

---

# Formal Methods & Accident Analysis: What's the Connection?

---

ATB Formal Methods' Team  
3rd Internal Workshop

*C. Michael Holloway*  
(in his last appearance in the  
program/administrative world for a while)

22 October 2003

---

## Formal methods and accident analysis are connected because ...

---

- ... they span the alphabet from A (ccident) to Z (ed).
- ... I've organized workshops at the Radisson Fort Magruder Hotel for both.
- ... post-traumatic stress syndrome can affect accident victims and theorem prover users alike.
- ... reseachers and practitioners in both are thought to be a tad on the strange side by 'normal' people.



---

## Formal methods and accident analysis are connected because ...

---

- ... **both** have their share of 'tool zealots', people who think their favorite tool or technique works for everything.
- ... **both** are (wrongly) criticized as telling us things we already know, for example

**formal methods:** several page proof to demonstrate that  $\sin(x) = 0$  when  $x$  is a multiple of  $\pi$

**accident analysis:** 100+ pages demonstrating that *NASA's organization is a mess*



---

## Formal methods and accident analysis are connected because ...

---

- ... using selected principles and techniques from formal methods can help improve accident analysis.
- ... recognizing and applying selected lessons from accident analysis can help improve formal methods.



---

## Formal methods can improve accident analysis by ...

---

- ... emphasizing the importance of precision in definitions and descriptions.
  - ▶ “For what is time? Who can easily and briefly explain it? Who can even comprehend it in thought or put the answer into words? Yet is it not true that in conversation we refer to nothing more familiarly or knowingly than time? And surely we understand it when we speak of it; we understand it also when we hear another speak of it. What, then, is time? If no one asks me, I know what it is. If I wish to explain it to him who asks me, I do not know.”

--- *Confessions of St. Augustine*, Bk.11, Ch. 14



---

## Formal methods can improve accident analysis by ...

---

- ... emphasizing the importance of precision in definitions and descriptions.
- ... providing notations for describing and reasoning about certain aspects of accidents.



---

## Formal methods can improve accident analysis by ...

---

- ... emphasizing the importance of precision in definitions and descriptions.
- ... providing notations for describing and reasoning about certain aspects of accidents.

Why-Because Analysis (Ladkin and Loer) introduces:

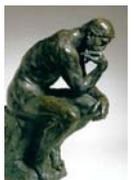
$\Rightarrow$  'cause',  $\Box \rightarrow$  'counterfactual',  $\Box \Rightarrow$  'necessary and sufficient'.

$$\frac{A \wedge B}{\frac{\neg A \Box \rightarrow \neg B}{A \Rightarrow B}}$$

$\neg A \Box \rightarrow \neg B$ : In possible worlds close to those in which A is false (did not happen), B is also false (did not happen).

This logic provides a semantics for informal concepts such as 'cause'.

Proof rules ensure consistency and sufficiency of reasoning.



---

## Formal methods can improve accident analysis by ...

---

- ... emphasizing the importance of precision in definitions and descriptions.
- ... providing notations for describing and reasoning about certain aspects of accidents.
- ▶ The extent to which formal notations are suitable for describing causal arguments is still an open question.
- ▶ No existing notation is without problems in two areas:
  - Correspondence of formal semantics to the real world
  - Suitability for use in reports to be read by non-logicians



---

## Accident analysis can improve formal methods by ...

---

- ... providing case studies upon which a compelling argument for the efficacy of formal methods might be built.
- ... emphasizing the fact that the real world is a truly messy place.
  - ▶ Not everything can be formalized.
  - ▶ Formalizations that do not correspond to the real world are *worse than useless* to engineers.
- ... encouraging a proper humility.

