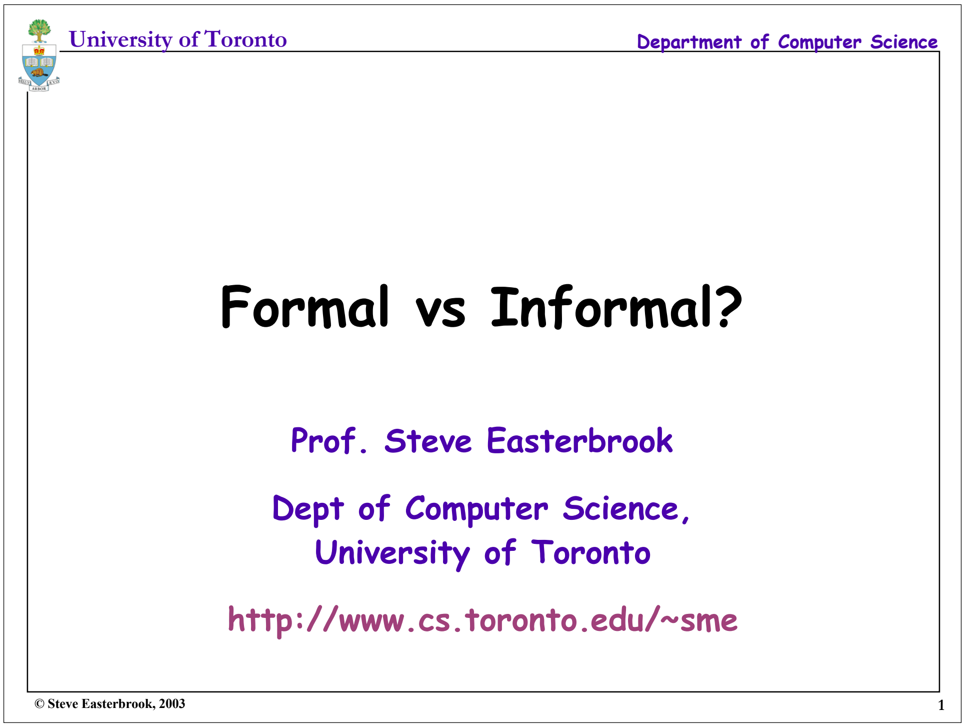
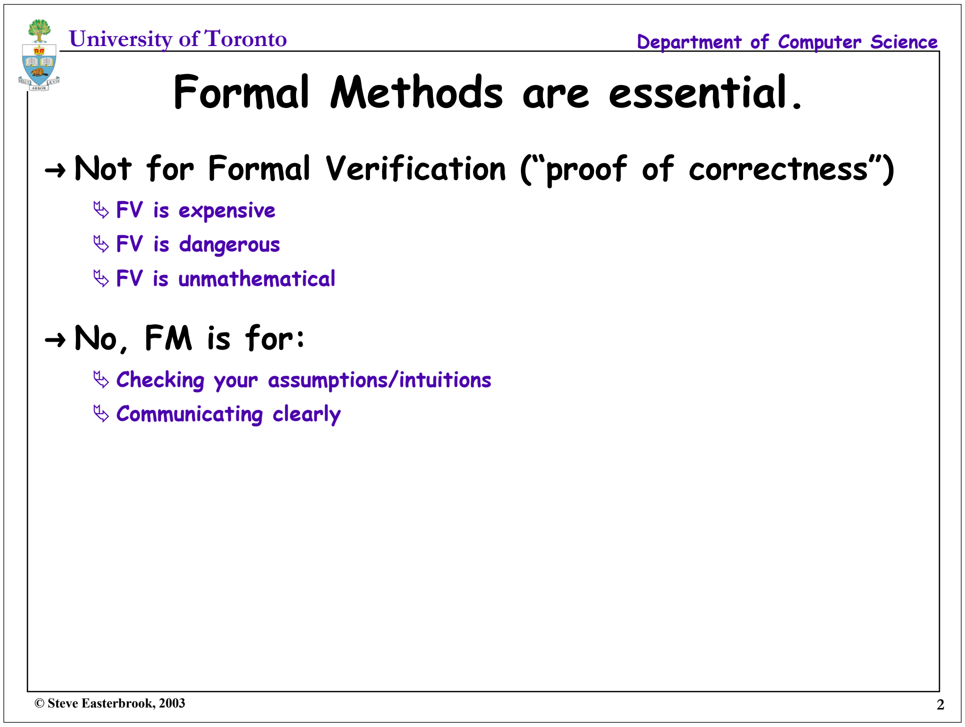


