard" for ascertaining whether an experimental result has merit (Ref 1). However, the result may have statistical significance but may represent a very small difference between the control and treatment groups and be of little or no practical importance. Some authors may be "bending" research data in the search for statistical significance in places where none exists. This may be the basis for the phenomena of "difficult to replicate" experiments that is now being seen by the scientific community (e.g., Ref 2). Alleged positive effects of treatments may be extremely small or non-existent making it difficult or impossible for another researcher to replicate the experiment.

The first technical paper in this issue is "Incremental Assurance Through Eliminative Argumentation" by Simon Diemert, John B. Goodenough, Jeff Joyce and Charles B. Weinstock. This paper proposes the notion of incremental assurance wherein the assurance case structure includes both the currently available evidence and a plan for incrementally increasing confidence in the system as additional or higher quality evidence becomes available.

The second technical paper is "The Difficulties with Replacing Crew Launch Abort Systems with Designed Reliability" by Shaun R. Ryan. Historical launch vehicle reliability is compared to system safety standards used in the commercial aviation industry to understand if future designs truly need a crew abort system.

The third paper "Quantification of Benefits for Medical Devices" is by Bijon Elahi. This paper proposes a methodology to quantify benefits, thereby creating more consistency, and clarity in the evaluation of benefits and the benefit/risk ratio.

The "TBD" column by Charlie Hoes discusses the difficulties one encounters when navigating our complex medical system.

As usual, I welcome your comments, letters to the editor and article submissions.

Regards,
Chuck

References

1. Denworth, L. "A Significant Problem," Scientific American, October 2019
2. Holz, R. L. "Most Science Studies Appear to Be Tainted by Sloppy Analysis" The Wall Street Journal, September 14, 2007

TBD

by Charles Hoes

I was called home from the last conference because my wife had been taken to the emergency room (ER) with a seizure that turned out to be caused by an aggressive, non-operable type of brain cancer. She has since experienced three bouts of seizures resulting in transfers to a number of places: emergency room (ER), Intensive Care Unit (ICU), rehabilitation facility, and home. She spent about a half of the last two months in the hospital, with me sitting next to her side many hours a day. She is currently living at home undergoing a lengthy treatment of radiation and chemo therapy. She is sleeping much of the day. While she sleeps I have enough free time for me to write this article. Of course we are hoping for the best. It has been a pretty rough road so far.

This series of events and hospital stays has given me a lot of time to observe the patient-staff interactions of a small slice of the healthcare system from the "System Safety" point of view. There are many excellent papers on many safety aspects of the healthcare industry, including Dev Raheja's extensive writings about many of the system safety issues found with health care facilities. His many "System Safety in Healthcare" articles in the Journal of System Safety cover a wide range of topics, from the importance of system safety analyses for medical hardware to the "softer" human factors issues of providing healthcare. His articles are an excellent source of information, considerations and recommendations for improvements across the field of healthcare. In this article I am looking at the problems from a slightly different perspective, that of a "user" of the healthcare system.

My family's health insurance plan covers a wide (but not all inclusive) range of healthcare services through a large hospital chain. The general approach that they use to manage the patient's needs is to assign a General Practitioner (GP) to each member. The GP takes care of most common healthcare needs, and acts as the central hub connected to a system of specialists through referrals; except when entering the system through the ER, in which case the responsibility for providing referrals to specialists seems to change as the situation progresses.

During "normal" use I find the approach of always going through the GP to access specialists awkward and frustrating because it inevitably results in long delays and multiple doctor visits before obtaining a referral to a specialist. This approach of treatment by the GP first, with referrals for cases that are outside of the GP's expertise is understandable in the sense that it provides a means for limiting access to the more expensive services of the specialists, but it is frustrating when you know which specialist is most appropriate and have to "get permission" to receive services.

One of my observations while sitting and watching has been that there is a very strong tendency to limit care options to those things that are covered by the health care plan, rather than those options that would be most beneficial for my wife. There was very little "thinking outside the box" to other options that might not be covered by insurance, or provided by this particular health care system. The decisions seem to be about whether or not something is covered rather than finding the best solution. Since we are in our "Medicare Years", their approach almost always reverts to what services are covered and "allowable" by Medicare. Part of my frustration is that we are not financially limited to just what is covered, my wife and I spent fifty-five years building a financial cushion sufficient to withstand significant health care expenses – only to have our options limited by a healthcare plan designed to comply with Medicare limitations. We don't even

get apprised of other options that are available outside of the plan. There is a constant limitation of suggestions, recommendations and potential options because of this "wall" created by the limitations of "the plan."

While these types of problems are frustrating, expensive and achieve far below "optimal" healthcare outcomes, they pale in comparison to the much larger problem of extreme "siloing" within the system. My wife's condition(s) result in many different groups working to help her during the same period of time. She is in need of parallel treatments, not serial treatments flowing from one silo to the next .The list of involved groups includes (but is not limited to) the initial Emergency First Responders, ER personnel and doctors, ICU staffing and doctors, in-patient staffing and doctors, other doctors and staff such as the neurosurgery group, the oncologists, the palliative care nurses, the hospitalist(s), separate hospitals such as those doing rehabilitation services (i.e.; physical rehabilitation, occupational rehabilitation, speech therapy, social services), cardiologists, home care professionals and more. Each of the various facilities has their own administrators looking after the "wellbeing" of the organization (apparently mostly concerned with staffing and resource issues). Within each location (e.g., ER, ICU, Rehab Facility) there are other subgroups for nursing, nutrition, facility cleanliness, laundry, doctors, etc. Each of those subgroups also include managers that look after the needs of that group. What is missing is someone looking after the care of the patient!

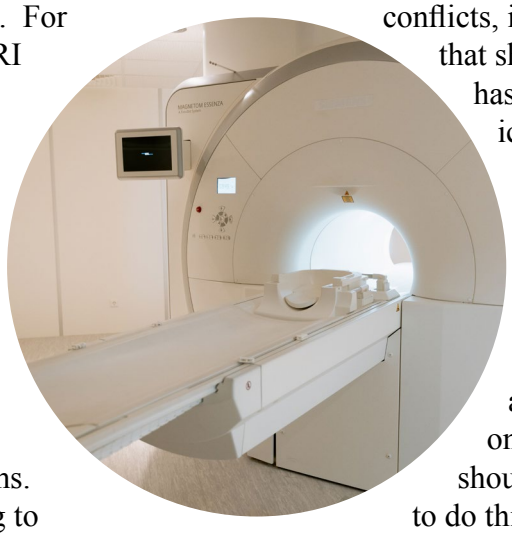
Medical records within the main hospital system are highly computerized and available to those with a need to know in that system. Great attention is paid to making sure that this medical record system is up-to-date and filled with the detailed information concerning what actions have been taken. The medical record system contains the details of the care including vital signs taken many times a day, the medications, schedules, details of bowel movements and trips to urinate, the type and quantity of food eaten, times of visits by nurses, doctors, technicians and more. These details make up the "medical record" but it is unclear how often users have the time or the focus to know what it contains or means. The record has a great amount of detail, but perhaps not enough summary/interpretation/knowledge. One of my main roles while sitting and waiting was acting as a "hub" for information. The people (doctors, nurses, therapists, etc.) that came to check and evaluate always wanted to know what was going on with the other specialties; asking me what the various doctors and nurses were finding and describing, what "the plan" was, and a high level description of how things were going. It was clear that they weren't just being friendly; they often didn't know much about the specific "system" consisting of my wife. They changed shifts, changed schedules and changed patients so often that there wasn't sufficient continuity or knowledge transfer. There was a brief hand-off between shift changes, but clearly not in sufficient depth or detail to fully understand her situation. For example, the nutrition folks would bring a meal and put it on her tray for her without opening containers or taking the shrink wrap off, and leave to go onto their next delivery. They didn't know that she couldn't use her hands, so she couldn't get to the food.

"While these types of problems are frustrating, expensive and achieve far below "optimal" healthcare outcomes, they pale in comparison to the much larger problem of extreme "siloing" within the system."

Photo: Pexels

She could handle a fork and spoon well enough to eat, but couldn't get past the shrink wrapping to access the food. She was always a "new" adventure for each person. It was clear that they really needed someone to add in the "other" details that weren't in the medical records, or that are just too difficult to tease out from the sea of details. (Of course, I would open the containers for her when I was there, but it wasn't unusual for me to come back from a break to find unopened food on her tray.)

The lack of communication and continuity is a serious problem within the organization, but becomes far worse when outside organizations come into the picture. For example, her first stay at a hospital was an out-of-plan hospital in a different town. They had a sophisticated medical record system, but a different one from "our" hospital; therefore there was no easy way for the doctors to communicate. For example, I had to hand-carry the MRI DVD disc from one hospital to the other so that the second neurosurgeon could see the original scan to determine what had changed. It was up to me to make sure that the neurosurgeon was aware of its existence. In addition to the disc, I carried a subset of the medical records to physically hand over to the next hospital because it is difficult to communicate between systems. The same thing happens when going to an "outside" service provider for the radiation treatment. I had to meet with doctors on both sides so that I can tell each what the other is seeing and doing. They don't have an automatic way of seamlessly communicating between facilities or organizations. "My" hospital oncologist provides a referral to the "other" facility to provide treatments, but gets little or no feedback on progress or status.



While the hospital has a fancy computerized scheduling system for appointments and the like, there is no way to tie in the "outside" services and schedules. The folks that are providing at home services (such as rehabilitation) don't have access to the schedules of the other providers. I have to work with each and every appointment to find a space where I can fit it in, there is nothing like an on-line scheduler to allow me (as the patient representative), or other providers, to add in their scheduling constraints. It is a constant frustration, one that most patients would be unable to navigate without a dedicated, full-time, helper such as myself. My wife couldn't do any of these things – after all she has brain cancer which is sort of interfering with her cognitive and physical abilities. Most patients have issues that make it difficult, or impossible, to actively participate in the care system beyond doing what they are directed to do. Depending upon the patient to take care of a huge portion of the "logistics" problem doesn't work effectively or efficiently.

In summary, a huge hole in the health care system is the lack of a patient "advocate" within the system. Someone needs to be assigned to each patient to make sure all of the details are working and coordinated properly. This must be someone who is knowledgeable enough to recognize when there are conflicts, incompatibilities, and deviations that shouldn't be happening. Someone has to be monitoring things like medications, vital signs, appointment schedules, missing needs, etc. I am attempting to do this for my wife but I don't have the knowledge, the time (I can't do this 24/7 as is needed), and access to the detailed medical records. I am mostly blind and ignorant, meaning I can pick up on the things I can, but not all that I should. The GP might be in a position to do this, but in this case she doesn't get the records, doesn't know what is happening, and doesn't have anywhere enough time to do that because she has a full case load of her "normal" patients. She wants me to update her on my wife's status now and then to find out what is happening and how things are going. She is depending upon me to do a job that I am not qualitied to do. During times of great stress (which have been common with my wife's condition) I am not emotionally suited to identify and understand the kinds of information that the GP, neurosurgeon, oncologist, cardiologists, and others want me to update them about.

Now that my wife has been discharged from the hospital almost all of her support has been eliminated. We have medicines to take, but not much else. I don't have the tools or knowledge to know how to do things like manage her pain, keep her nutrition appropriate

now that she has lost interest in food, make sure she is getting "enough" exercise now that she sleeps almost all of the time, what I should be doing to prevent problems associated with too much inactivity. The list goes on, but there is no easy place to turn to for help. I can call the "advice nurse" who generally helps make the decision of whether or not to go to the ER – but little else. I can contact her GP who has almost no knowledge of her specific issues or history with regard to her current problems, and just refers me to someone else. The oncologist gives me cancer related advice and information. The physical and occupational therapists only have advice on how to rebuild strength once it has been lost and the cause of the loss has been eliminated, rather than on what we can do to minimize the loss. The radiation treatment facility only checks to make sure the treatments are being performed on schedule. They tell me to make sure she gets enough nutrition and exercise, but offer no guidelines or details about what that means or how I might accomplish it. All of the various doctors treating her at the hospital are no longer involved because she is no longer in "their" department – I am left on my own without any advice, equipment or knowledge about what to do now or in the near future as her condition deteriorates. Each time she gets re-admitted, an entirely new set of people get assigned to her care, with almost no historical knowledge of previous conditions from a month ago. I don't have sufficient information to allow me to effectively plan ahead.

