Hazards, accidents and events - A land of confusing terms

Rune Winther[1] William Marsh[2]

[1]Division Transport
COWI Norway

[2]School of Electronic Engineering and Computer Science
Queen Mary, University of London, London, UK

ESREL 2013, Amsterdam

Outline

Hazards and Why They Matter

- Safety depends on understanding potential accidents
- Risk assessment using hazards
  - Consistency: can we agree the hazards?
  - Coherence: just one hazard
- Important context
  - Modular analysis of systems
  - Reuse of hazard analysis

Example Definitions

EN 50126	
Hazard	A physical situation with a potential for human injury.
EN 50129 and CSM RA	
Hazard	A condition that could lead to an accident.
Accident	An unintended event or series of events that results in death, injury, loss of system or service, or environmental damage.
EU Single Sky Regulation 1035/2011	
Hazard	Any condition, event, or circumstance which could induce an incident.
US DoD Mil-Std 882e	
Hazard	A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

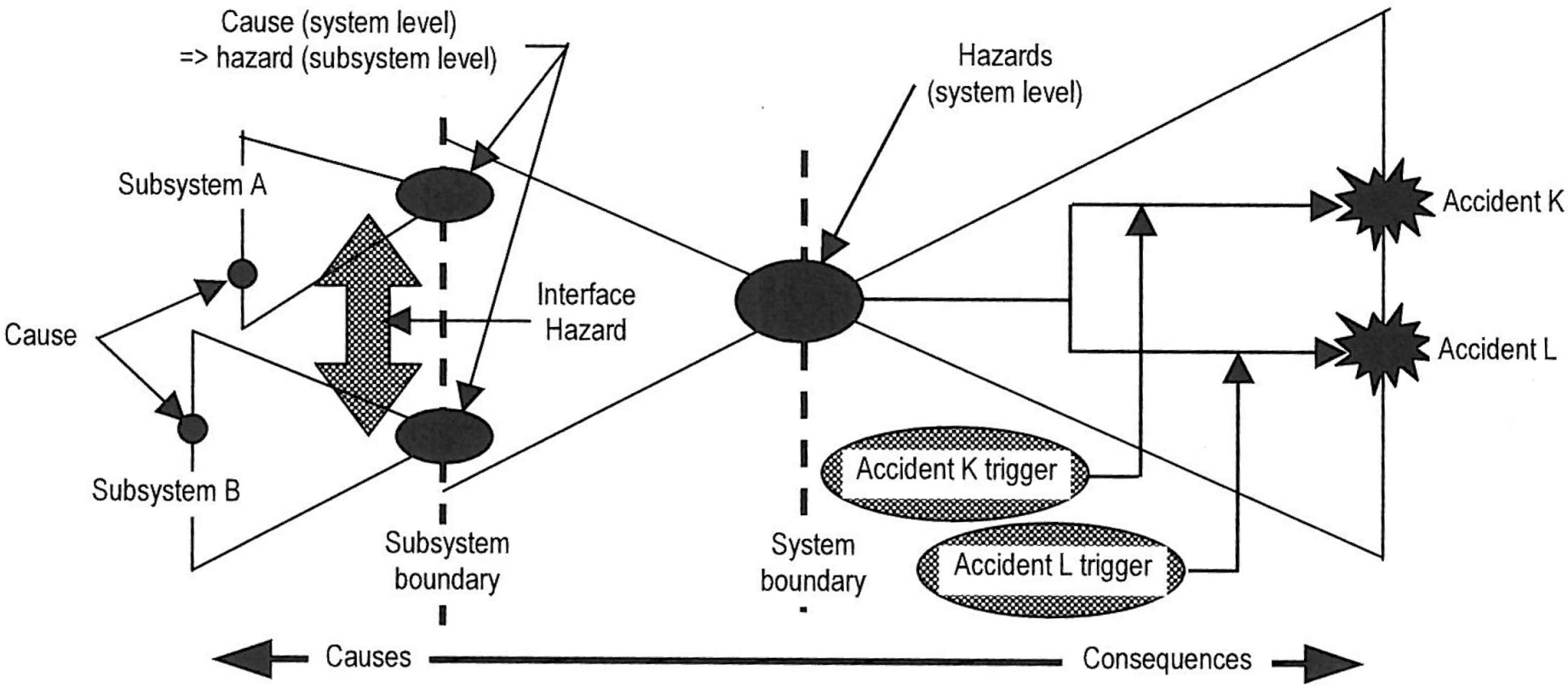
Points of Confusion

- What harm?
  - Death and injury
  - Material and environmental damage
  - Financial loss
- Condition or event?
  - Words include *condition*, *situation*, *physical situation*, *circumstance*, *a state of a system*, and *event*
- How does a hazard contribute to an accident?
  - Words include *potential for*, *lead to*, *contribute to*, *induce* and *source of*

Relatively: Where in the Causal Chain?

- Chain of event model of accident
  - Failure *leads to* Hazard *leads to* Accident
- Consider the following sequence:
  1. Wet leaves fall on track.
  2. Train's breaking distance is longer than normal.
  3. Train passes a red signal.
  4. Train collides with car at level crossing.
- Which is the hazard?

