Need for Scenario-Based Accident Modeling

Leadership ViTS Meeting

January 03, 2005

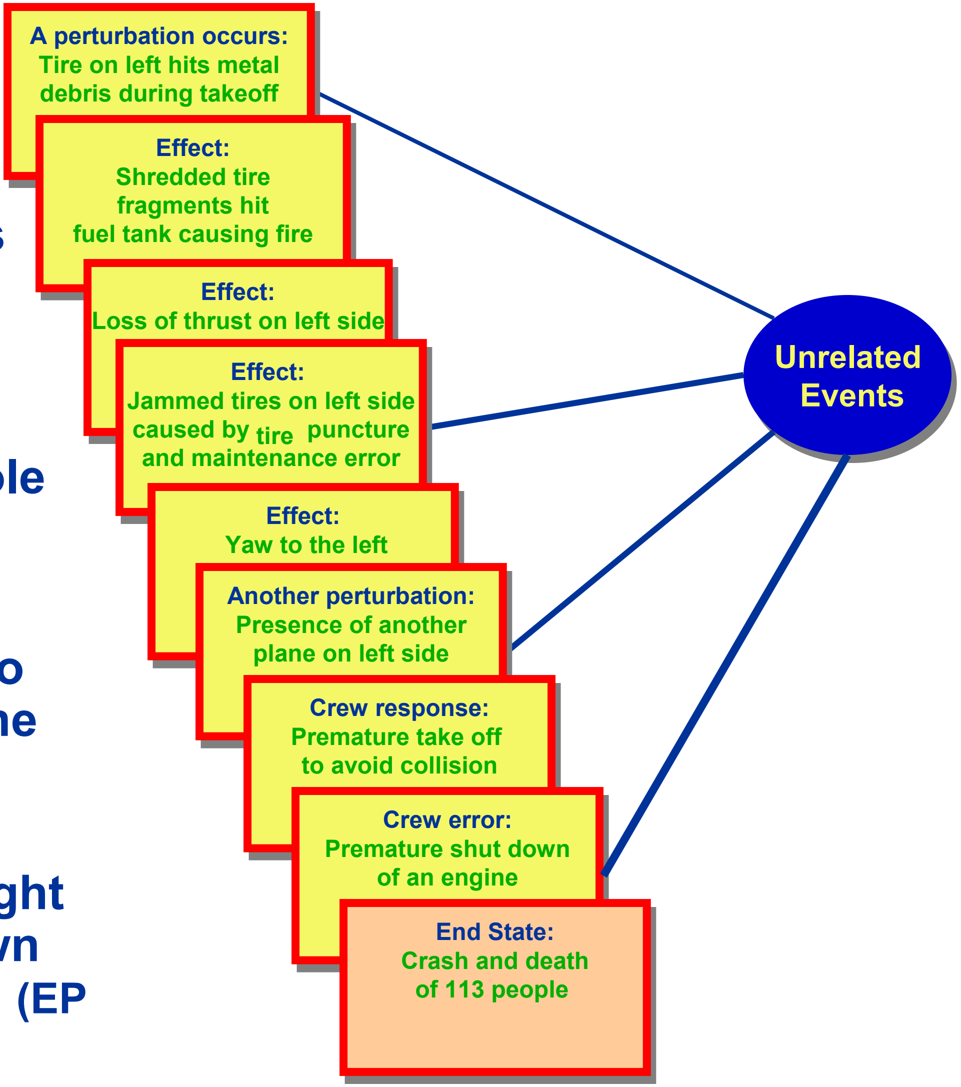
Bryan O’Connor
Chief
Office of Safety and Mission Assurance

Need to Identify Complex Accident Scenarios

- Experience has shown that multiple, unrelated, and sometimes benign perturbations have challenged our systems in complex ways we would have never expected.
- High-consequence scenarios can emerge as a result of the occurrence of multiple unrelated events.
- Traditional system safety evaluations (e.g., FMEA) often model the response of the system to a single perturbation (failure or process deviation):
  - Accident scenarios predicted by these models tend to be incomplete.
  - From a risk management point of view, relying solely on such analyses, may cause relatively unimportant issues to receive excessive attention, while other important issues may go unidentified.

Crash of Air France Concord in July 2000 Involved Multiple Events

- Metal strip on runway punctures tires.
- Piece of tire comes free and punctures the fuel tank.
- Fuel pours out the punctured hole and ignites.
- Left tires jam.
- The pilot prematurely takes off to avoid collision with another plane waiting to cross Concorde’s runway.
- At 25 feet off the ground, the Flight Engineer prematurely shuts down #2 engine which was not on fire. (EP specifies engine shutdown at 400 ft)