The bottom line is that their "system" doesn't seem to have a working system with regard to the patient. Their "system" works as long as she is within a narrow "silo" of concerns, but situations that cross into other "silos" (such as transferring from the ER to the ICU), or stretch over time, get missed or confused. Now that she is not in anyone's silo, she is in my care – and I don't have the resources or knowledge necessary to take care of what comes up. Even if she ends up going back to the hospital, or into a "skilled nursing facility", the problem of maintaining a unified, coordinated care regime will still be faced with the silo problem.

Original Article
https://doi.org10.56094/jss.v58i1.215

International System Safety Society

www.jsystemsafety.com

Journal of System Safety

Established 1965 Vol. 58 No. 1 (2023)

Incremental Assurance Through Eliminative Argumentation

Simon Diemert[ab], John B. Goodenough[c], Jeff Joyce[d], Charles B. Weinstock[c]

[a] *Corresponding author email: simon.diemert@cslabs.com*
[b] *Critical Systems Labs, University of Victoria; Victoria, Canada*
[c] *Carnegie Mellon Software Engineering Institute; Pittsburgh, United States*
[d] *Critical Systems Labs; Vancouver, Canada*

Keywords
assurance cases, confidence, eliminative argumentation, goal structuring notation

Peer-Reviewed
Gold Open Access
Zero APC Fees

Online: 22-Feb-2023

Cite As:
Diemert S. et al, Incremental Assurance Through Eliminative Argumentation. Journal of System Safety. 2023;58(1):7-15. https://doi.org10.56094/jss.v58i1.215

ABSTRACT

An assurance case for a critical system is valid for that system at a particular point in time, such as when the system is delivered to a certification authority for review. The argument is structured around evidence that exists at that point in time. However, modern assurance cases are rarely one-off exercises. More information might become available (e.g., field data) that could strengthen (or weaken) the validity of the case. This paper proposes the notion of incremental assurance wherein the assurance case structure includes both the currently available evidence and a plan for incrementally increasing confidence in the system as additional or higher quality evidence becomes available. Such evidence is needed to further reduce doubts engineers or reviewers might have. This paper formalizes the idea of incremental assurance through an argumentation pattern. The concept of incremental assurance is demonstrated by applying the pattern to part of a safety assurance case for an air traffic control system.

INTRODUCTION

Assurance cases are important engineering artifacts used to demonstrate that a critical system is acceptably safe or secure; they are comprised of a structured argument supported by evidence generated throughout the system's development lifecycle (Kelly, 1998; Assurance Case Working Group, 2021). Assurance cases are required for compliance with standards such as ISO 26262, UL 4600, and EN 50126, and are necessary for regulatory submissions in some jurisdictions. Assurance cases adopt a goal-oriented approach to assurance that is suitable for development of modern systems where the reasons why the system is safe or secure are complex.

Evidence is an essential ingredient of an assurance case. Without evidence, the arguments therein cannot be substantiated. However, while developing an assurance case a question that often arises is: what evidence is needed to support the case? Since assurance cases have a role to play across all phases of systems development, there are many contexts where this question is relevant and in each context the answer might be different. For example, during early prototyping of a system the evidence necessary to convince stakeholders that the system will eventually achieve its safety or security objectives is different from the evidence presented to an assessor during regulatory review. Regardless, in all contexts the evidences' role is to support an argument that aims to convince a reader (management, business partners, assessors, or the public) that the system has achieved the identified safety or security objectives.

Viewing an assurance case's purpose as one of persuasion allows the question posed above to be re-framed into one of confidence: what evidence is needed to be confident that a claim in the assurance case is valid? From this perspective, not all evidence is the same and different pieces of evidence will contribute by varying degrees to confidence in a claim. For example, for a software routine, a formal proof is typically considered to be more convincing than test results for establishing that the routine is defect free.

To complicate matters, not all evidence is available when an assurance case is prepared. Assurance cases are valid at a specific point in time, such as the day the system is delivered to a certification authority for review. As a result, the argument is structured around what evidence is expected at that point in time, as if this is the final state of what will ever be known about the system by engineers responsible for assuring the system. However, modern assurance cases are rarely one-off exercises and stakeholders may anticipate that more information will become available, such as field data, that could strengthen (or weaken) the validity of the assurance case argument (Koopman & Wagner, 2020). This means that confidence in the assurance case will change (and hopefully increase) as further evidence becomes available.

Since different types of evidence, each carrying a different weight in terms of confidence they afford, become available at different times it follows that confidence in the assurance case changes incrementally over time. As each piece of evidence becomes available, confidence in the top-level claim of the case increases (or decreases) by some incremental amount. This paper applies this notion of incremental assurance to the existing Eliminative Argumentation (EA) method for developing confidence in an assurance case (Goodenough, Weinstock, & Klein, 2015). The idea of incremental assurance is formalized as an argumentation pattern that may be employed in any EA-style assurance case. The pattern is applied to an assurance case fragment for an air traffic control system to illustrate incremental assurance in a real-world use of EA.

ASSURANCE CASES AND ELIMINATIVE ARGUMENTATION

An assurance case is a structured argument showing why one should have confidence in the validity of a claim given certain evidence. By providing explicit claims and reasoning for why evidence is believed to support the claims, an assurance case makes explicit the reasoning that is otherwise often implicit in arguments intended to show that a system is acceptably safe or secure (or any other property of interest). The assurance case has its roots in the notion of a safety case, which is used in safety critical system development. This section provides a brief introduction to the Eliminative Argumentation (EA) method for developing assurance cases.

THE ROLE OF DOUBT IN SAFETY ARGUMENTATION

Safety arguments that aim to directly "prove" that a system is safe are subject to confirmation bias. The fatal crash of the Nimrod military aircraft in Afghanistan in 2006 is a well-known of example of how confirmation bias can undermine an assurance case. The post-crash investigation found that: "the Nimrod Safety Case [was] fatally undermined by an assumption by all the organisations and individuals involved that the Nimrod was 'safe anyway', because the Nimrod fleet had successfully flown for 30 years, and they were merely documenting something which they already knew. … The Nimrod Safety Case became essentially a paperwork and 'tickbox' exercise" (Haddon-Cave, 2009).

An assurance case starts with a top-level claim which is recursively decomposed into sub-claims which are eventually supported by evidence. Traditional notations (e.g., GSN) do not emphasize the expression of doubt and therefore it is less likely that the claims and evidence expressed will be questioned. There is no way to express residual risk.

In practice, engineers have many reasons to doubt the safety of a system. Doubting oneself and subsequently addressing those doubts with further claims and evidence is central to the scientific and engineering approach to problem solving. But enumerating doubts is not, on its own, sufficient to mitigate confirmation bias. Enumeration of doubt only shifts the question from "Do the sub-claims completely support the top-level claim?" to "Have all doubts been identified?" However, this question, in turn, necessitates further argument explaining why one believes that there is, at most, a slight possibility that a relevant doubt has been overlooked. For example, one might doubt the completeness of a set of failure modes derived for a component in the system based on a Failure Modes and Effects Analysis (FMEA). An argument countering this doubt might claim that a combination of experienced persons and systematic methodology provide confidence in the completeness of the failure modes. Even so, a residual doubt will exist and be communicated to stakeholders as a risk associated with the component.

PRIMER ON ELIMINATIVE ARGUMENTATION

The question arises: Why should we believe an assurance case? A lack of confidence in a claim implies that there are doubts that it is true. If doubts exist, we cannot be completely confident in the claim. Every time a doubt is resolved (i.e., minimized or eliminated), confidence in the claim increases. When all doubts have been sufficiently resolved, there is high confidence in the claim. The practice of postulating and resolving doubts about an assurance argument is the basis for Eliminative Argumentation (EA) introduced by Goodenough et al. as an adaption of Toulmin's and Kelly's notation (Goodenough, Weinstock, & Klein, 2015; Kelly, 1998; Toulmin, 2003). EA provides a framework for constructing an argument and assessing confidence in the argument based on the identification and eventual resolution of doubts[1].

EA addresses confirmation bias by including the notion of doubt as a first-class citizen. In EA, these doubts are called "defeaters" in the sense that they defeat aspects of an argument. There can be doubts that rebut claims (e.g., "the valve will open" might be rebutted by "unless the valve is stuck"), undermine evidence (e.g., "all tests pass" might be undermined by "but the system tested is not the one deployed"), or undercut inferences (e.g., "if all the doubts about the claim have been resolved, then the claim is true" might be undercut by the defeater "unless there is an unidentified doubt that should have been considered"). When defeaters describe doubt that is considered acceptable as residual doubt (without further argument), then they are marked as "residual" and contribute to the overall residual doubt associated with the case.

For an example of the EA notation, consider a case arguing that it will snow in Vancouver, Canada tomorrow shown in Figure 1. A strategy node (S0002) describes the argumentation strategy. The strategy has two child defeaters that challenge the top-level claim. D0003 suggests that there might be insufficient moisture to cause snow. The presence of a storm over the Pacific Ocean near Vancouver resolves this defeater (C0006). Two defeaters rebut this claim: it is possible that the wind will change direction (D0007), or the storm will not reach Vancouver (D0008). Further evidence (E0009 and E0012) is presented to resolve these defeaters. But each piece of evidence is undermined by additional doubt (D0010 and D0013). Neither of these undermining defeaters are resolved and therefore represent residual doubt in the case (annotated as "Res"). D0004 suggests that the temperature might not drop low enough to cause snow; however, this doubt is resolved by evidence (E0015) which is accepted without further doubt (annotated as "OK"). An inference rule (IR0005) relates the two defeaters (D0003 and D0004) to C0001. Defeater D0017 undercuts the rule by suggesting that it is unsound. Evidence E0018 is presented to resolve the undercutting defeater. The

[1] *In many cases it is not possible to completely eliminate doubt. This paper uses "resolve" to indicate that doubt is reduced to a low enough level that it is accepted as not significant enough to challenge the validity of the case.*

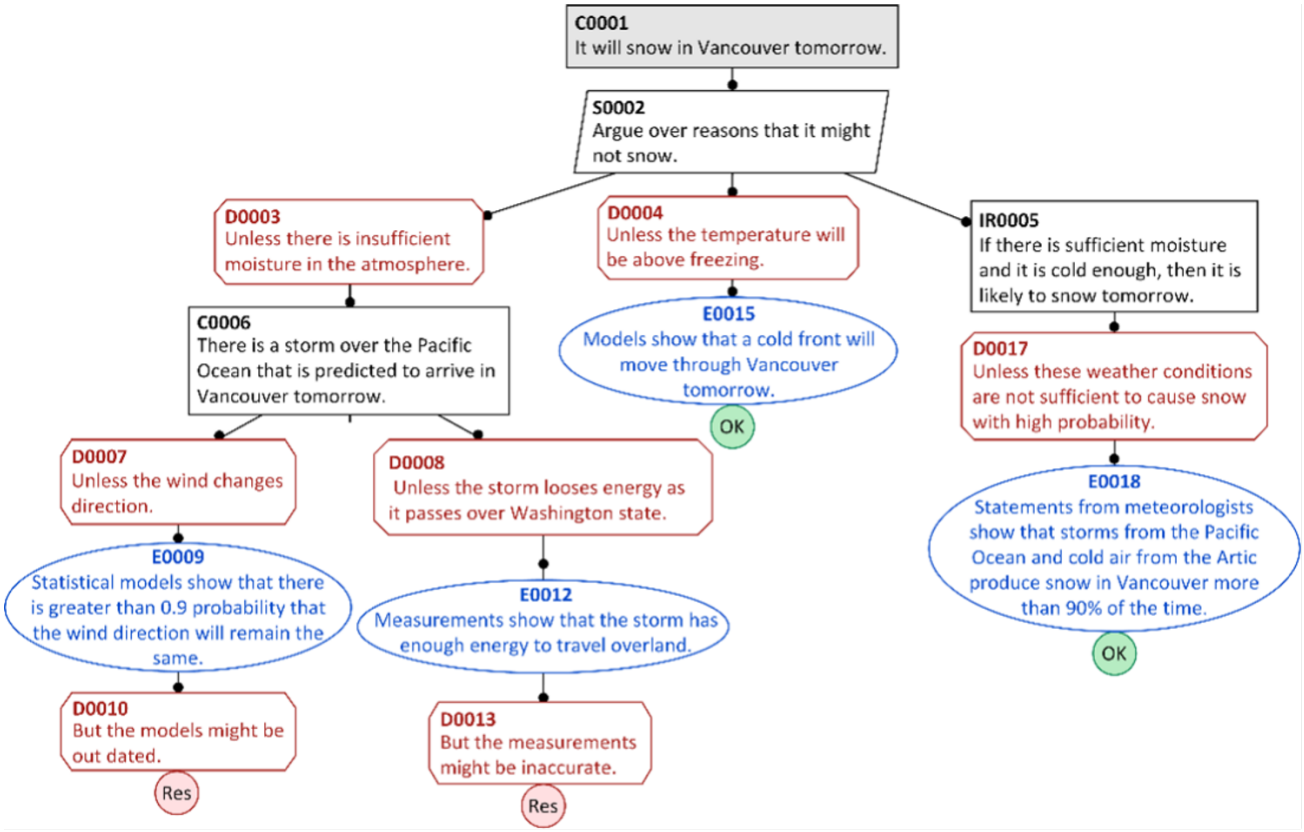


Figure 1: Sample EA case for arguing that it will snow in Vancouver.

