

# A SAFETY CONUNDRUM ILLUSTRATED: LOGIC, MATHEMATICS, AND SCIENCE ARE NOT ENOUGH

C.M. Holloway\*, C.W. Johnson<sup>†</sup>, K.R. Collins<sup>‡</sup>

\*NASA Langley Research Center, 100 NASA Road, Hampton VA, 23681-2199, USA, c.m.holloway@nasa.gov

<sup>†</sup>Dept. Of Computing Science, University of Glasgow, Glasgow, G12 9QQ, UK, johnson@cs.gla.ac.uk

<sup>‡</sup>Dept. of Computer Science, 151 Engineer's Way, University of Virginia, Charlottesville VA, 22904, USA, krc2p@virginia.edu

**Keywords:** safety, argument, evidence, logic, fiction.

## Abstract

In an ideal world, conversations about whether a particular system is safe, or whether a particular method or tool enhances safety, would be emotion-free discussions concentrating on the level of safety required, available evidence, and coherent logical, mathematical, or scientific arguments based on that evidence. In the real world, discussions about safety are often not emotion-free. Political and economic arguments may play a bigger role than logical, mathematical, and scientific arguments, and psychological factors may be as important, or even more important, than purely technical factors. This paper illustrates the conundrum that can result from this clash of the ideal and the real by means of an imagined conversation among a collection of fictional characters representing various types of people who may be participating in a safety discussion.

## 1 Introduction

In an ideal world, conversations about whether a particular system is safe, or whether a particular method or tool enhances safety, would be emotion-free discussions concentrating on the level of safety required, available evidence, and coherent logical, mathematical, or scientific arguments based on that evidence. A quick perusal of a safety-critical systems e-mail list, a few minutes sitting in a standards creating committee, a hour or two attending a system safety conference, or a day participating in a safety review meeting are enough to demonstrate conclusively that the real world is often far from ideal.

In real world discussions about safety, emotions often flow freely; opinions, anecdotes, and pronouncements from experts may substitute for evidence; and political and economic arguments may play a bigger role than logical, mathematical, and scientific arguments. Psychological factors such as emotion, mood, and affect may be as important as, or even more important than, purely technical factors.

To illustrate the conundrum that can result from this clash of the ideal and the real, and to reduce the likelihood that anyone will be directly offended, this paper is written as a conversation among a collection of fictional characters. Although the conversation is realistic (so much so that

probably every system safety researcher or practitioner reading this paper will be able to identify with it), the people, organizations, products, and standards mentioned in the paper are entirely fictional. Any resemblance to real people (living or dead), organizations (operating or defunct, private or public sector), or products (sold or discontinued) is purely coincidental; any resemblance to real standards is not coincidental.

The rest of the paper is organized as follows: Section 2 introduces the fictional conversation; Sections 3-6 contain the conversation itself; and Section 7 presents suggestions about how the conversation might be used fruitfully by system safety researchers and practitioners.

## 2 Background

This section introduces the characters that participate in the fictional safety discussion, the context in which that discussion takes place, and the format in which it is presented.

### 2.1 The Players

Six characters constitute the cast.

- Samantha (called Sam by her friends, and those who instinctively shorten any name that can be shortened): a brilliant, conscientious, humble engineer whose sole professional goal is to advance the state-of-the-practice in system safety engineering. She is an independent consultant.
- Lawrence (never called Larry even by his few friends): a brilliant, ambitious, egotistical academic researcher at Yafordton University, one of the world's most highly respected universities. His sole professional goal is to insure the adoption of his tools and methods throughout the world, not because he is unethical, but because he has convinced himself that they are the best tools and methods available.
- Martin: a hard-working, but not particularly intelligent, engineering manager in whose hands rests the final decisions about the tools, methods, and standards to be used on safety-critical systems developed by his employer, Only the Best Products (OBP). Most everyone thinks Martin believes everything that Lawrence says, but Martin denies it.

- Isadora: a senior researcher at SLG (Safety Laboratory of the Government), a government research laboratory that has sponsored much of Lawrence's work. Many people think she harbours resentment towards him because of negative comments he frequently makes about the competence of SLG researchers.

