

# Assurance Cases

## The Home for Verification\*

*(Or What Do We Need To Add To Proof?)*



**John Knight**

Department of Computer Science  
University of Virginia

&

Dependable Computing LLC  
Charlottesville, Virginia

\* **Computer Assisted**



---

# A LIMERICK

# A Limerick

---

There once was a young man named Rushby  
Mechanical proof he cried, just trust me  
He tackled clock synch  
Took proof to the brink  
And finally algorithms were bug free



What does  
it mean?

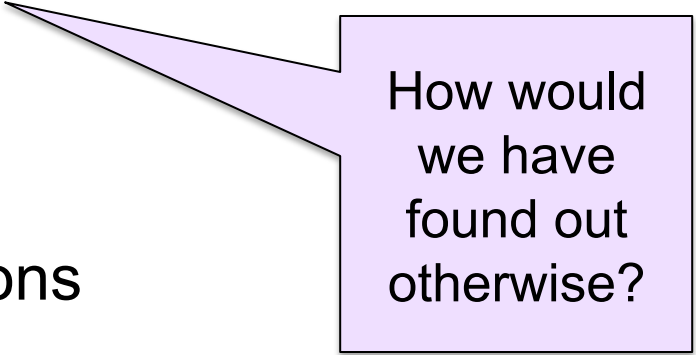


This is a *true* story.  
The work was a *remarkable* achievement

# So What?

---

- Rushby's proofs were mechanical checks of:
  - Proofs developed by humans
  - Published in a peer reviewed journal
- Human proofs were in ***error***
- Rushby:
  - Identified the flaws
  - Indicated the necessary corrections
- Mistakes were subtle
- Results eventually sorted out successfully



How would we have found out otherwise?

# About Proof

---

- We need to be careful with proofs:
  - How should we develop them?
  - What do they mean?
  - How do we use them?
  - **Do we believe them?**
  
- Mechanical proofs can be “wrong”:
  - Incorrect statement
  - Proof system in error
  - Incorrect use of proof system
  - Etc.

Proofs are about ***belief***

What is the ***rationale*** for belief?

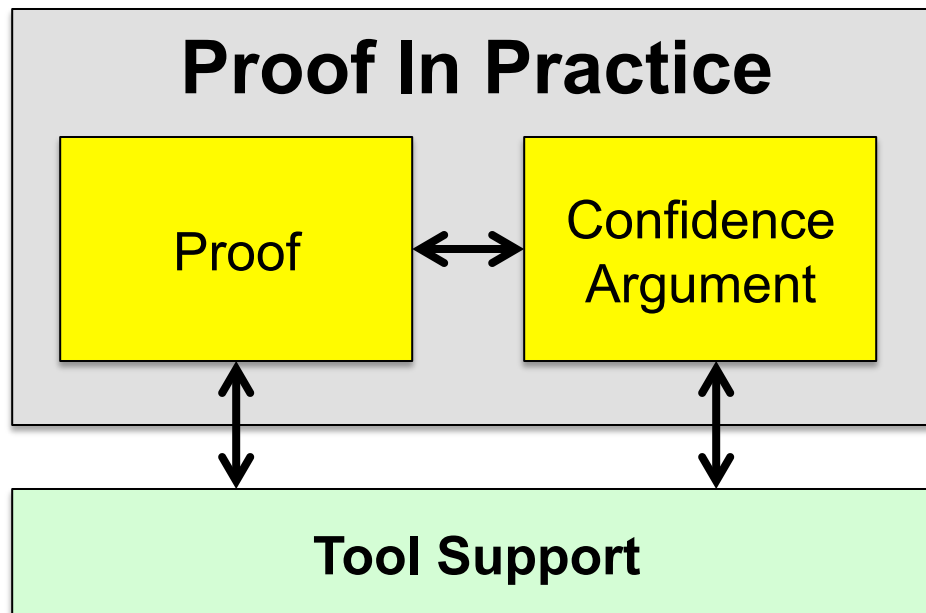
Proof needs assurance  
***No assurance, no belief***

# New Entity – *Proof In Practice*

---

**Q: What is an Assurance Case?**

**A-1: That which leads me to believe the proof**





---

# AN EVEN MORE SERIOUS ISSUE

Apologies to those who have heard the example before

# Asiana Flight 214



- ❑ Boeing 777
- ❑ Landing at SFO
- ❑ July 6, 2013
- ❑ Seawall impact



- ❑ NTSB blamed pilots
- ❑ Safety issues relate to:
  - ... need for Asiana pilots to adhere to standard operating procedures regarding callouts;



# Proof About Pilot Error?

---

***But wait, was it pilot error?***

*Let's look at the report from Asiana Airlines...*

# Asiana Airlines Report

*March 17, 2014*

---

The ***probable cause of this accident was the flight crew's failure to monitor and maintain a minimum safe airspeed during a final approach***, resulting in a deviation below the intended glide path and an impact with terrain. Contributing to this failure were (1) ***inconsistencies in the aircraft's automation logic***, which led the crew to believe that the autothrottle was maintaining the airspeed set by the crew; and (2) ***autothrottle logic that unexpectedly disabled the aircraft's minimum airspeed protection***.