EA notation also includes context, assumption, and undeveloped nodes, not shown in Figure 1[2].

INCREMENTAL ASSURANCE

In an EA assurance case, confidence in the top-level claim is established by showing that reasons to doubt the case have been resolved. Of course, it is difficult to eliminate doubt with absolute certainty. Instead, authors of assurance cases present enough evidence to give the reader sufficient confidence the doubt is resolved. This necessitates that the author (and in turn the reader) of the assurance case make a judgement about the level of confidence provided by each piece of evidence and the inference rule. Each piece of evidence added to the assurance case incrementally increases confidence that a doubt has been resolved and thus increases overall assurance in the system.

This notion of incremental assurance is implicitly used in functional safety standards such as IEC 61508, ISO 26262, DO-178C, and EN 50126. These standards employ a level-of-rigor approach whereby confidence in the safety integrity of a system is increased by prescribing more demanding engineering activities. For example, per ISO 26262 Part 6, for software assigned Automotive Safety Integrity Level (ASIL) A (lowest criticality) fault injection testing is recommended; however, for software assigned ASIL D (highest criticality) fault injection testing is a highly recommended activity. In other words, the level of assurance is incrementally increased as additional doubts are identified and resolved with appropriate evidence. Functional safety standards also prescribe the minimum criteria for accepting evidence as sufficient for the purpose of resolving implicit doubts about the safety of a system.

[2] *This example and others in this paper were prepared using Socrates – Assurance Case Editor, a web-based tool for collaborative assurance case development and maintenance that supports the EA and GSN notations. See https://safetycasepro.com for more information on the Socrates tool.*

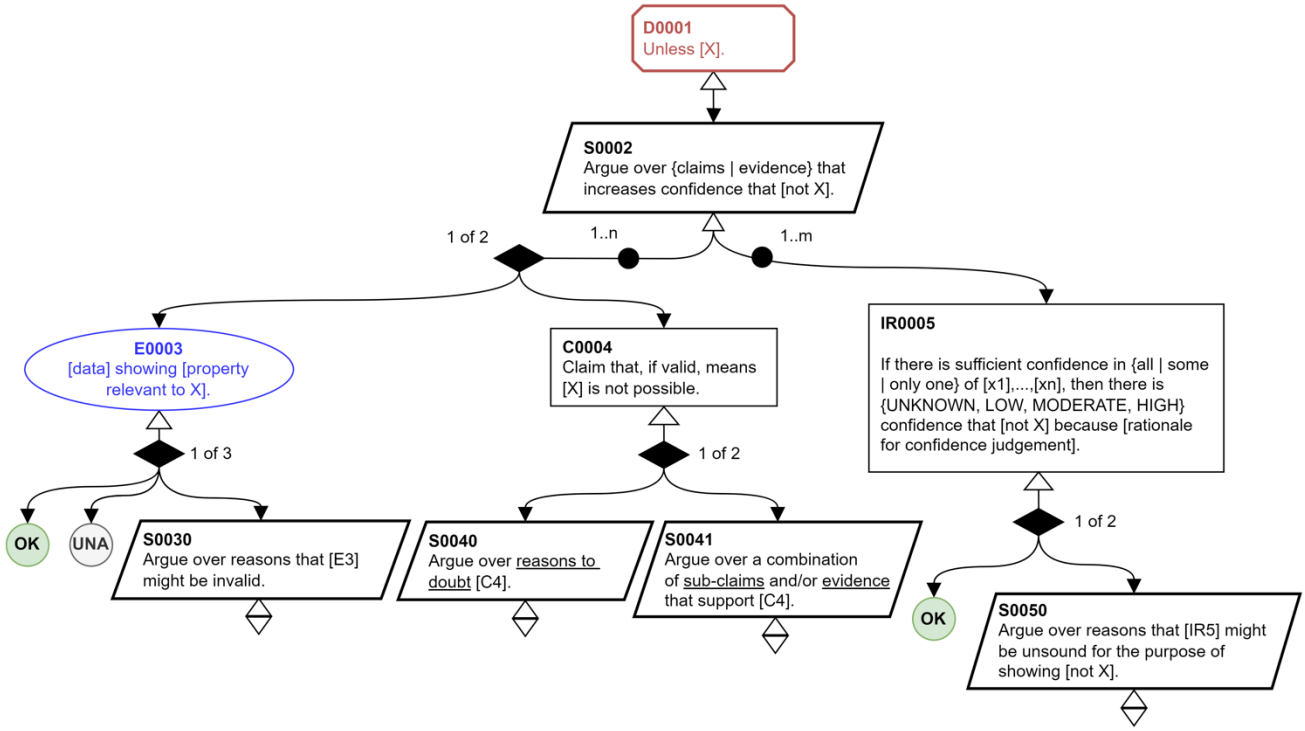


Figure 2: Specification of pattern for incremental assurance using Eliminative Argumentation.

This section presents the main contribution of this paper: an EA reasoning pattern for incremental assurance. While many assurance case patterns exist for GSN-style assurance cases (Kelly, 1998; Szczygielska & Jarzebowicz, 2017), to the authors knowledge, this is the first published pattern using EA. The pattern is a type of a "syntactic pattern" that describes how to correctly express the idea of incremental assurance using the EA notation. This kind of syntactic pattern differs in character from argumentation patterns that describe the system's function. The pattern explicitly describes how individual pieces of evidence, or claims that are ultimately supported by evidence, may be combined to achieve confidence that a defeater in an EA argument is resolved. An essential idea in the pattern is to explicitly describe a confidence calculation in an inference rule that gives the degree of confidence that the defeater is resolved.

The pattern for incremental assurance is depicted in Figure 2 using the pattern specification notation described in the 3rd Edition of the GSN Community Standard (Assurance Case Working Group, 2021). Additionally, within the pattern specification Figure 2 uses braces "{…}" to denote choices for the author and square braces "[…]" denote wording or values that should be populated when the pattern is instantiated. The wording in the pattern specification is generic: some adjustments to wording are required upon instantiation.

The pattern is rooted in a defeater (D0001) that describes a doubt [X] about an arbitrary parent node in the argument. The pattern is applicable regardless of whether the root defeater (D0001) is rebutting a parent claim, undermining evidence, or undercutting an inference rule. Following the style of EA, either claims or evidence (or both) may be presented against the root defeater. The rationale for combining the claims and evidence to address the root defeater is captured in one or more inference rules (IR0005). Critically, each inference rule describes the level of confidence that the root defeater is resolved when there is sufficient confidence in a combination of the claims (C0003) and evidence (E0004). Multiple inference rules should be used to express varying degrees of confidence that might arise from different combinations of claims/evidence; for example, see inference rules IR0026 and IR0034 in Figure 4.

The pattern uses a qualitative assessment of confidence with an ordinal scale: UNKNOWN confidence, LOW confidence, MODERATE confidence, or HIGH confidence. A qualitative

assessment is used (as opposed to a quantitative measure) since assessment of confidence arising from a combination of claims and evidence is typically the subject of engineering judgement based on project context, experience, and best practices described in technical standards, such as IEC 61508 and ISO 26262. When instantiating the pattern, the author(s) of the assurance case should provide a rationale for why a particular combination of claims and evidence gives the indicated level of confidence. The inference rule, though expressed in natural language, is in fact a confidence calculation that indicates how to propagate confidence through the assurance case's argument structure. The pattern depicted in Figure 2 gives a template for a simple instance of such a confidence calculation that requires a minimum number of evidence (or claims) be sufficiently substantiated. However, more sophisticated calculations are possible. In practice, if the calculation is too complex to fit within the confines of box in a diagram, it can be expressed in narrative text accompanying the assurance case.

The pattern specification in Figure 2 provides an opportunity to include further argumentation under the evidence (E0003), claim (C0004), or inference rule (IR0005). This is shown using strategy nodes (S0030, S0040, S0041, S0050) which provide "hooks" to continue to develop the argument structure using EA. Under the evidence (E0003), reasons to doubt the evidence may be captured as undermining defeaters (S0030). Under the claim (C0004), reasons to doubt the claim may be captured as rebutting defeaters (S0040) or supporting claims and evidence may be presented (S0041). Note that in Goodenough et al.'s original formulation of EA, claims could not be supported by sub-claims; however, in practice it is useful to be able to decompose a complex claim into sub-claims that can be more easily argued. Finally, there might be reasons to doubt the soundness of the inference rule used to combine the claims and evidence; these are expressed as undercutting defeaters (S0050).

In addition to evidence or claims advanced to resolve the defeater, it is possible that counter-evidence is available that strengthens the credibility of the defeater. For instance, reports from field trials of a software system might describe a particular misbehavior of the software that increases the credibility of the defeater. For a general discussion of counter-evidence in EA arguments see Goodenough et al.'s report on EA (Goodenough, Weinstock, & Klein, 2015). In the context of this pattern, counter-evidence may be included by presenting it as an instance of E0003 in the pattern and using an inference rule (IR0005) to indicate how the existence of the counter-evidence modifies the confidence that the root defeater (D0001) has been addressed.

In Figure 2, the inference rule (IR0005) indicates how to combine claims and evidence to address the root defeater. However, it depends on "sufficient confidence" (or some other criteria chosen by the author as part of their confidence calculation) being established in the validity of the rule's premises. The pattern requires the user to determine the level of confidence afforded to combinations of claims and evidence. In this regard, there are several cases to consider. First, the case where the evidence (E0003) is not available (marked as "UNA") or where the claim (C0004) is undeveloped is clearly insufficient. Second, the case where evidence (E0003) and/or a claim (C0004) has unaddressed defeaters indicating residual doubt associated with them is more difficult: how much residual doubt can be tolerated without changing the level of confidence indicated by the

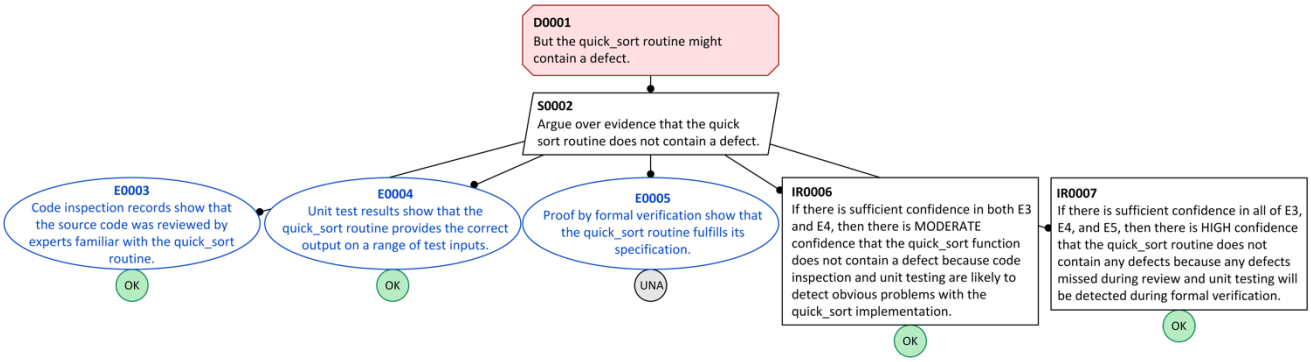


Figure 3: Example of pattern instantiation for a quick_sort routine.