- Jill: a former graduate student of Lawrence's; now an important member of the international committee revising the IRV-36 standard, which is applied widely across the world in several industries to safety-critical software systems. She continues to respect Lawrence's intellect and accomplishments, but no longer considers him to be infallible; she works for OBP's chief competitor, Really the Best, Incorporated (RBI).

- Calvin: a first year graduate student at a local university. He is attending his first system safety conference in hopes of getting ideas for thesis research topics.

## 2.2 The Setting

These six people find themselves sitting together at a lunch table during the second day of an international system safety conference. After a bit of idle chit-chat, the conversation turns more serious.

## 2.3 The Format

The remaining sections of the paper present the fictional conversation. The name is given whenever the speaker changes. Quotation marks are omitted. Non-spoken actions or clarifying remarks are denoted by *italics*.

## 3 The Conversation: Act I

Lawrence: Enough about kids, cats, and other drivel. Let's talk about something important to us all. *He turns his attention towards Jill.* What I want to know is if there's a chance, Jill, that you people are going to get it right this time. What do you think?

Jill (*looking perplexed*): I think I don't know what you are talking about.

Lawrence: Sure you do. I'm asking if you think that the standards committee you're on is going to fix the mess it made last time with IRV-36.

Isadora: Oh, come on, Lawrence, what do you expect her to say: 'No, we're trying to keep it a mess?'

Jill: Well, if you think the current version is bad, I don't think you're going to be thrilled with the revision. We aren't making any radical changes. There's no reason to — it works.

Lawrence (*clucking his tongue*): How can you say it works!?! You've read my technical criticisms! You know everyone thinks it costs industry millions!

Martin: That's the truth. If we didn't have to comply with 36, we could save a ton of money.

Samantha: I hear that all the time, but I've never seen any data to substantiate the claim.

Martin: It's not like we're going to show the world our financial records.

Isadora: Nope, OBP won't even let us, a government research lab, see anything when we're willing to keep the data private and sanitize it so we can try to get a handle on what's really going on. And, of course, it's not just OBP, RBI won't do it, either, nor will any of the other companies.

Samantha: Even if you did get the data somehow, it wouldn't necessarily mean anything. Suppose companies *are* spending a whole lot of money complying with IRV-36. How do we know that this is money that wouldn't have to be spent to make a system sufficiently safe anyway, even if there wasn't IRV-36?

Lawrence (*rolling his eyes, and looking quite thoroughly disgusted*): I don't know you, Sam, and apparently you don't know my work. If you did, you'd know that I've shown how to prove systems safe in ways that aren't even mentioned in 36, and they're so simple and easy to use no one can doubt they'd be cheaper.

Jill: Despite what you think, Lawrence, just because you write something doesn't make it true. In the real world, most of us want to see some data, not just accept pronouncements from ivory towers. Unless I'm mistaken, no system is out there being used by the public that was developed using your methods. There are hundreds, perhaps thousands, of real systems with subsystems or components that were created following IRV-36. There's yet to be an accident to a single one of those systems that's been attributed to a 36-compliant subsystem.

Samantha: Right, that's the point. Following the standard works. Perhaps it costs a whole lot to follow it — although I'd still not be convinced of that — but so what? Better safe than sorry.

Martin: That's easy for you to say, Samantha, since you're a consultant. Much of the money we spend goes to people like you to help us comply with the standard. I'd be astonished if you wanted anything to change.

Samantha (*with a pained expression*): Hey ...

Martin: Sorry, that wasn't really fair. ... I just think there are too many safety people who act like money doesn't matter, and that any mention of cost is somehow unethical.

Jill (*trying to alleviate some of the tension*): It's not that thinking about money is unethical, but it essentially comes down to what is more important: safety or money? A good

engineer will try to ensure safety first. Both are important concerns for the engineer, so I do agree with you there Martin.

Samantha: I agree with Jill. Talking about costs isn't unethical, it's important. I just think that without any real data to substantiate claims of something costing too much, and with real data about safety, the only wise thing to do is to stay with what's gotten us there.

Lawrence: Sammy, Sammy, Sammy, I taught you better. Just because systems built to comply with IRV-36 end up being safe — and I'm not conceding that's even true — does not mean that IRV-36 had anything to do with it. They could be safe **despite** the standard.