Significant contributing factors to the accident were (1) inadequate warning systems to alert the flight crew that the autothrottle had (i) stopped maintaining the set airspeed and (ii) stopped providing stall protection support; (2) a low speed alerting system that did not provide adequate time for recovery in an approach-to-landing configuration; (3) the flight crew's failure to execute a timely go-around when the conditions required it by the company's procedures and, instead, to continue an unstabilized approach; and (4) air traffic control instructions and procedures that led to an excessive pilot workload during a high-energy final approach.

# Boeing 777 Autothrottle

---

- B777's autothrottle system:
  - Provides stall protection
  - Ensures that the aircraft maintains a safe airspeed in ***almost*** all situations
- Seemingly comprehensive airspeed protection is subject to a ***narrow exception*** during which the autothrottle is deactivated and will not wake up

**So?**

# The “FLCH Trap”

---

- ❑ Unbeknownst to them, crew had fallen into what is known in industry as “**FLCH trap**”
- ❑ When aircraft descending in FLCH mode and throttles are moved to aft stop position -- either by pilot **or** autothrottle system -- autothrottle setting will **automatically and without pilot intervention** change to HOLD, thereby disabling airspeed protection
- ❑ As a result, **autothrottle will not wake** up to provide stall protection, even when plane slows well below commanded speed

# Was The FLCH Trap Unknown?

---

- ❑ FAA's B787 lead test pilot, Captain Eugene Arnold, noticed the issue in August 2010 and, concerned for its **safety implications**, brought it to Boeing's attention
- ❑ In May 2011, EASA issued Major Recommendation for Improvement #3, in which it stated:

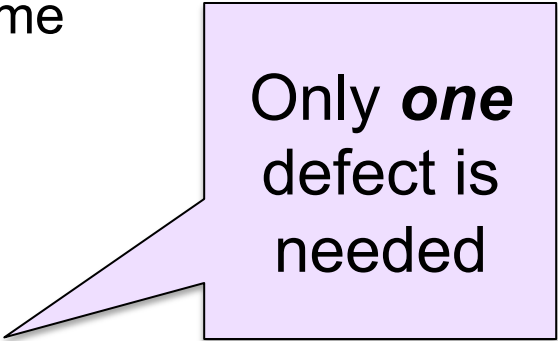
'Unfortunately there are on the B787 (as well as some other previous Boeing models) at least two automation modes (FLCH in descent and VNAV speed in descent, with ATHR on HOLD) for which the "Autothrottle Wake up" function is not operative and therefore does not protect the aircraft. ...

Inconsistency in automation behaviour has been in the past a strong contributor to aviation accidents. The manufacturer would enhance the safety of the product by avoiding exceptions in the "Autothrottle wake up" mode condition.'

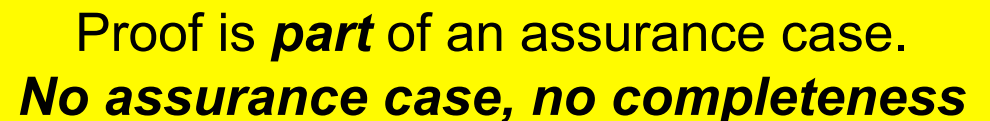
# So What?

---

- ❑ Catastrophic failure
- ❑ Many *many* faults of *many* types
- ❑ No amount of proof would have fixed this:
  - But any proof of any property would be welcome
  - Push for proof
- ❑ A proof in which we believe gives us:
  - **One** piece of evidence about one claim
  - Let's not get intoxicated with this
- ❑ Other claims that *matter* are all over the map:
  - System installation, operation, maintenance – done right?
  - Hazard analysis – complete?