EN50126 Guide: Boundaries and Systems



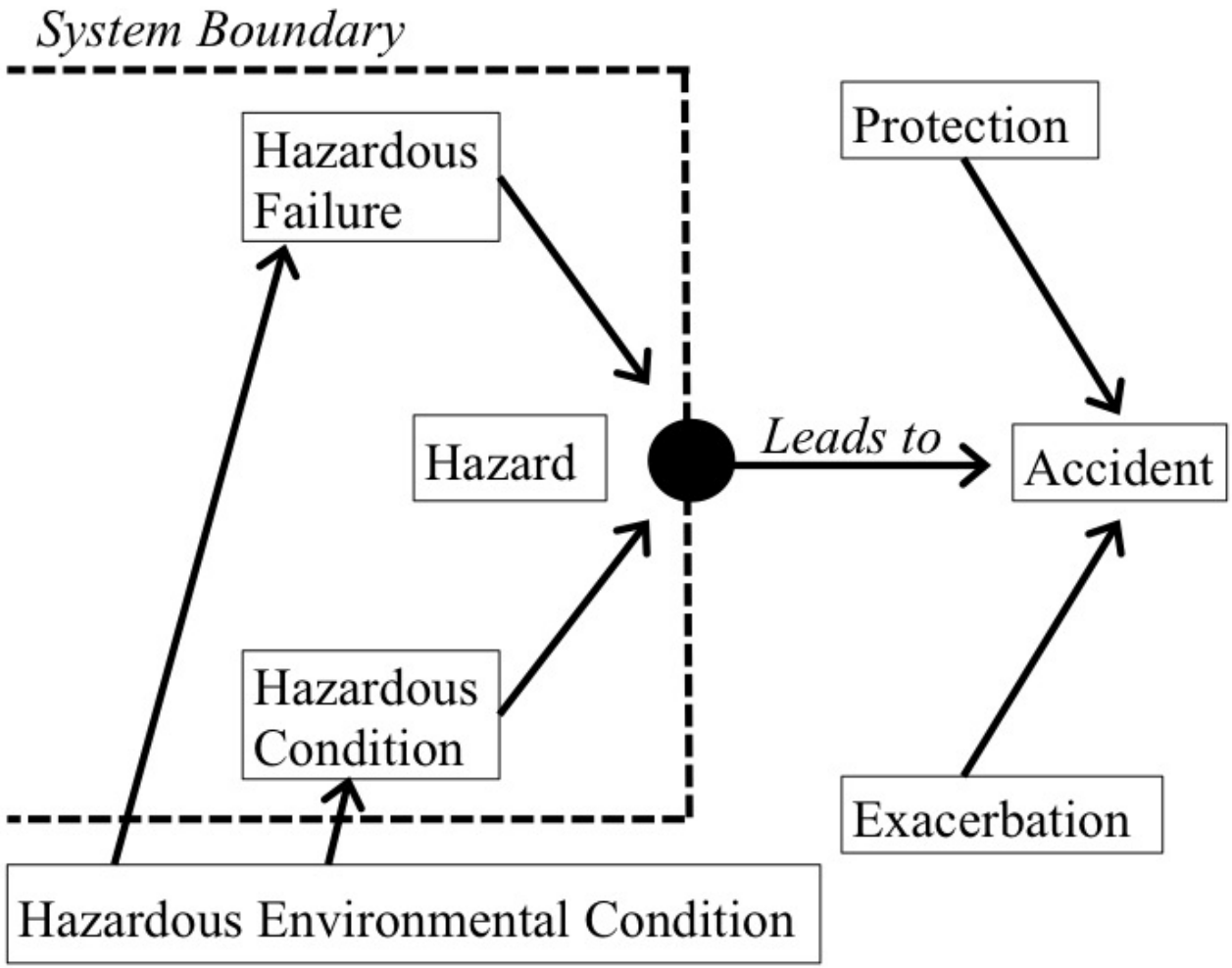
Goals for a More Precise Hazard Ontology

1. To resolve the relativity problem by including a concept of system boundary in the definition of hazard.
2. To distinguish between events and conditions by showing the causal relationships between all the terms in the ontologies.
3. To explain the relationship between subsystems and hazards.