Isadora: I **could** be an alien from Alpha Centauri, too, but I think we're all better off assuming I'm not. Same thing here. It may be theoretically possible that IRV-36 has nothing to do with the safety of the systems, but since it's about the only thing common across a wide spectrum of systems, we're better off assuming it has something to do with it.

Samantha: Isadora's right, Lawrence. The data doesn't **prove** that following 36 guarantees safety, but it is consistent with that being the case. And we have no data to the contrary.

Lawrence: Ah, but we have something better than data: formal proofs. I've proven in several papers that it is possible to satisfy some of the requirements in 36 without truly accomplishing what those requirements claim to accomplish. It doesn't catch everything. So the standard is deficient. Q.E.D. We don't need data to know it.

Jill: No one is claiming that the standard is perfect. I wouldn't be on the revision committee if I thought it was perfect. Sure, it has deficiencies. But it has been used for over a decade, and, as I've said before, there has yet to be an accident. That says a lot more about the standard than your so-called proofs ever could.

Calvin (*hesitantly*): Um ... sorry to jump in here ...

Isadora: Don't be sorry, you've got as much right as any of us to talk.

*Lawrence frowns, but does not say anything.*

Calvin: OK .... thanks. I'm a bit confused. (*Looking at Jill*) Are you saying that formal proofs don't have any value?

Jill: No, no, that's not what I'm saying at all.

Calvin: Phew. I was worried about what to say to my advisor when I get back to school. He's big on formal methods. So, what are you saying?

Jill: Formal proofs, model-checking, all that stuff can have real value when used properly. Some of my clients have

found problems using formal methods that would've been really hard to find any other way. I wasn't making a general criticism, just a specific criticism of Lawrence giving more weight to his proofs than to the operational data that's out there.

Isadora (*looking at Lawrence*): Is that what you really think Lawrence? Do you really think we should disregard the evidence, because it contradicts your analysis?

Lawrence: Of course not. Don't be silly. I'm surprised that you (*pointing at Isadora*) could even ask such a question. I'm all for evidence, and a scientific foundation for all that we do. That's what my career has been all about.

*At this point, the main course for lunch is served, so the conversation at the table quiets down, not quite to silence, but to nothing more than polite banter.*

## 4 The Conversation: Act II

*As people finish up their lunches, Martin is the first one to steer the conversation back to technical topics.*

Martin: So, before the food came, Lawrence had said that his career was all about building a scientific foundation for what we do. That's how I've always seen it. (*A tiny grin crosses Lawrence's face.*) But I'm not sure we've made any real progress (*The grin disappears*).

Isadora: What do you mean?

Martin: Well, take my company for example. We're building this new product. I can't tell you anything about it, 'cause we've not announced it to the public yet, and I'd get fired if I let something slip that Jill could take back to RBI. But the details aren't important anyway, just that it has major safety issues: if it works right it could save lives, but if it works wrong it could kill people. ... (*Martin pauses to take a sip of water*) ... I'm asking my people the same questions about this product as I've been asking them for 20 years, and they're giving me the same answers. Same thing happens between me and my bosses. It's hard to see any progress.

Jill: What sorts of questions? And, no, I'm not asking you to spill any company secrets.

Martin: Stuff like this ... We did a preliminary hazard analysis, and came up with some catastrophic hazards. How do we know we identified them all? We assigned likelihoods to those hazards occurring, using the same combination of historic data, calculations, and engineering judgement we always use. How do we know we didn't get it wrong?

Lawrence: My ...

Isadora (*interrupting*): Yeah, we know, your tools would answer those questions.

Lawrence: Actually, that's not what I was going to say. I was going to say that my tools *might help* answer those questions.

Martin: Right. That's the point. Your tools, or someone else's tools, *might help*. You don't really know. Yet, if we had a solid scientific foundation, we ought to *know* whether they'd help. Bridge builders don't sit around wondering whether some piece of cable is strong enough to hold the weight it's supposed to hold. They know.

Samantha: Let's not give bridge builders too much credit. Bridges fall down, you know. Remember Tacoma-Narrows and Minneapolis?

Jill: True, but still, Martin has a point. Civil engineers have a lot more universally accepted techniques and standards to rely on than we do.