Only **one** defect is needed

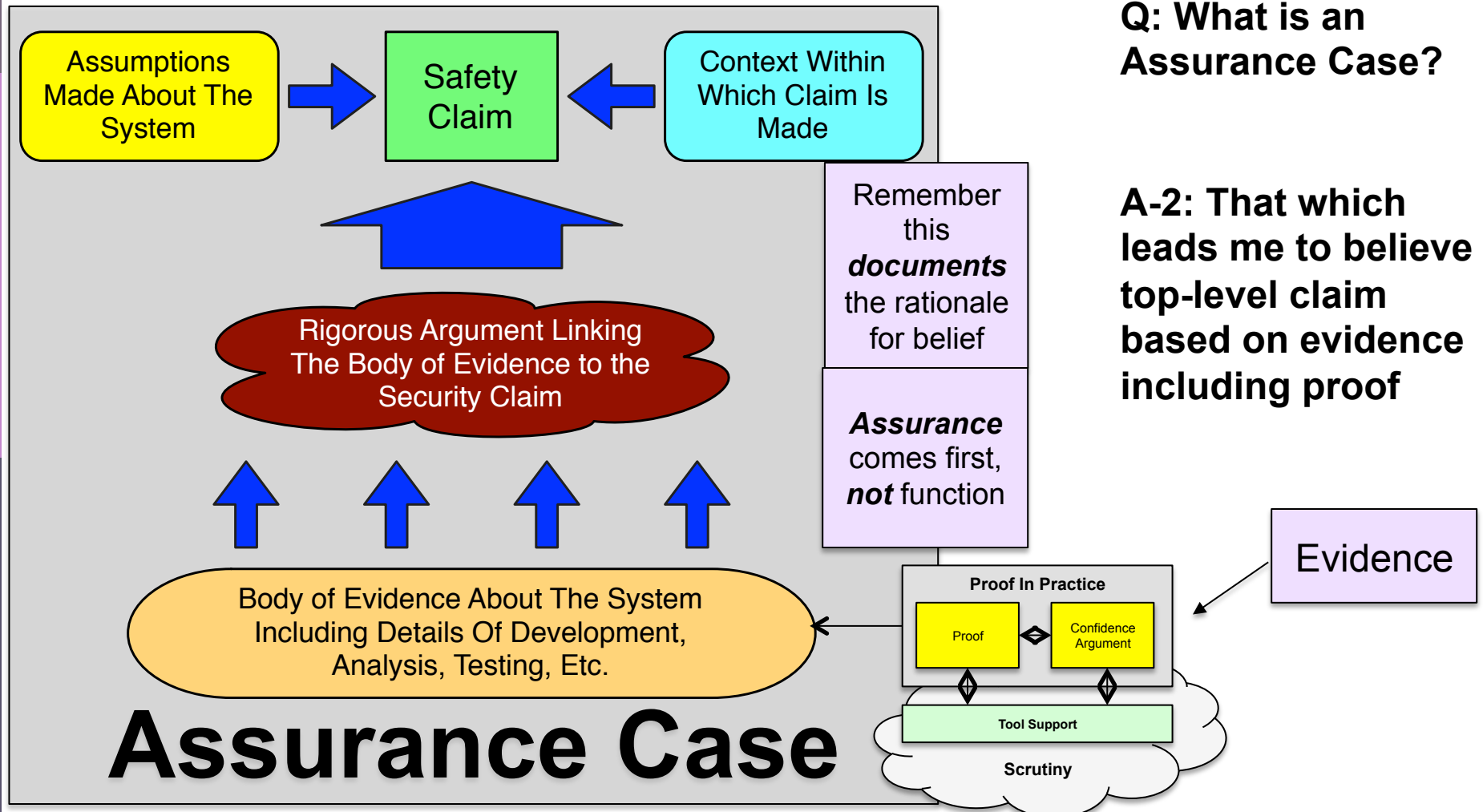


Proof is *part* of an assurance case.  
**No assurance case, no completeness**

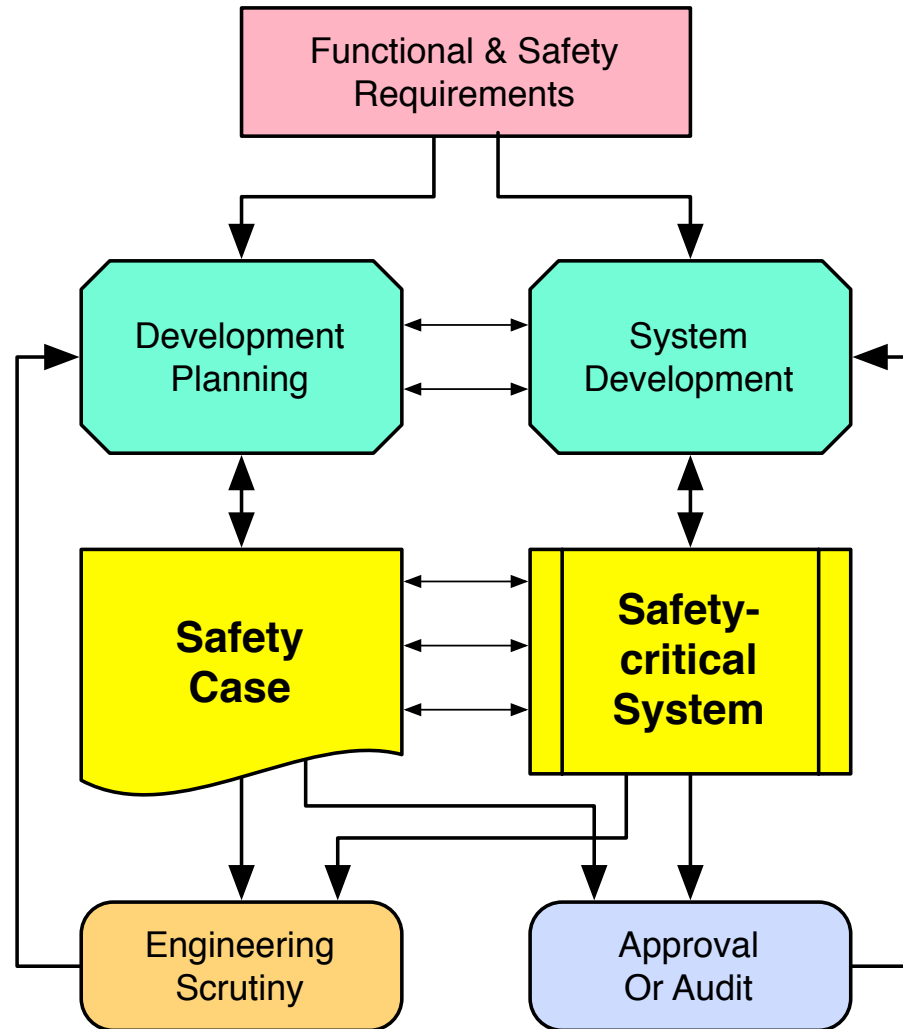
# Practice And Proof

**Q: What is an Assurance Case?**

**A-2: That which leads me to believe top-level claim based on evidence including proof**



# Using An Assurance Case



Assurance case is at the **heart** of the development process

**This** is the process, **not** XP, SCRUM, or MUMBLE\*

\*Monumental Useless Mount of Bungled Language Experiments aka Java





---

# **MORE THAN SYSTEM SAFETY**

# A Letter I Received Recently

---



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

From: Chief Information Officer

Dear JOHN KNIGHT,

**PIN**

I am writing to inform you that the U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have exposed your personal information.

Since the incident was identified, OPM has partnered with the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) to determine the impact to Federal personnel. OPM immediately implemented additional security measures and will continue to improve the security of the sensitive information we manage.