Formal vs Informal?

Prof. Steve Easterbrook

Dept of Computer Science,
University of Toronto

http://www.cs.toronto.edu/~sme



Formal Methods are essential.

- Not for Formal Verification ("proof of correctness")
  - FV is expensive
  - FV is dangerous
  - FV is unmathematical
- No, FM is for:
  - Checking your assumptions/intuitions
  - Communicating clearly

Example Requirement

... the C&C MDM CSCI shall set the e,c,w, indicator ... if a backup BC is available, the BC has been switched in the last 20 sec, the SPD card reset capability is inhibited, or the SPD card has been reset in the last 10 major (10-second) frames, and either:

1) the transaction errors are from multiple RT's, the current channel has been reset within the last major frame, or

2) the transaction errors are from multiple RTs, the current channel's reset capability is inhibited, and the current channel has not been reset within the last major frame.

Backup BC available	T	T	T	T
BC switched last 20 secs	T	T	T	T
SPD card reset inhibited	T	T	-	-
SPD card reset in last 10 frames	-	-	T	T
Errors from multiple RTs	T	T	T	T
Channel reset last major frame	T	F	T	F
Channel reset inhibited	-	T	-	T

SCR Mode Table for the Bus Controller

Current Mode	Conditions											Next Mode
	errors in two cons. frames	bus swch'd last frame	bus switch inhibit	bus swch'd this frame	backup BC avail.	BC swch'd in last 20 sec	card reset inhibit	card reset last 10 frames	errors from mult. RTs	channel reset last frame	channel reset inhibit	
Normal	@T	-	-	F	-	-	-	-	-	-	-	switch buses
	@T	-	T	F	-	-	-	-	-	-	F	reset the channel
	@T	T	-	F	-	-	-	-	-	-	F	
	@T	-	-	-	-	-	F	F	T	T	-	reset the card
	@T	-	-	-	-	-	F	F	T	F	T	
	@T	T	-	-	-	-	-	-	F	T	-	switch RT to backup
	@T	F	T	-	-	-	-	-	F	T	-	
	@T	T	-	-	-	-	-	-	F	F	T	
	@T	F	T	-	-	-	-	-	F	F	T	
	@T	-	-	-	T	F	T	-	T	T	-	switch BC to backup
	@T	-	-	-	T	F	T	-	T	F	T	
	@T	-	-	-	T	F	-	T	T	T	-	
	@T	-	-	-	T	F	-	T	T	F	T	
	@T	-	-	-	T	T	T	-	T	T	-	switch all RTs
	@T	-	-	-	T	T	T	-	T	F	T	
	@T	-	-	-	T	T	-	T	T	T	-	
	@T	-	-	-	T	T	-	T	T	F	T	