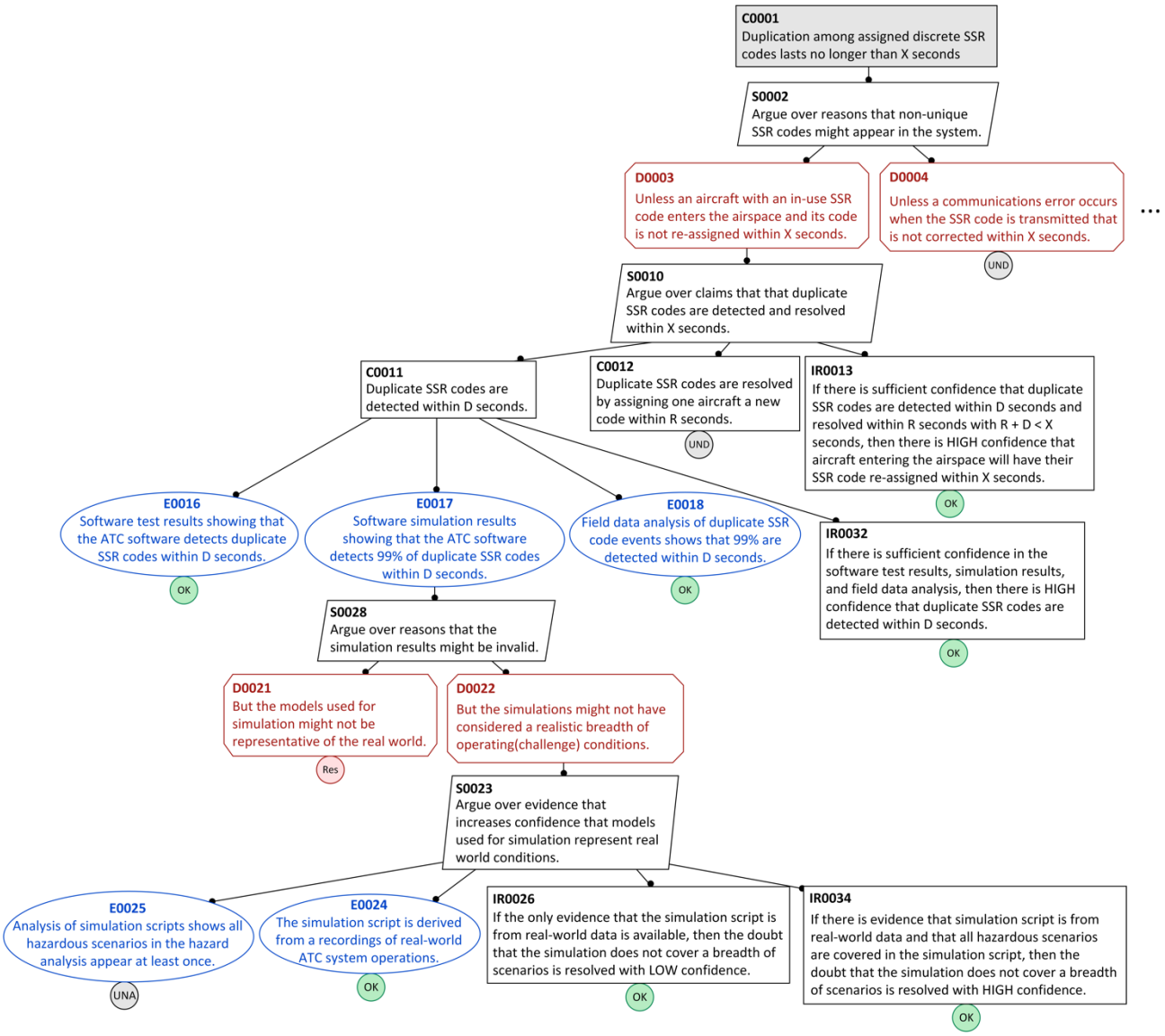


Figure 4: Example of applying the pattern to an air traffic control system.

inference rule (IR0005)? One might (somewhat naively) suggest that zero residual doubt is tolerable in the inference rule. However, in real-world systems there is almost always residual doubt that cannot be resolved, and it is therefore not practical for the pattern to demand zero residual doubt. The confidence calculation in the inference rule (IR0005) should incorporate the tolerable level of residual doubt in the claims and evidence advanced against the root defeater. Formalizing the calculation to combine varying degrees of confidence in the supporting claims and evidence is a topic of on-going research.

To illustrate the core idea(s) of incremental assurance, the pattern is instantiated as an argument fragment related to a quick_sort software routine, see in Figure 3. The root of the fragment is a defeater (D0001) describing a doubt that the software routine has a defect. Three pieces of evidence are proposed to address this defeater: code inspection records (E0003), unit test results (E0004), and a proof using formal verification techniques (E0005). The code inspection and unit test results are marked as "OK" indicating they are available and determined to be acceptable. However, the formal proof is marked as unavailable ("UNA"). Two inference rules (IR0006, IR0007) describe how to logically combine the evidence to address the root defeater, these are instances of IR0005 from Figure 2. These rules reflect

widely accepted software quality assurance practices. If there is sufficient confidence in the code inspection and unit testing then there is moderate confidence that the routine is defect free; however, there cannot be high confidence because testing and inspection cannot absolutely prove the absence of software defects (IR0006). If the formal proof is added, then confidence is increased (IR0007). In this example, since only the inspection and unit test results are available, the authors of the assurance case may conclude that the root defeater is addressed with moderate confidence. When a formal proof becomes available, then the level of confidence can be incrementally increased.

APPLICATION TO AN ASSURANCE CASE FOR AN AIR TRAFFIC CONTROL SYSTEM

The pattern for incremental assurance was applied to a fragment of an assurance argument for an air traffic control system. This application is motivated by direct experience with the development of a safety assurance case by Raytheon Canada for an air traffic management system delivered to Canada's air navigation services provider, Nav Canada. The argument fragment addresses duplicate discrete SSR code events that occur when a discrete SSR code, the unique identifier assigned to an aircraft by air traffic control, is used by more than one aircraft in the same airspace. Since the SSR code is used as a "primary key" by air traffic management software, duplication events could contribute to a hazardous loss of minimum separation distance between two aircraft (for example, a duplicate SSR code event could cause radar altitude data for one aircraft to displayed as the current altitude for a different aircraft).

In practice, duplicate SSR code events are not necessarily rare but should normally be resolved by air traffic controllers and pilots before they become serious concerns. The argument fragment in Figure 4 argues that discrete SSR codes assigned to aircraft in the controlled airspace are unique over a tolerable interval of X seconds (C0001). For illustrative purposes, two defeaters are advanced against this claim: aircraft arriving from another airspace might be using a code that is already in-use in the current airspace (D0003), or communication errors between controllers and pilots might contribute to duplication events (D0004); other reasons to doubt the top-level claim exist but are not listed for brevity.

Defeater D0003 and its descendants S0010, C0011, C0012, and IR0013 are the first instance of the pattern described above in Figure 2. In this instance, the possibility that an aircraft enters the airspace with a duplicate SSR code is addressed by a combined strategy of detecting the duplicate code (C0011) and resolving the duplication (C0012) within a duration of time that is less than the tolerable interval X. The inference rule shows that if this "detect and resolve" strategy is shown (by further argumentation) as valid with sufficient confidence, then there is high confidence that the duplicate SSR code events arising from incoming aircraft are resolved within a tolerable duration (IR0013). Further argumentation is provided for Claim C0011.

Claim C0011 is supported by three pieces of evidence: software test results (E0016), simulation results (E0017), and historical field data analysis (E0018). This evidence in combination with the inference rule (IR0032) forms a structure that is similar to the pattern. In particular, the inference rule (IR0032) describes how to combine the evidence (E0016-E0018) to support a parent (C0011). However, instead of establishing confidence that a doubt is resolved, this inference establishes confidence that Claim C0011 is valid. In turn, confidence in Claim C0011 resolves the parent defeater (D0003) via Inference Rule IR0013.

The simulation results described by Evidence E0017 are undermined by two additional defeaters: the models used for simulation might not represent the real-world system (D0021), and the simulation studies might not have covered a sufficient breadth of operational conditions (D0022). For this example, Defeater D0021 is left undeveloped. However, D0022 is addressed using another instance of the pattern for incremental assurance. In this instance, two additional pieces of evidence are listed. First, that Evidence E0024 says that simulation scripts are derived from real-world operations. Second, Evidence E0025 says that the simulation scripts cover the identified hazardous scenarios. Two inference rules are given that indicate how to combine these pieces of evidence together to assess the confidence that Defeater D0022 is resolved. According to the Inference Rule IR0026, if Evidence E0025 is not available, then there is at best "low confidence" that the simulations cover a range of scenarios. However, per Inference Rule IR0034, if a coverage analysis is available, then there is "high confidence" that Defeater D0022 is resolved.

In Figure 4, note that Evidence E0025 is marked as unavailable (UNA). Then only Inference Rule IR0024 applies and there is low confidence that the simulations cover a breadth of operating conditions (D0022). This low confidence in E0025 is propagated through the argument using the Inference Rules IR0032 and IR0013. Overall, even disregarding the undeveloped (UND) Claim C0012 and the residual (RES) Defeater D0021, it is concluded that Defeater D0003 cannot be resolved ("eliminated") with high confidence because there is not sufficient confidence in Claim C0011, i.e., that duplicate SSR codes are detected in a timely way.

CONCLUSION AND FUTURE WORK

Assurance cases are important engineering artifacts produced for safety and security-critical systems. As a system progresses through the lifecycle additional evidence may become available that increases confidence in the assurance case. This paper introduced the concept of "incremental assurance" in which the confidence in an assurance case, expressed using the Eliminative Argumentation method, is increased by providing additional evidence or argumentation that resolves doubts expressed as defeaters within the case. An essential idea is using inference rules to explicitly describe the change in confidence afforded by additional evidence or claims that a doubt is resolved. The concept of incremental assurance was described as an argumentation pattern, which is also the first pattern to employ the Eliminative Argumentation method. The pattern was illustrated by applying it to an argument fragment for an air traffic control system. Future work in this area will identify additional patterns for incremental assurance and extend the idea of confidence propagation using inference rules.

ACKNOWLEDGEMENTS

This material is based upon work funded and supported by Critical Systems Labs Inc. and the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

REFERENCES

[1] Assurance Case Working Group. (2021). Goal Structuring Notation Community Standard - Version 3. Safety-Critical Systems Club.

[2] Goodenough, J. B., Weinstock, C. B., & Klein, A. Z. (2015). Eliminative Argumentation: A Basis for Arguing Confidence in System Properties. Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University.

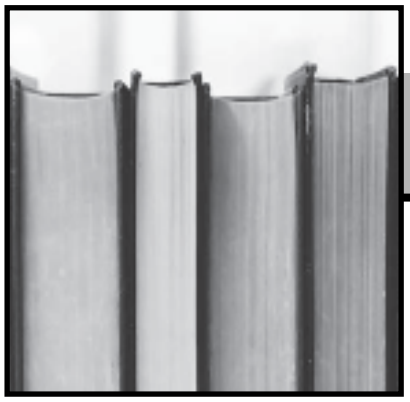
[3] Haddon-Cave, C. (2009). The Nimrod Review. London, UK: London Stationary Office.