Isadora: Sure, but civil engineering has been around for a very long time. Even if the name is only a few hundred years old, no one can tell me that the Egyptians didn't do some civil engineering when they built the pyramids. Or the Romans with their roads and aqueducts.

Lawrence: Can we get back to Martin's situation? I'm not sure I get your point. Are you saying that the systems we build today aren't any safer than the ones we built in the past?

Martin: Not really. Sure, some things have gotten safer. If I got in an accident in my car twenty years ago, I'd probably get killed. Today, I might not even get a scratch. But I'm not sure any of this has come about because system safety engineering is on any firmer foundation now than it was in the past.

Isadora: I tend to agree. Shoot, there are some papers being presented here this year that could've been presented at the first one of these conferences back before Calvin here was even born.

Samantha (*looking at Martin*): I want to get back to the product you can't tell us anything about for a moment. And maybe this isn't really a fair question to ask you. If it isn't don't answer. But are you really concerned that OBP is going to start selling a product that isn't as safe as it could be?

Lawrence: Before he answers, I think we need to make that question more precise. As stated, the answer has to be yes. Every product ever sold could've been made safer. There are always more hazards that could be eliminated. We could completely get rid of the risk of mid-air collisions by only allowing one plane in the sky at a time.

Samantha (*giving Lawrence a look of mild disgust*): I think everyone knows what I meant, but I'll rephrase the question for the benefit of pedants like you. Martin, are you concerned that your company may start selling this new product before you're confident that it is as safe as reasonably practicable?

Martin: You're right; it isn't really a fair question.

Samantha: Then don't answer it.

Martin: That's okay. The answer is sort of 'yes and no'. I don't worry that we will intentionally start selling the product knowing that it has dangers in it that we could've fixed if we'd tried. No one in my company would do such a thing, and if they tried, I'd blow the whistle without a second thought. ...

Jill (*during Martin's pause*): Just for the record, I feel the same way about RBI, and I'd blow the whistle, too, if it turned out I was wrong.

Martin: What does worry me ... it even keeps me up at nights some times ... is that we might miss a hazard, ... or think that it's extremely improbable to occur when it's not, ... or, ... and this is probably my biggest worry, we might decide to spend more money mitigating one particular hazard and less on another, when the second hazard turns out to be the one that bites someone. We just don't know enough to be sure we won't do those things.

Lawrence (*jokingly*): You just need to hire smarter people, Martin.

Isadora (*not recognizing the joke*): Not everyone is a genius like you, Larry.

*At this point, the Conference Chair comes to the microphone to make various announcements about the afternoon and evening events, while the servers collect the entree plates, and distribute dessert.*

## 5 The Conversation: Act III

*After the Chair sits down, Calvin speaks up.*

Calvin: Mind if the newbie asks another question? (*Hearing no objections, he continues.*) All of you seem to be committed to doing the best you can in your jobs, yet you seem to disagree on some rather basic things. Like whether the standard that's the most widely used --- I think that's right, isn't it, IRV-26 ...

Jill: 36. IRV-36. It is the most widely used.

Calvin: Thanks, sorry. Yeah. You can't even agree on whether IRV-36 is a good standard or not. Here's my question. Why do you all think that is? Why can't you agree? I'd like to hear what each of you thinks, if that's okay.

Isadora: That's a great question, Calvin.

Lawrence (*looking at Isadora*): So, are you going to answer it?

Isadora: Sure, but why don't you go first?

Lawrence: Gladly. I don't think the standard is any good, for the reasons I've stated in my papers. But you're not really interested in what we think about the standard so much as why we think reasonably intelligent people would disagree about it.

Calvin: Right.

Lawrence: I think we disagree, because some people do not fully understand the relative merit of different types of evidence. So, you have people like Jill here, who is a really smart woman by the way (*He smiles and nods in Jill's general direction*), who don't realize that formal, logical, rigorously defined evidence — like my proofs — should carry more weight than empirical evidence. It's not her fault, really. The education system failed her. By the time she came to me as a graduate student, it was too late. Think about the legal system, we still have jurors who give more weight to eyewitness testimony and circumstantial evidence than they do to DNA. It's preposterous but they do. For system safety, the closest thing we have to DNA is formal analysis. But not everyone understands that.