You are receiving this notification because we have determined that the data compromised in this incident may have included your personal information, such as your name, Social Security number, date and place of birth, and current or former address. To help ensure your privacy, upon your next login to OPM systems, you may be required to change your password.

This is a true story – 21,500,000 stolen  
This is a national catastrophe



---

# WHY DO SYSTEMS FAILS?

# Software System Failures

---

To a first approximation, requirements defects are the **dominant source** of problems in safety-critical and high-assurance **software** systems

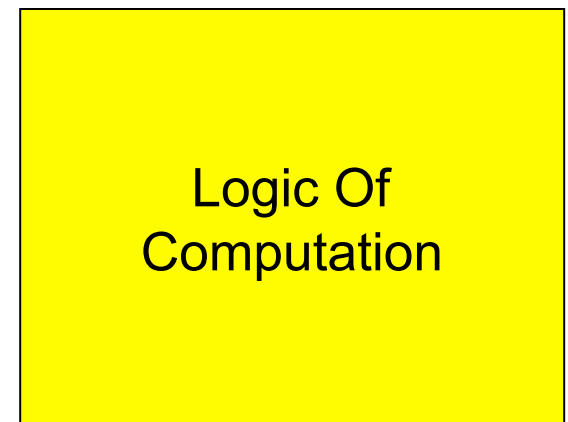
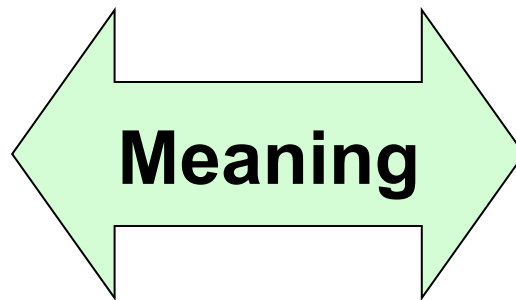
# Software System Failures

---

- “Majority of safety-critical defects derive from poor requirements”  
-- *Lutz*
- “Majority of *all* defects derive from poor requirements”  
-- *AF Rome Laboratory*
- “The hardest single part of building a software system is deciding precisely what to build”  
-- *Brooks*

# Specification And Meaning

---



# The Essential Role Of Natural Language

*Specification As It Needs To Be*