[4] Kelly, T. P. (1998). Arguing safety - A Systematic Approach to Safety Case Management. University of York.

[5] Koopman, P., & Wagner, M. (2020). Positive Trust Balance for Self-driving Car Deployment. Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops. Springer. https://doi.org/10.1007/978-3-030-55583-2_26

[6] Szczygielska, M., Jarzebowicz, A. (2017). Assurance Case Patterns On-line Catalogue. Advances in Dependability Engineering of Complex Systems (pp. 407-417). Springer. https://doi.org/10.1007/978-3-319-59415-6_39

[7] Toulmin, S. E. (2003). The Uses of Argument. Cambridge University Press. https://doi.org/10.1017/CBO9780511840005



System Safety Bookshelf

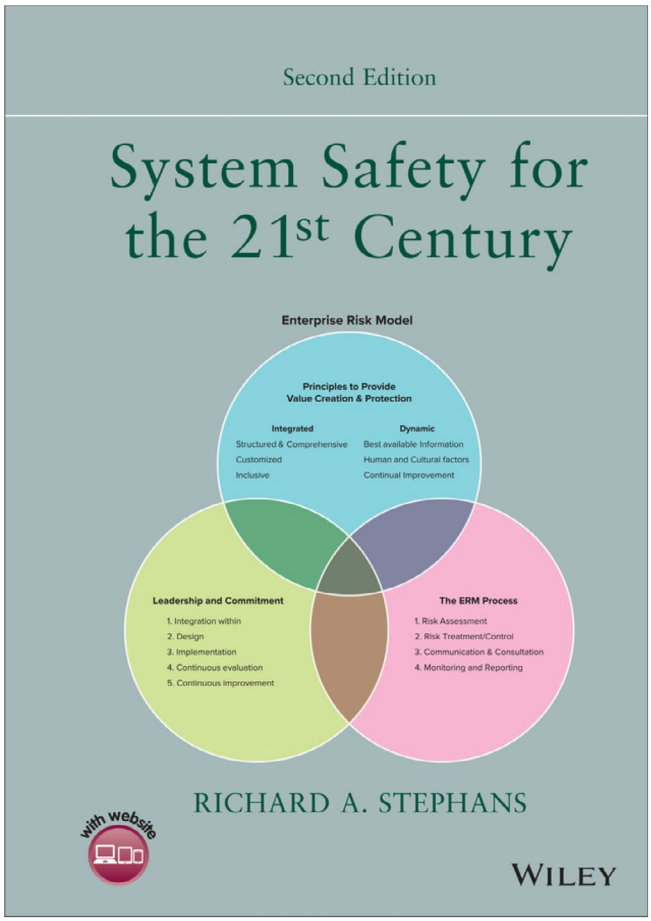
by Malcolm Jones

System Safety for the 21st Century

2nd Edition

Activities, processes and products are undertaken for a reason and that is for an overall benefit. However, all are subject to hazards and risk and there must be a constant process of looking for the correct benefit/risk balance – of course no activity, process or product is completely free from risk – or the concept zero risk. The comprehensive approach to achieving this desired balance sits under the heading of System Safety. So, what is it? It is the process and the set of support tools which enable one to minimise the hazards and detriments associated with the relevant activities. In order to accomplish this one must define the system and its boundaries and then to both identify the hazardous conditions that can arise within the boundary together with the threats that impinge on the system from outside of the boundary, and in addition, the threats to the environment emanating from inside of the boundary. In the former case they can arise from quality failures, including human reliability, and logic failures arising from 'as yet' not understood fault sequences. In the 'external case' they arise from failures such as poor training, environmental uncertainties and in the setting of incorrect policy and strategy. Over many decades System Safety has evolved from a more re-active nature - learning from failures and improving – not really suitable for high consequence enterprises - to today's more pro-active form. This is now based on better fundamental understanding, better assessment processes, better standards, more comprehensive analysis tools with better audit and regulation procedures. However, unlike 'set educational subjects' such as engineering, science, technology and mathematics, there are less opportunities for formal System Safety education and training in academia and elsewhere, even though system safety impacts on all aspects of life. One hopes that this will continue to be rectified.

This leads us directly to the importance and value of this book, which gives a complete insight into the nature of what System Safety is all about, including its approaches, methodologies and tools, and which provides guidance on the successful application of a comprehensive, pro-active approach for ensuring safe system design.



Richard A. Stephans
ISBN: 978-1-119-63475-1
Print | September 2022 | 416 Pages

This is a book that will prove valuable to all practitioners in System Safety, ranging from the experienced proponents who need reminding of the range of procedures and techniques available for tackling the challenges that lie in front of them, to the new practitioners who are about to embark on new and fruitful careers in this exciting and valuable field. The essential guide to start them soundly on their way. The book is written in a form whose preface directs the reader to the appropriated parts of the book to satisfy each category of interested recipient, whether safety manager, student or dedicated safety professionals. The original Edition of 2004 has now been updated to include important System Safety developments that have evolved since that time and as such, brings the subject up to date.

It is not the purpose of the book to delve into detail in all specific areas, follow on detail can be found from the supporting reference list, but rather it identifies in a comprehensive fashion the range of where and how System Safety can be applied. As such, it acts as the launching points for further detailed practitioner application on an as-needed custom basis.

Not only should System Safety be valued for its moral dimension, but a successful and well-structured safety culture is invaluable within the competitive environment which enterprises inhabit. For well-understood reasons, good safety represents a major attribute for enterprise brand and commercial success. At the extreme end lie enterprises where safety failure can be catastrophic and where the application of System Safety should be paramount. The author's valuable experience in these areas is reflected in the contents of the book.

The book also ventures into Artificial Intelligence aspects of System Safety, but this is restricted to health aspects. Of course, we are now seeing a burgeoning of AI in many other areas of System Safety, coupled with associated concerns about its probabilistic rather than deterministic relationship between cause and effect, when applied to high consequence enterprises.

The author has many decades of experience in hands-on successful application of System Safety in a wide range of areas and is a member of a cadre of pioneers in the US who established the concept of the System Safety profession, and which eventually founded what has become the International System Safety Society. He was a prominent member of that evolution and has continued to play a significant role in its subsequent developments, both in leadership and educator roles. He is a Co-Editor of the Society's "System Safety Analysis Handbook". The author was very familiar with the System Safety challenges that engineers faced in those early days and his direct involvement and experience has enabled him to clearly highlight the System Safety development history in the book. This 2nd edition brings us up to date with modern approaches. The author has also capitalised on this experience in relation to his role as an educator, and this is again reflected in the style of the book and of course in its associated Instructor Manual, which forms part of this review. The Manual gives comprehensive advice on how an Educator can best develop teaching courses by way of best structuring and ordering of chapter coverage. Each chapter in turn has an associated set of questions to best support student learning through enabling a deeper and more reflective

> "The book covers the whole range of System Safety from system concept through to disposal and along the way covering all aspects of risk management, control processes, accident analysis and sound design principles."

Photo: Pexels

understanding of contents of each chapter.

The author's System Safety fund of knowledge and experience is founded in his extensive career in US DOD, DOE and environmental restoration programmes. For this reason, the book inevitably has a strong US slant, for example with its references to US aviation, DOE, DOD, NASA, EPA, OSHA and the US nuclear industries. As such, its contents may not be immediately familiar to an international audience. For example, in the UK, where system safety activities are based around Relevant Good Practice, Joint Service Publications and the Ministry of Defence requirements for an enveloping Formal Safety Case, with its emphasis on demonstrating that the risk is As Low as Reasonably Practicable (ALARP). The latter being a legal requirement in the UK. Nevertheless, from a general perspective, the book's contents will be familiar, understood and applicable internationally. After all, the processes of System Safety including its problems, techniques, procedures and requirements are somewhat common the world over. For this reason, the book will not suffer from this national bias base.

The book covers the whole range of System Safety from system concept through to disposal and along the way covering all aspects of risk management, control processes, accident analysis and sound design principles. This is complemented with a comprehensive range of risk analysis tools and procedures, with examples of application given to set the reader in the right direction. Perhaps one approach that is not covered is the Systems -Theoretic Accident Model and Processes (STAMP) methodology advocated by Nancy Leveson of MIT.

This revised edition now includes a section on the value of System Safety in hospital health care and management, together with the general medical field, reminding the reader of how wide-ranging is the application of System Safety. We are all now very well aware of its value in the field of infection control given the recent/current Corona virus pandemic.

The book contains an extensive list of references, again mainly of a US nature, for those who require to delve in more depth into the various processes and tools of System Safety. One to note is the 1997 Edition of the System Safety Analysis Handbook, Second Edition, St Pauls MN, Published by the International System Safety Society.

In summary, System Safety practitioners within whatever areas and level of business they occupy; technical, management, medical, educational, would surely benefit from having this on their bookshelf and the associated Instructor Manual a must for the latter category.

Reviewed by - Malcolm Jones, BSc, PhD, C. Eng, C. Phys, F. int P, MBE, a long time Fellow of the International System Safety Society. He is a Physicist by training and has more than 50 years of experience in safety in the UK's nuclear Industry, within which he still plays an active role. During his career he has gained a number of National and International awards, including the International Systems Safety Society's development award for lifetime contributions to the development of the System Safety process.

Original Article
https://doi.org10.56094/jss.v58i1.216

International System Safety Society

www.jsystemsafety.com

Journal of System Safety

Established 1965 Vol. 58 No. 1 (2023)

The Difficulties with Replacing Crew Launch Abort Systems with Designed Reliability

Shaun R. Ryan[ab]

[a] *Corresponding author email: shaun.r.ryan@lmco.com*
[b] *Lockheed Martin Space; Sunnyvale, California, USA*

Keywords
launch, crew, abort, human spaceflight

Peer-Reviewed
Gold Open Access
Zero APC Fees

Online: 22-Feb-2023

Cite As:
Ryan S., The Difficulties with Replacing Crew Launch Abort Systems with Designed Reliability. Journal of System Safety. 2022;58(1):19-24. https://doi.org10.56094/jss.v58i1.216

ABSTRACT

As the space industry continues to innovate and new paradigms arise to challenge the status quo, human spaceflight is now perceived as safer and more accessible than ever before. This has led to a new line of thinking in which crewed launch vehicles should be reusable and reliable like commercial airplanes, forgoing the need for an abort system. This paper will counter that line of thought with an analysis of the spectrum of coverage historical crew abort systems provided during launch and use historical data from launch rate successes and failures to glean insight into what reliability in the human spaceflight industry can expect when designing the vehicles of the future. This historical launch vehicle reliability will then be compared to system safety standards used in the commercial aviation industry to understand if future designs truly need a crew abort system. Through this analysis, the rationale for why these crew abort systems have historically been used can be better understood.

INTRODUCTION

While a lot of attention is focused on performance and capabilities of launch vehicles, crew launch abort systems are often overlooked. While maybe not as flashy as tonnage to low earth orbit or pushing boundaries with complex combustion cycles, crew safety is critically important in human spaceflight. The danger of human spaceflight is not isolated to the vacuum of space but extends down to the ascent phase as well. The earliest crew abort systems on launch vehicles used aircraft-derived ejection seats. Featured in the Gemini and Vostok programs, ejection seats have a very limited window of effectiveness. They must be deployed at an altitude high enough for the parachutes to fully unfurl, which renders them ineffective for pre-launch aborts and for the first few seconds of flight. Additionally, once launch vehicle speeds and aerodynamic forces become too great, the ejection itself could result in loss of crew. Subsequent programs like Mercury, Soyuz, and Apollo transitioned to the use of crew launch abort systems using rocket motors attached to the capsules. These designs leveraged the pre-existing reentry functionality of crew capsules, repurposing them for a suborbital return. With this design philosophy,

rocket motors affixed to the capsule would quickly accelerate the crew away in the event of launch vehicle failure. Once a sufficient distance is reached, reentry devices such as parachutes would deploy to land the crew capsule. This system has the advantage that it is designed to be used on the pad as well as on ascent, propelling the capsule to a sufficient altitude for parachute deployment in the event of an on pad failure. This design philosophy is still used today on the Orion, Starliner, and Crew Dragon capsules.