Jill: I agree with Lawrence's basic premise: different understandings of the relative merit of different types of evidence are at the root. I even like his legal system analogy. Where I disagree is where the various types of evidence available in system safety fit within the analogy. I think that can vary from system to system, and even from parts of a system to other parts of a system. For some things, formal analysis may be the analogue to DNA, but for others, it may deserve no more weight than a demonstratively unreliable eyewitness. Lawrence is a brilliant man, but I don't think he really comprehends the complexity of the real world.

Samantha: I was planning to say something entirely different, but it is hard to not to follow the lead of those two. (*She pauses briefly, glancing at Jill and then Lawrence*). I, too, think the root of the disagreements rests in relative merit of evidence. When it comes to the specific issue of whether IRV-36 is a good standard or not, the theorist in me wants to say that it isn't, for many of the same reasons that Lawrence explained in his papers. But the practical side of me can't get past the fact that all of the operational evidence out there that seems to say that it is, at worst, not so bad.

Martin: There's a little more to it than just differences about relative merit of types of evidence. We could agree about relative merit, and still disagree about how to interpret a particular piece of evidence. For IRV-36, I think interpretation is the biggest cause of differences. Even among people who give no weight to Lawrence's criticisms, which is just about everyone I know by the way, there are sharp disagreements about whether the accident-freeness of systems developed with 36 really means anything. And despite the scepticism of some of the rest of you here, I still think there's something to the claims that it costs too much.

Isadora: Wow. I've not really given the question enough thought to have a good answer for you, Calvin. But what the rest of you have said has been much more interesting than anything I've heard in the conference sessions so far. I think some of the things that we've discussed here could be great areas for research. I'm going to look into getting something going at SLG.

*As Isadora finishes talking, the Conference Chair tells everyone it is time to head to the next sessions.*

## 6 The Conversation: Epilogue

*As people get up from the table to go their separate ways, Calvin taps Samantha on the shoulder, and speaks to her quietly.*

Calvin: Is it always like this?

Samantha: What do you mean?

Calvin: Bickering, sniping, talking past one another, stuff like that ... does it happen all the time?

Samantha (*laughing*): No, not all the time. Mostly just at meetings like this one. When people get down to doing real work, they're usually quite reasonable ... even Lawrence ... occasionally.

Calvin (*relieved*): That's good to know. I was starting to wonder if I ought to get into some other field. It got better near the end, 'though. Everyone seemed to take my question seriously.

Samantha (*seriously*): It was a great question. We really need bright young people like you working in the field. Safety isn't glamorous, and not many people strike it rich ensuring systems are safe, but there aren't a whole lot of things you could do that are more important.

## 7 Using the Paper

We conclude by suggesting three ways that system safety researchers and practitioners may be able to use this paper.

One use is to stimulate personal introspection by considering questions such as these: Which character comes closest to matching your beliefs and opinions about system safety issues? Which character comes closest to matching your attitudes towards others in the field? What might the positive and negative aspects of that character reveal about your own positives and negatives? Knowing your own biases might help you facilitate constructive dialog among your peers.

Another use is to stimulate group discussions. Potential topics for discussion based on the conversation include the following: the proper role of standards compliance in ensuring and assuring safety; how to combine formal and informal arguments; how personal attitudes and demeanor

may affect technical disagreements; the relevant merit and interpretation of different types of evidence; how much progress has been made in the field over the last few decades; and what can be learned from other disciplines about evaluating arguments and evidence.

The third way that system safety professionals may consider using this paper is to promote the importance of constructive dialog within the profession. As an informal reviewer of the first draft of this paper said, perhaps the most fictitious aspect of the paper is that, in the end, the characters are generally cordial with one another. Too often within the system safety community, particularly within the research community, disagreements are not discussed cordially, and more effort seems to be devoted to tearing down the work of others than in advancing the field cooperatively. We hope that this paper contributes a bit towards changing this unproductive tendency.

## **Acknowledgements**

Funding for K.R. Collins participation was provided by the National Aeronautics and Space Administration's Motivating Undergraduates in Science and Technology (MUST) Project.

## **References**

Most of the substantive statements contained in the fictional conversation could be linked to similar statements from the literature. We believe that creating such links would be counterproductive.