A perturbation occurs:
Tire on left hits metal debris during takeoff

Effect:
Shredded tire fragments hit fuel tank causing fire

Effect:
Loss of thrust on left side

Effect:
Jammed tires on left side caused by tire puncture and maintenance error

Effect:
Yaw to the left

Another perturbation:
Presence of another plane on left side

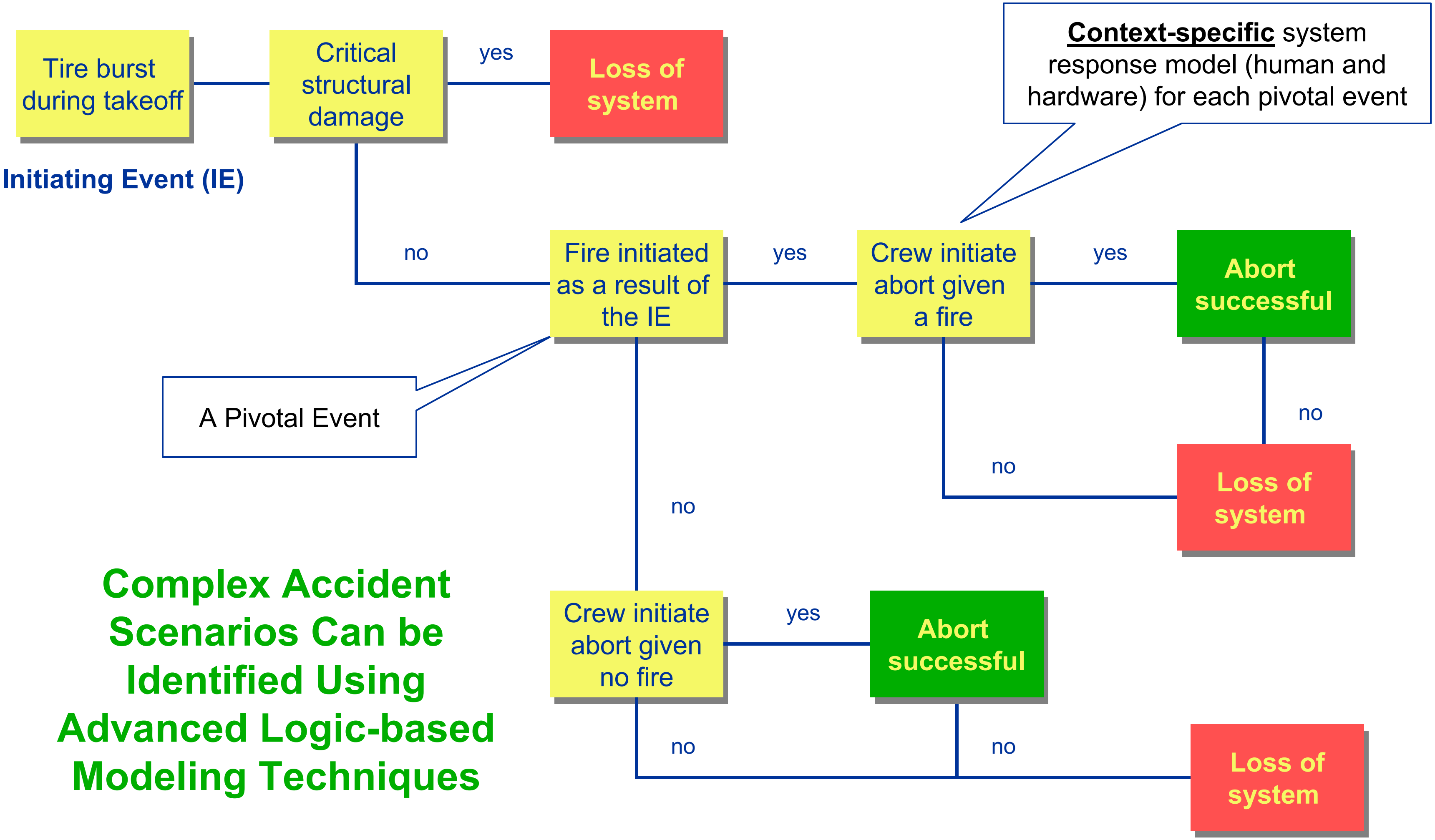
Crew response:
Premature take off to avoid collision

Crew error:
Premature shut down of an engine

End State:
Crash and death of 113 people

Unrelated Events

An Example of Event Sequence Diagram (ESD)


Tire burst during takeoff
Initiating Event (IE)
Critical structural damage
yes
Loss of system
no
Fire initiated as a result of the IE
A Pivotal Event
yes
Crew initiate abort given a fire
yes
Abort successful
no
Loss of system
no
no
Crew initiate abort given no fire
yes
Abort successful
no
no
Loss of system

Context-specific system response model (human and hardware) for each pivotal event

Complex Accident Scenarios Can be Identified Using Advanced Logic-based Modeling Techniques

Conclusions

- Complex accidents scenarios can emerge as a result of combination of several unrelated mishap events
- A typical FMEA cannot identify complex scenarios such as the the one that led to the crash of the Concord.
- Identification of complex accident scenarios in safety assessment is both necessary and challenging.
- Application of systematic and logic-based safety assessment techniques, such as Event Sequence Diagrams, Event Trees, and Fault Trees, to accident scenario development and analysis is essential to predict complex mishap events
- Effective risk management strategies cannot be devised without the knowledge of plausible accident scenarios.