APOLLO CREW LAUNCH ABORT COVERAGE

A good example of the coverage that a crew launch abort system can give can be found in the system used on the Apollo missions. The ascent phase of the mission was considered an especially dangerous part of the mission (Lyndon B. Johnson Space Center [JSC], 1972), so a great deal of planning went into their crew launch abort scenarios. The four main ascent related abort modes considered for the mission are shown in Figure 1 below.

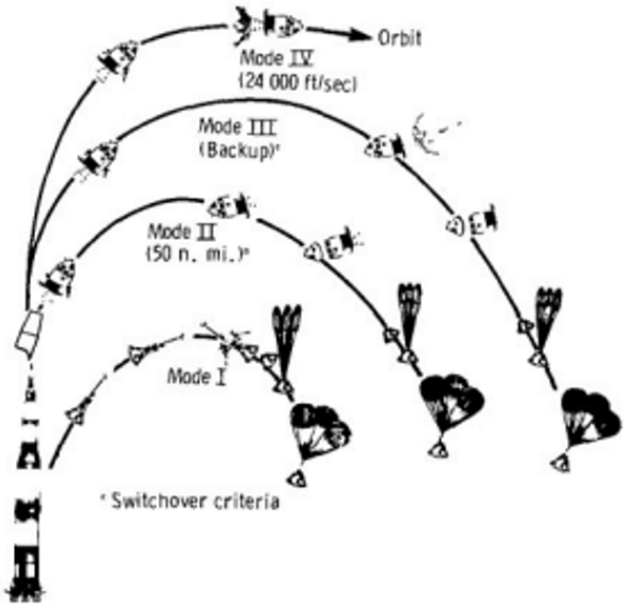


Figure 1: Apollo Abort Modes (JSC, 1972)

The first mode, or Mode I, was used for the major atmospheric phases of the flight. It was armed before launch to cover any pre-launch failures of the launch vehicle, with the vehicle fully loaded with propellants and after the crew boarded the command service module (Marshall Space Flight Center [MSFC], 1969). This mode lasted until the first few minutes in flight, at which the launch escape tower was jettisoned. If activated during this phase, the command module would separate from the service module as the launch escape tower fires. Once a safe distance away, the parachutes would fire, and the command module would hopefully land somewhere along the ground track (depending on when it was activated).

The second mode, Mode II, covers the phase of ascent after the highest atmospheric loads are experienced. Occurring after launch escape tower jettison, this mode relies on the traditional separation of the command service module and launch vehicle. After separation the command service module would maneuver itself clear of the launch vehicle and orient itself for landing. The service module would be jettisoned, and the command service module would return on a suborbital trajectory.

The third mode, Mode III, is a contingency mode used to prevent the command module from a land landing as the capsule was only designed to safely land on water. This would be executed in a similar way as the second mode, but with an additional retrograde burn by the command service module to constrain its down range landing to a pre-designated site (JSC, 1975).

The fourth mode, Mode IV, is essentially an abort to orbit. Once far enough along in its flight but still on a suborbital trajectory, an additional burn from the launch vehicle or service module would be performed to boost the command service module into orbit. Once in orbit a landing site could be designated and a return from orbit would be performed.

This crew abort plan was envisioned to provide the maximum possible coverage for all phases of the ascent. While never required to be used, it shows a great example on how to mitigate against a catastrophic failure of a launch vehicle.

THE SPACE SHUTTLE

The Space Shuttle program marked a major shift in design philosophy, with a new emphasis on reusability (Jones, 2018). The shuttle was a launch system consisting of a reusable space-plane based orbiter, a large expendable external tank, and two refurbishable solid rocket boosters (John F. Kennedy Space Center [KSC], 2022). This mindset shift also

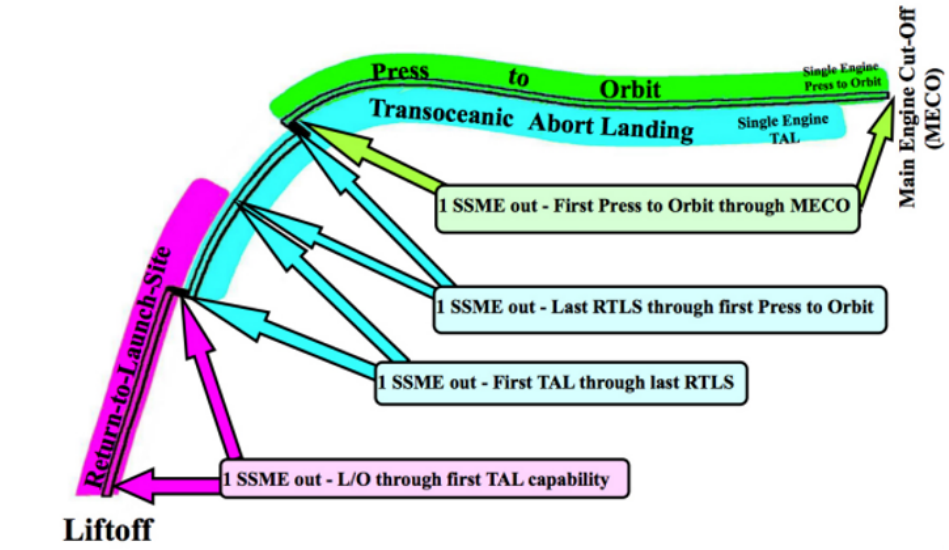


Figure 2: Space Shuttle Abort Modes (Henderson et al., 2011)

affected the crew launch abort planning for the shuttle. There was a new focus on robustness of the system which NASA thought could reduce the need for a crew launch abort system (Henderson & Nguyen, 2011). Instead, the in-flight abort scenarios utilized the intact orbiter for coverage throughout ascent profiled in Figure 2.

The first major mode is the Return to Launch Site (RTLS) abort. RTLS involves pitching the orbiter around to decrease down range trajectory. The burn is continued after the pitch around to give the shuttle extra velocity to enable a glide back to the launch site. The orbiter is then pitched down so that the external tank can be safely detached. The shuttle then performs its final unpowered glide back to the landing strip at the launch site. This abort mode is active from solid rocket booster separation until it is too far downrange to successfully glide back.

The second major mode is Trans-oceanic Abort Landing (TAL), in which the shuttle lands in pre-selected runways in Europe or Africa. For TAL, the ascent profile would remain very similar to a nominal launch, except with an earlier Main Engine Cutoff (MECO). The external tank would be separated in a way to minimize the risk of debris from a tank rupture impacting the orbiter. Then the orbiter would glide to a landing site.

The third major mode is an Abort to Orbit (ATO) in which the shuttle would continue to press on and achieve a stable orbit. Then the orbiter could select a more favorable landing time and location. Additionally, there is a small window for an Abort Once Around (AOA) in between modes. In a contingency AOA scenario, the shuttle would achieve just high enough velocity to make it once around the earth to then land back in the continental United States.

All these scenarios were developed for if one of the space shuttle's main engines were out. The picture of this abort plan becomes more clear when you look at the pre-Challenger contingency abort scenarios in Figure 3.

For the shuttle, contingency abort scenarios are for when two-out-of-three or three-out-of-three of the main engines are out. It is here that we can see the black out zones that are created when there is a catastrophic failure with the shuttle. While these focus on main engine out scenarios, Figure 3 makes it more clear that any major failures that occur in the solid rocket boosters would most certainly result in a loss of the crew, like what we tragically saw with Challenger in 1986. The shuttle design offered no protections for the crew in the event of launch vehicle destruction on the pad. In a stark difference to the Apollo philosophy, the shuttle attempted to design away the need for a crew launch abort system

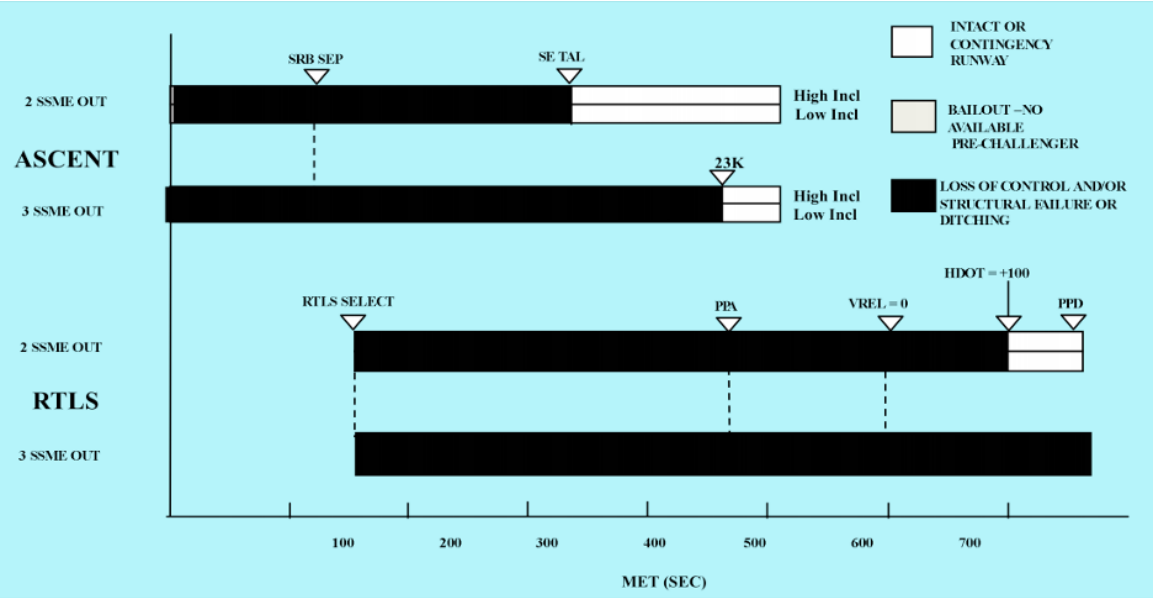


Figure 3: Pre 1986 Shuttle Contingency Aborts (Henderson et al., 2011)

assuming their vehicle was like a commercial airliner and their attempt failed (Jones, 2018).

REAL WORLD RELIABILITY OF LAUNCH VEHICLES

While there have since been technological advancements since the shuttle was designed, it is useful to look at the data from historical launch vehicles. This can be used to give a little insight into the human spaceflight industry and how it has performed. Using data from incidents and close calls in crewed space launches, a rough reliability of launch vehicles can be shown. For this paper the word reliability is being used in a general sense, divorced from probabilistic calculations. Below is a table of close calls and incidents that occurred during launch and ascent, sourced from NASA data with a focus on aborts and loss of crew/mission.

As of the writing of this paper, Soyuz has conducted 147 crewed launches and 3 resulted in aborts. This gives it a very rough reliability of about 99.97%, not taking into account uncrewed launches. For the shuttle's 135 launches and 2 ascent related incidents it gets a back of the envelope calculation at 99.99%. These two "reliability" numbers show how often an abort system was used to save the crew or crew was lost without such a system in place. While these numbers definitely don't tell a complete story, they will be useful to keep in mind as a basis of comparison. For an outside example, ULA calculated their reliability of the Atlas V 401 to prevent loss of crew as 99.96% (Patton & Barr, 2009). This value

Table 1: Close Calls and Incidents (JSC, 2019)

Mission	Incident/Close Call
STS-51L	Combustion gas leak in the solid rocket motor resulted in vehicle destruction. Loss of crew.
Soyuz T-10-1	Fuel spill ignited the launch vehicle while on the pad. Crew abort system activated. Crew saved
STS-51F	Faulty sensors resulted in premature engine shutdown and forced an Abort to Orbit. Auto-shutdown of second engine overridden to ensure AOA succeeded. Crew saved.
Soyuz 18-1	First stage failed to separate cleanly, and the vehicle was sent off course. Crew launch abort system activated. Crew saved.
Soyuz MS-10	Collision of boosters during staging resulted in destruction of the second stage. Crew abort system activated. Crew saved.