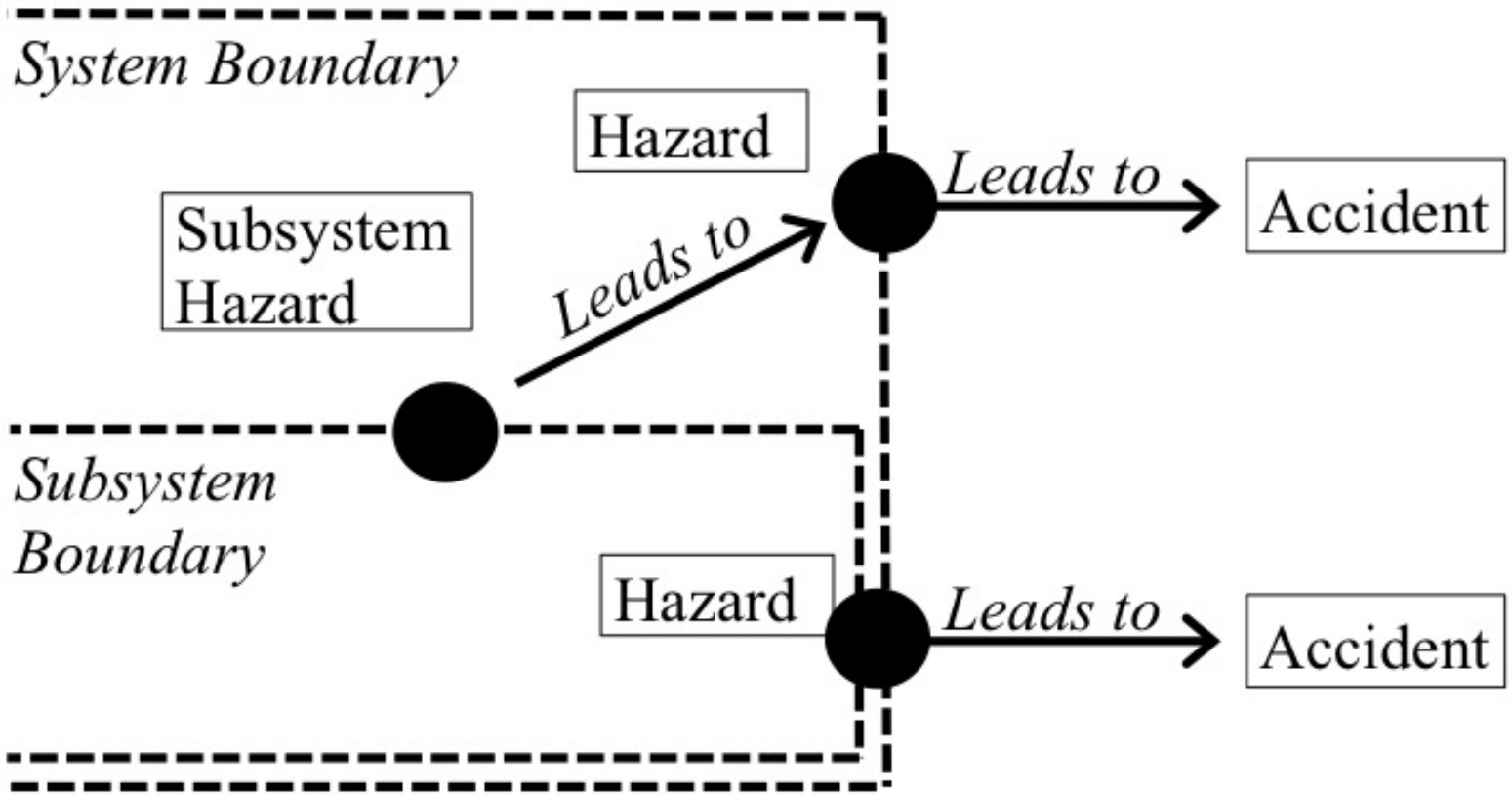
Definitions of Ontology Terms

Term	Definition
Hazard	An event or state at the boundary of a system that can lead to an accident.
Hazardous failure	A event within the system that may lead to a hazard of the system.
Hazardous condition	A state of the system that may contribute to the occurrence of a hazard of the system, or the severity of an accident.
An interface hazard	An event or state at the boundary between subsystems that may lead to a hazard in a system of which these subsystems are a part.
Subsystem hazard	An event or state at the boundary of a subsystem that can lead to a hazard in the system of which the subsystem is a part.

The proposed ontology



The proposed ontology



Example Problem: Rail Tunnel Evacuation

A rail tunnel has a number of systems to protect against fire.
Chain of events:

1. Fire on board a train inside the tunnel.
2. Ventilation in the tunnel activated.
3. Passengers unable to open emergency exit door, because of air pressure.
4. Passengers exposed to smoke from the burning train.

System is the complete railway infrastructure, with ventilation and emergency exits are two different subsystems.

Analysis of Example Using Ontology

Term	Application
Hazard	Tunnel does not allow passenger evacuation.
Hazardous failure	Inability of the emergency exit doors to be opened when exposed to differential air pressure.
Hazardous internal condition	The emergency exit doors might be affected by the differential air pressure caused by an active ventilation system.
Protection	Availability of ventilation and emergency exits.
Interface hazard	Ventilation subsystem exerts air pressure on emergency exit doors, prohibiting them from being opened.
Subsystem hazard	Emergency exit doors cannot be opened when there is a fire in the tunnel.

Summary

- Current definitions of ‘hazard’ cause practical problems
  - What harm?
  - Condition or event?
  - Hazard $\longrightarrow$ Accident
- Ontology of hazard terms
  - Richer causal model
  - Hazards occur at a system boundary
  - Distinguish sub-system and interface hazards
- Framework for reuse, within limits

Further work:

- Examples from actual projects
- Method for reusable, modular risk analyses