Challenger Launch decision

Jan 27, 1986

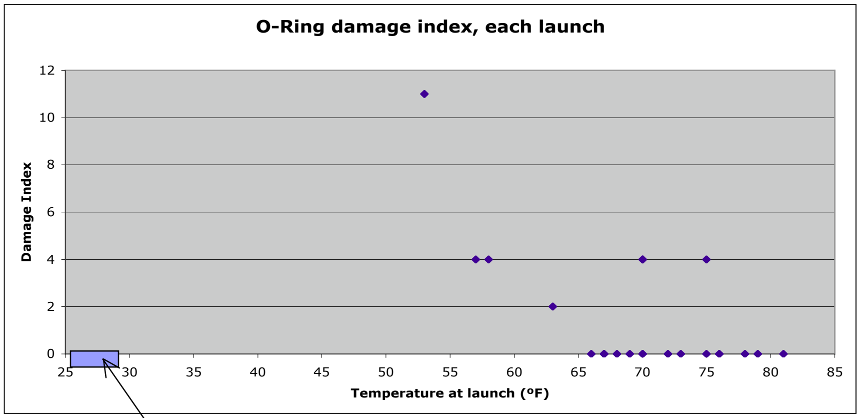
- 2:30pm Thiokol engineers express concern at predicted low temperature
- 5:45pm Thiokol presents its concerns to Marshal
  - recommends launch should be delayed
- 8:45pm Thiokol re-presents its conclusions to larger meeting
  - Marshall criticizes it for changing the launch criteria
- 10:30pm meeting recessed for Thiokol discussion
  - engineers express strong objections to launch
- 11:00pm meeting reconvened
  - Thiokol management withdrew objections to launch

Jan 28, 1986

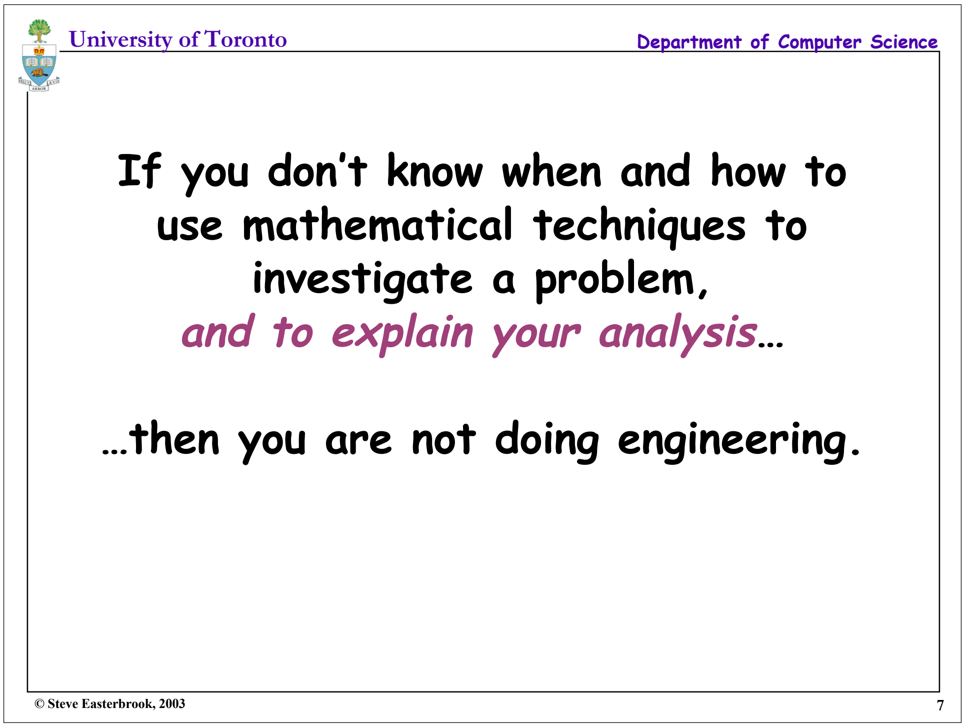
- 11:39am: flight 51-L launched
  - 73 seconds later, Challenger explodes

Importance of Communication

- The graph that was never drawn…
  - For the Challenger launch decision, this data was available
  - But was never collected and presented this way



range of forecast temperatures for launch on Jan 28, 1986



If you don’t know when and how to use mathematical techniques to investigate a problem,

and to explain your analysis…

…then you are not doing engineering.