Probability (Quantitative)	Per flight hour 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable	Improbable		Extremely Improbable
	JAA	Frequent / Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor	Major	Severe Major	Catastrophic
	JAA	Minor	Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	• slight reduction in safety margins • slight increase in crew workload • some inconvenience to occupants	• significant reduction in safety margins or functional capabilities • significant increase In crew workload or in conditions impairing crew efficiency • some discomfort to occupants	• large reduction in safety margins or functional capabilities • higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely • adverse effects upon occupants	• all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D	Level C	Level B	Level A

Figure 4: Failure Severity as Related to Probability Objectives (SAE International, 1996)

shows that the oversimplified method above still falls within the range of numbers calculated using more traditional and robust reliability analysis.

RISK BASED ON AIRCRAFT STANDARDS

When new crewed space launch vehicle concepts are designed without crew launch abort systems, the comparison to commercial aviation is often made. The claim is that launch vehicle technology has sufficiently advanced enough that a risk posture similar to aviation can be adopted. In order to examine this claim, it is important to understand the thresholds that the aviation industry has adopted.

SAE's ARP 4761 is the de facto standard for System Safety in commercial aircraft design and manufacturing. In Figure 4 we can see that the probability objective for a catastrophic hazard in an aircraft is 1.0E-9, or 1 in a billion chance of occurrence per flight hour. To accurately gauge how the Soyuz and Shuttle compare to this, the previously calculated reliability should be normalized per each launch vehicle's ascent time for an ISS mission. The ascent times tend to be short, with the Soyuz at 0.15 hours (National Aeronautics and Space Administration [NASA], 2010), the Shuttle at 0.14 hours (NASA, 2007), and the Atlas V 401 at 0.20 hours (United Launch Alliance [ULA], 2022). If you take the ascent time for the vehicles and multiply by their total number of launches you can get a total hours accumulated per vehicle. Using the very simple formula below (eq. 1), the resulting launch vehicle normalized probability per flight hour objectives can be seen in Table 2.

$$\frac{(100 - Calculated\ Reliability)/100}{Cumulative\ Flight\ Hours} = Adjusted\ Probability\ Per\ Flight\ Hour \quad (eq1)$$

In this case, the Adjusted Probability Per Hour represents the probability a catastrophic event occurs that could result in loss of the crew per every flight hour. So for every flight hour, each of the launch vehicles would need to have a catastrophic failure less than the probabilities in Figure 4. The calculated Adjusted Probabilities Per Hour for the crewed launch vehicles do not compare favorably to the ARP 4761

Table 2: Adjusted Probability Per Ascent

Vehicle	Calculated Reliability	Ascent time (Hours)	Total Crewed Launches	Cumulative Flight Hours	Adjusted Probability Per Hour
Soyuz	99.97%	0.15	147	22.05	1.4E-5
Shuttle	99.99%	0.14	135	18.90	5.3E-5
Atlas V 401	99.96%* *From ULA	0.20	40* *No Crewed Launches to date so uncrewed used as a stand-in	8.00	5.0E-5

probability objectives for catastrophic hazards. The Soyuz comes in at the best with a probability of 3 in 200000. Then it is the Atlas V 401 with a probability of 1 in 20000. Lastly is the Shuttle with a probability of 53 in 1000000. These far exceed the probability thresholds for a catastrophic hazard by a significant margin.

These calculations are highly dependent on the data set used as well as an oversimplified definition of reliability. However, they remain useful as a litmus test between the commercial aviation and crewed spaceflight industries.

CONCLUSION

Crew launch abort systems are still a much-needed mitigation against launch vehicle failures in today's space industry environment. Crewed launch vehicles still have a way to go to meet commercial aircraft levels of reliability. The probability objectives from aviation system safety standards are a useful yardstick to measure how far vehicles have to go moving forward. Additionally, programs from the past can show us the risks we are assuming by leaving large black zones in crew launch abort capabilities. There is still a long road ahead before crew launch abort systems should be eliminated from designs.

REFERENCES

[1] Lyndon B. Johnson Space Center. (1972). Apollo Experience Report - Abort Planning. (Hyle, Foggatt, & Weber.) Retrieved from https://ntrs.nasa.gov/api/citations/19720017278/downloads/19720017278.pdf

[2] Marshall Space Flight Center. (1969). Saturn V Flight Manual SA-507. Retrieved from https://history.nasa.gov/afj/ap12fj/pdf/a12_sa507-flightmanual.pdf

[3] Lyndon B. Johnson Space Center. (1975). Apollo-Soyuz Test Project Recovery Requirements JSC-09436. Retrieved from https://history.nasa.gov/astp/documents/Astp-recoveryreq.pdf

[4] Jones, H. W. (2018). NASA's Understanding of Risk in Apollo and Shuttle. 2018 AIAA SPACE and Astronautics Forum and Exposition. https://doi.org/10.2514/6.2018-5235

[5] John F Kennedy Space Center. Space Shuttle Era Facts. Retrieved 2022, from https://www.nasa.gov/pdf/566250main_SHUTTLE%20ERA%20FACTS_040412.pdf

[6] Henderson, E. M. and Nguyen, T. X. (2011) Space Shuttle Abort Evolution. AIAA SPACE 2011 Conference & Exposition. https://doi.org/10.2514/6.2011-7245

[7] Lyndon B. Johnson Space Center. (2019) Significant Incidents & Close Calls in Human Spaceflight. Retrieved 2022, from https://sma.nasa.gov/SignificantIncidents/

[8] Patton, J. A. and Barr, J. D. (2009). Atlas and Delta Capabilities to Launch Crew to Low Earth Orbit. AIAA SPACE 2009 Conference & Exposition. https://doi.org/10.2514/6.2009-6729

[9] SAE International. (1996). GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT (ARP4761). https://www.sae.org/standards/content/arp4761/

[10] National Aeronautics and Space Administration. (2010). Soyuz Launch Overview and Timeline. Retrieved 2022, from https://www.nasa.gov/mission_pages/station/structure/elements/soyuz/timeline_overview.html

[11] National Aeronautics and Space Administration. (2007). STS-121: Ask the Mission Team - Question and Answer Session. Retrieved 2022, from https://www.nasa.gov/mission_pages/shuttle/shuttlemissions/sts121/launch/qa-leinbach.html#:~:text=It%20takes%20the%20shuttle%20approximately,8%2D1%2F2%20minutes

[12] United Launch Alliance. (2022). Atlas V to Launch Starliner OFT-2. Retrieved 2022, from https://www.ulalaunch.com/missions/next-launch/atlas-v-starliner-oft-2

Original Article
https://doi.org10.56094/jss.v58i1.217

International System Safety Society

www.jsystemsafety.com

Journal of System Safety

Established 1965 Vol. 58 No. 1 (2023)

Quantification of Benefits for Medical Devices

Bijan Elahi[ab]

[a] *Corresponding author email: bijan@medtechsafety.com*
[b] *MedTech Safety, Sarasota, FL, USA*

Keywords
medical device, patient safety, FDA, quantification

Peer-Reviewed
Gold Open Access
Zero APC Fees

Online: 22-Feb-2023

Cite As:
Elahi B., Quantification of Benefits for Medical Devices. Journal of System Safety. 2023;58(1):25-28. https://doi.org10.56094/jss.v58i1.217

ABSTRACT

One of the most prominent challenges in safety risk management of medical devices is the Benefit-Risk Analysis. This paper proposes a methodology to quantify benefits, thereby creating more consistency, and explainability in the evaluation of benefits and the benefit/risk ratio.

Leveraging the guidance from the FDA, we define four Dimensions for appraising benefits. The product of the rankings of a benefit in all four Dimensions is used as a quantitative measure of a benefit.

The quantitative score for the overall benefit of a medical device would be the sum of the scores of the individual benefits.

INTRODUCTION

One of the most prominent challenges in safety risk management of medical devices is the Benefit-Risk Analysis. EU MDR refers to reducing risks as far as possible without adversely affecting the benefit/risk ratio. Computation of the benefit/risk ratio necessitates numerical values in the numerator and the denominator. We have techniques to quantitatively compute risks, but benefits are not typically quantified. Therefore, estimation of the benefit/risk ratio has been merely a subjective opinion.

This paper proposes a methodology to quantify benefits, thereby creating more consistency, and explainability in the evaluation of benefits and the benefit/risk ratio.

A further advantage of quantification of benefits is the ability to more objectively compare the benefits of two comparable products, which could be successive generations of the same product, or competitive products.

Leveraging the guidance from the FDA (2012), we define four Dimensions for appraising benefits. The product of the rankings of a benefit in all four

Dimensions is used as a quantitative measure of a benefit.

The quantitative score for the overall benefit of a medical device would be the sum of the scores of the individual benefits.

BACKGROUND

Benefit is defined in ISO 14971:2019 as: "positive impact or desirable outcome of the use of a medical device on the health of an individual, or a positive impact on patient management or public health". There is also Note 1 to entry that says: "Benefits can include positive impact on clinical outcome, the patient's quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or positive impact on public health."

The FDA has released several guidances on Benefit-Risk analysis for PMA, De Novo, and 501(k) devices. In these guidances the FDA puts forth four factors for assessing the extent of a benefit:

A. Type of benefit
B. Magnitude of the benefit
C. Probability of the patient experiencing the benefit
D. Duration of the effect (benefit)

In this paper we leverage these four factors to quantify the extent of a benefit.

It is noteworthy that the perspective of the FDA guidances considers devices that provide therapeutic benefits to patients, while there are many other types of medical devices that do not provide therapeutic benefits, such as surgical tools and sterilizers. As such, in this paper the definitions of each FDA factor have been extended within the four specified Dimensions, to encompass the non-therapeutic medical devices as well.

SOLUTION DESCRIPTION

Using the 2-step method described below, we compute a numerical score for each benefit.

STEP 1

Leveraging the FDA Guidance, we define 4 Dimensions A-D for the evaluation of each benefit of a medical device.

Dimension A – Type of Benefit

Rank each benefit based on the type of benefit, as defined in Table 1 below. The rankings imply the degree of importance.

For accessories to a medical device, where the accessory makes it possible for the medical device to deliver its intended function, the accessory inherits the medical device's benefit type.

Table 1: Type of Benefit

Rank	Description of Benefit Type	Examples
1	Simplifying care Clinical Efficiency - Ease of Patient Care - Convenience | basic protection | Improved hygiene | Simple diagnostics	wound protection (bandages); maintaining antiseptic practices (surgical gloves); oral health (toothbrush); blood pressure measurement (sphygmomanometer)
2	Relief from symptoms (basic)| facilitating delivery of care to patients	pain reduction (Transcutaneous Electrical Nerve Stimulation); palliative care (pain pump); facilitating surgeries (reusable surgical instruments); medical imaging (diagnostic X-ray)
3	Relief from symptoms (advanced) | Improvement of impaired body function	infusion of analgesics (infusion pumps); pain relief (SCS); alignment of vertebrae (vertebral fixation)
4	Life-extending benefit – reduced probability of mortality| Restoration of body function | minimally invasive interventions | Advanced diagnostics	identification of the genes responsible for breast cancer; opening of arterial lesions (stents); minimally invasive surgery (surgical robot)
5	Life-Critical benefits – loss of benefit could cause serious injury or death	restoration of normal cardiac rhythm (ICD), cranial navigation (SW); breathing support (ventilator)
6	Sustaining life – loss of benefit would result in immediate death	circulating blood in the body (artificial heart), oxygenating and circulating blood (cardiopulmonary bypass machine)

Table 2: Magnitude of Benefit

Rank	Description	Examples
1	Small benefit | < 50% improvement | low impact on patient care	wound protection (bandages), maintaining antiseptic practices (surgical gloves), enabling mobility for handicapped persons (wheelchair)
2	Medium benefit | 50-80% improvement | moderate impact on patient care	stabilizing the knee (external knee joint brace), staples (Surgical staplers); cardiac mapping (electro anatomic mapping)
3	Large benefit | > 80% improvement | high impact on patient care	infusion of analgesics (infusion pumps); defibrillator; sterilization (autoclave);

Dimension B – Magnitude of Benefit

Rank each benefit on the scale in Table 2 above. Assume all the benefit is received, as intended. For example, a TENS (Transcutaneous Electrical Nerve Stimulation) device at best, offers temporary pain relief – it's not a cure. A clinician might rank the magnitude of its benefit a 1 or a 2.

Note that magnitude of a benefit is independent of its type. For example, a bandage that is used on a wound to prevent bleeding and infection maybe a type 1 but have a magnitude 3 benefit.

For devices that do not directly provide a therapeutic benefit, e.g., surgical instruments, navigation, or diagnostic devices, estimate the impact of the benefit on patient care.

Dimension C – Probability of Receiving the Benefit

Rank each benefit on the scale in Table 3 below.

Guidance

For therapeutic benefits, the Clinical Evaluation would be a good source of information for Dimension C ranking.

The probability of receiving benefit for an individual can be computed as the ratio of A/B, where A = the number of people who have received the benefit, and B = the number of people who have received the therapy. In many cases the decision as to who received the benefit is not so clear. For example, a Spinal Cord Stimulator (SCS) may provide significant pain relief to some, but moderate/low pain relief to others. In such cases, a threshold of benefit can be defined and thus people who receive at least that much benefit would be counted in the A group.

In some cases, the probability of receiving the benefit could be estimated for a whole population, as the ratio of C/D, where C = the estimated number of people in a population (e.g., a country) who would receive the therapy, and D = the estimated number of the people in that population who could benefit from the therapy (e.g., people with the relevant medical condition). This would treat the accessibility of a therapy in a given population as a public health benefit.

For devices that do not directly provide a therapeutic benefit, e.g., surgical instruments, navigation, or diagnostic devices, use the reliability/specificity estimates.

Table 3: Probability of Receiving the Benefit

Rank	Description
1	Small | < 50% of the users/patients are expected to receive the benefit | reliability <80%
2	Medium | 50-80% of the users/patients are expected to receive the benefit | reliability 80-95%
3	Large | > 80% of the users/patients are expected to receive the benefit | reliability > 95%

Table 4: Duration of the Benefit

Rank	Description
1	Short duration of benefit | Short device lifetime
2	Medium duration of benefit | Medium device lifetime
3	Long duration of benefit | Long device lifetime

Dimension D – Duration of the Benefit

Rank each benefit on the scale in Table 4 above, based on the expected duration of the benefit.

Guidance

For therapeutic benefits, the Clinical Evaluation would be a good source of this information.

For devices that do not directly provide a therapeutic benefit, e.g., surgical instruments, navigation, or diagnostic devices, use the device lifetime as compared to the user need. For example, if three models of a reusable medical device can be used 5, 20, and 50 times, they would be ranked 1, 2, and 3 respectively.

STEP 2

Compute the benefit score by multiplying the rankings of each benefit along the four Dimensions. Example:

Device X has the following ranking:

- Dimension A – 5
- Dimension B – 3
- Dimension C – 2
- Dimension D – 3

The benefit score = 5 x 3 x 2 x 3 = 90

DISCUSSION

Although the rankings in the four Dimensions are mostly subjective, and partially based on factual clinical data, this method yields a more objective way of appraising a benefit. This method is especially beneficial when comparing the relative value of the same benefit over the progressive iterations of the same device. Or, when comparing the benefits of competitive devices.

The quantitative score for the overall benefit of a medical device would be the sum of the scores of the individual benefits, as identified in the Clinical Evaluation Report.

It should be noted that this whitepaper presents a framework for the quantification of benefits of medical devices. This framework can be adapted to best suit the needs of the manufacturers. For instance, by modifying the descriptions in the tables provided for each Dimension, or by increasing/decreasing the granularity of the rankings in each Dimension.

NORMALIZATION OF BENEFITS

There have been attempts, e.g., by Chung, et. al. (2022) to normalize the quantified values of benefits vs. the quantified values of risks. Normalization of benefits vs. risks affords the ability to compute a benefit/risk ratio where if value of the fraction is > 1, one could claim that the benefits outweigh the risks. No attempt is made in this paper, to normalize benefits vs. risks. The presented approach computes a score for benefits, independent of risks. Therefore, the ratio of benefit/risk would result in a value that would be compared against predetermined acceptance criteria. This is very similar to RPN computation and usage in Failure Modes and Effects Analyses (FMEA).

FUTURE WORK

REFINEMENT

Depending on the uncertainty on the estimates in rankings withing the four Dimensions, we may assign a correction factor to attenuate a computed benefit score.

Conversely, if a benefit meets an important unmet need, we may assign a correction factor to amplify a computed benefit score.

REFERENCES

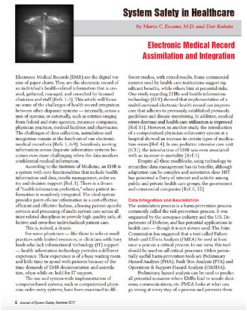
[1] US Food and Drug Administration. Factors to consider when making benefit-risk determinations in medical device premarket approval and de novo classifications. Issued March. 2012.

[2] Chung, B., Kutty, J., Benefit-Risk Determination: A Quantitative Approach, March 2022, , RQM+, Retrieved from www.rqmplus.com

From the JSS Archives

Effective April 2022, JSS announced that it was transitioning to a Gold Open Access publishing model, and we launched our new website at jsystemsafety.com.

To date we have published eight years (2014-2022) of our back issues to the new website. We ultimately plan to republish the entire 57 year archive! This page highlights a few of the many articles currently available in our archives.

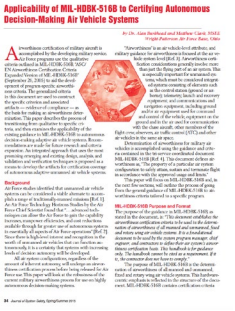

System Safety in Healthcare

Electronic Medical Record Assimilation and Integration

System Safety In Healthcare

Dev Raheja

This long-running column examines healthcare and patient safety from a system safety perspective.


Applicability of MIL-HDBK-516B to Certifying Autonomous Decision-Making Air Vehicle Systems

Applicability of MIL-HDBK-516B to Certifying Autonomous Decision-Making Air Vehicle Systems

Alan Burkhard
Matthew A. Clark

An integrated approach for airworthiness certification.


Augmenting a Hazard Analysis Method with Error Propagation Information for Safety-Critical Systems

Augmenting a Hazard Analysis Method with Error Propagation Information for Safety-Critical Systems

Fryad Rashid
John D. McGregor

This paper explores potential effects of residual hazards in the operational system context.


A Review of Functional Safety Models for Public Safety Management Systems

A Review of Functional Safety Models for Public Safety Management Systems

S. B. Aanandh et al

Review and comparison of safety models, including causal, systemic, and cognitive models.

System Safety On Demand

Past Webinars Available On Demand

Challenges and Potential Benefits of AI to Software Safety Assurance

Model-based Systems Engineering or System Safety: An Introduction

Occupational Hazard and Risk Management Techniques

Requirements Analysis using Karnaugh Maps

International System Safety Society Chapter Contacts

ASIA PACIFIC
Singapore Chapter
Eng Ling Onn
011-65-9632-6256
onnel@stengg.com

CANADA
Tony Zenga
514-825-7845
tzenga@cmtigroup.com

UNITED STATES OF AMERICA

ALABAMA/TENNESSEE/MISSISSIPPI
Tennessee Valley Chapter
Tim Browning
tbrowning@apt-research.com

ARIZONA
Saguaro Chapter
Adam Hughes
978-852-8053
ahughes3245@gmail.com

CALIFORNIA
Bay Area Chapter
Graham Murray
408-756-2674
Graham.t.murray@lmco.com

Central California Chapter
Miguel Trujillo
805-606-1533
Miguel_trujillo@yahoo.com

Sierra High Desert Chapter
Glen McCue
760-939-3531
glen.s.mccue.civ@us.navy.mil

Southern California Chapter
Francis McDougall
310-653-1309
Francis.mcdougall@us.af.mil

MAINE/NEW HAMPSHIRE/VERMONT/MASSACHUSETTS/RHODE ISLAND/CONNECTICUT/PENNSYLVANIA/NEW YORK/NEW JERSEY
Northeast Chapter
John Hewitt
203-522-3974
john.e.hewitt@lmco.com

NEW MEXICO
Stacey Durham
riparian77@hotmail.com

TEXAS
North Texas Chapter
Tom Haeussler
505-284-9748
Thomas.a.haeussler@lmco.com

VIRGINA/MARYLAND/DELAWARE
Washington DC
Chapter
John Burchett
301-744-2307
john.burchett@navy.mil

VIRTUAL CHAPTER
Doanna Weissgerber
831-278-0800
Doanna@pacbell.net

RVP ASIA PACIFIC
Eng Ling Onn
(Singapore)
011-65-9632-6256
onnel@stengg.com

RVP EUROPE
Gabriele Schedl
(Austria)
43 (1)811-50-2758
gabriele.schedl@frequentis.com

Mark Your Calendar

Activities

Through its local chapters, committees, executive council, publications and meetings, the Society provides many opportunities for interested members to participate in a va-riety of activities compatible with Society objectives. In addition to the basic operating committees, Society activities include several noteworthy publications and events.

Publications

- Journal of System Safety is the official Society journal. Published three times a year, JSS is a peer-reviewd scholarly journal that keeps members informed of the latest developments in the field of system safety.
- Chapter newsletters are published periodically to disseminate news of chapter activities and items of interest to chapter members.
- Proceedings of Society-sponsored conferences and symposia are made available to members at a special discount.

Meetings — Conferences — Symposia

- International System Safety Conferences are sponsored annually. These conferences have proven to be a very popular and effective means for highlighting the latest techniques, applications and social/legal aspects of system safety.
- Mini-symposia are sponsored by local chapters to provide an in-depth exploration of a specific system safety-related topic.
- Chapter dinner meetings, field trips and panel discussions are held at intervals throughout the year.
- The Society is a co-sponsor of various system safety-related symposia and conferences.

Membership in the Society is open to all persons having an interest in or currently involved in work related to system safety or an allied discipline. Professional member-ship grades are available for those able to demonstrate sufficient qualifications, experi-ence and training. Annual dues are $150 (USD), while student memberships are free. Society members and subscribers are located in all areas of the United States and many countries around the world:

Australia
Austria
Cameroon
Canada
Chile
China
France
Germany
Greece
Israel
Italy
Japan
Netherlands
Nigeria
Norway
Russia
Saudi Arabia
Singapore
South Aftrica
Spain
Sweden
Switzerland
United Kingdom
(England, Northern Ireland, Scotland and Wales)
United Arab Emirates
United States of America

Requests for membership applications, subscription orders, requests for Conference Proceedings and other matters related to membership and services should be addressed to the International System Safety Society, 1000 Westgate Dr., Suite 252, Saint Paul, MN 55114, or contactsystemsafety@system-safety.org. Visit our Website at http://www.system-safety.org.

The **International System Safety Society** is a non-profit organization of professionals dedicated to the safety of systems, products and services through the effective implementation of the system safety concept. Under this concept, appropriate technical and managerial skills are applied so that a systematic, forward-looking hazard identification and control function becomes an integral part of a project, program or activity at the planning phase and continues through the design, production, testing, use and disposal phases.

The Society's Objectives

- To advance the art and science of system safety
- To promote a meaningful management and technological understanding of system safety
- To disseminate advances in knowledge to all interested groups and individuals
- To further the development of the professionals engaged in system safety
- To improve public understanding of the system safety discipline
- To improve the communication of system safety principles to all levels of management, engineering and other professional groups

International System Safety Society

Professionals Dedicated to the Safety of Systems, Products and Services

International System Safety Society
1000 Westgate Dr, Suite 252
Saint Paul, MN 55114

Society Website: https://www.system-safety.org
Journal Website: https://www.jsystemsafety.com