Risk Assessment
3. Hazards and Threats

Stein Haugen
stein.haugen@ntnu.no

Marvin Rausand
marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 0.1)

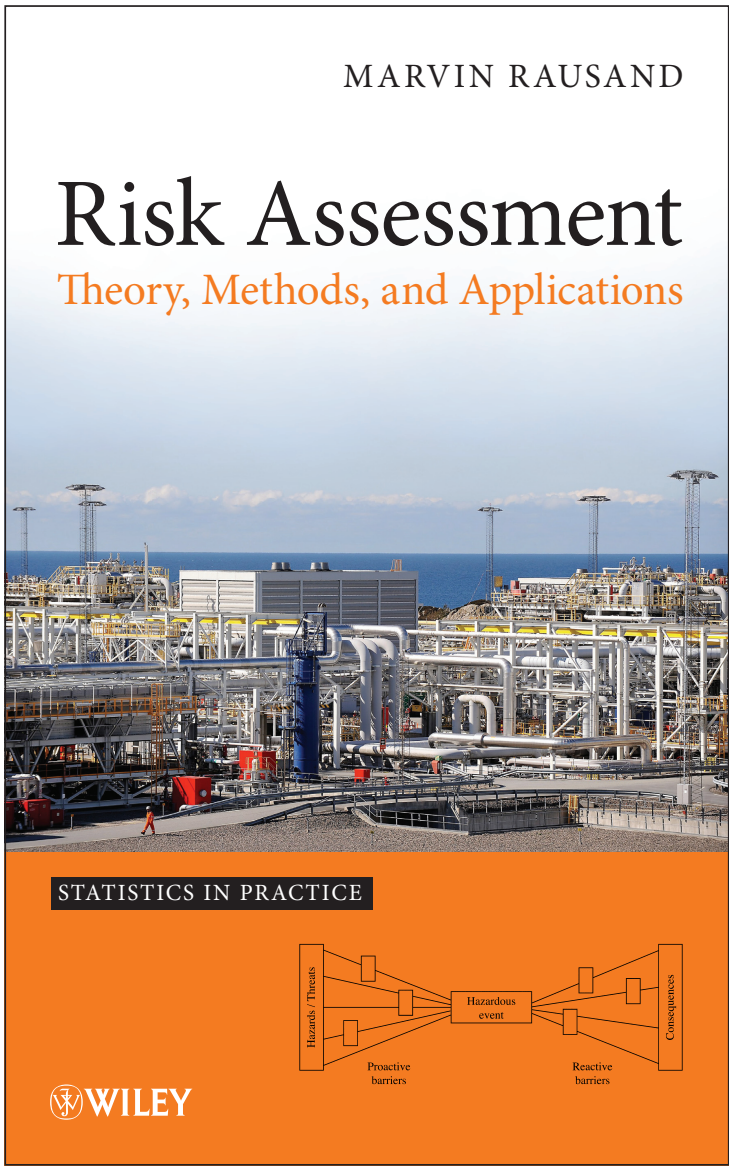
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

Risk Assessment
Theory, Methods, and Applications

Wiley, 2011

Homepage of the book:
http://www.ntnu.edu/ross/books/risk

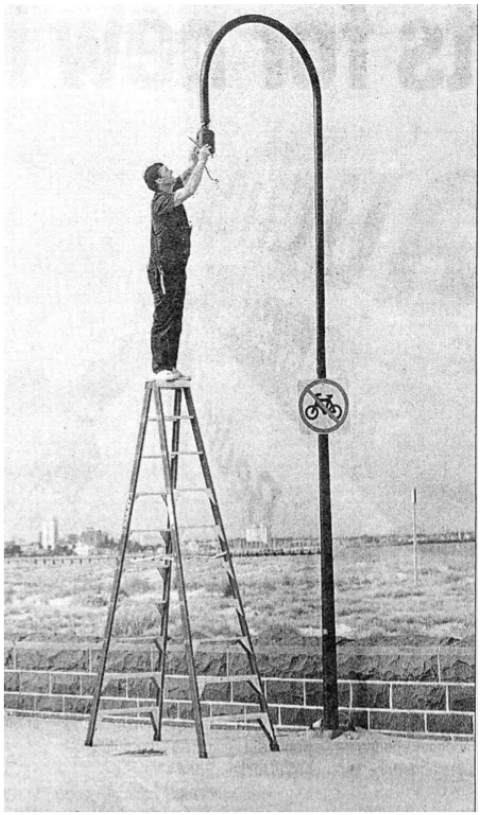


Hazard

☞ Hazard: A source of danger that may cause harm to an asset.

A hazard is:

- A property, a situation, or a state.
- Not an event but a prerequisite for the occurrence of a hazardous event..
- Often, but not always, related to energy of some kind.



Energy sources

- Acoustic
- Atmospheric
- Chemical
- Corrosive
- Electrical
- Electromagnetic
- Explosice, pyrophoric
- Flammable
- Gravitational
- Hydraulic
- Kinetic (linear)
- Kinetic (rotational)
- Magnetic
- Mechanical
- Nuclear
- Patogenic
- Pneumatic
- Potential
- Pressure
- Thermal
- Toxic

Triggering event

☞ Triggering event: An event or condition that is required for a hazard to give rise to an accident.

- Triggering events and hazardous events may be the same.
- Triggering events may also be interpreted as events that cause a hazardous event.

- Active failures: Events that trigger unwanted events.
- Latent conditions: Not triggers, but conditions that may increase the probability of active failures.

Classification of hazards

- Natural hazards
  - Floods, earthquakes, tornados, tsunamis, lightning
- Technological Hazards
  - Industrial facilities, structures, transportation systems, consumer products, pesticides, pharmaceuticals
- Organizational hazards
  - Long working hours, inadequate competence
- Social hazards
  - Assault, war, sabotage, communicable disease
- Behavioral hazards
  - Drug abuse, alcohol, smoking, and so on

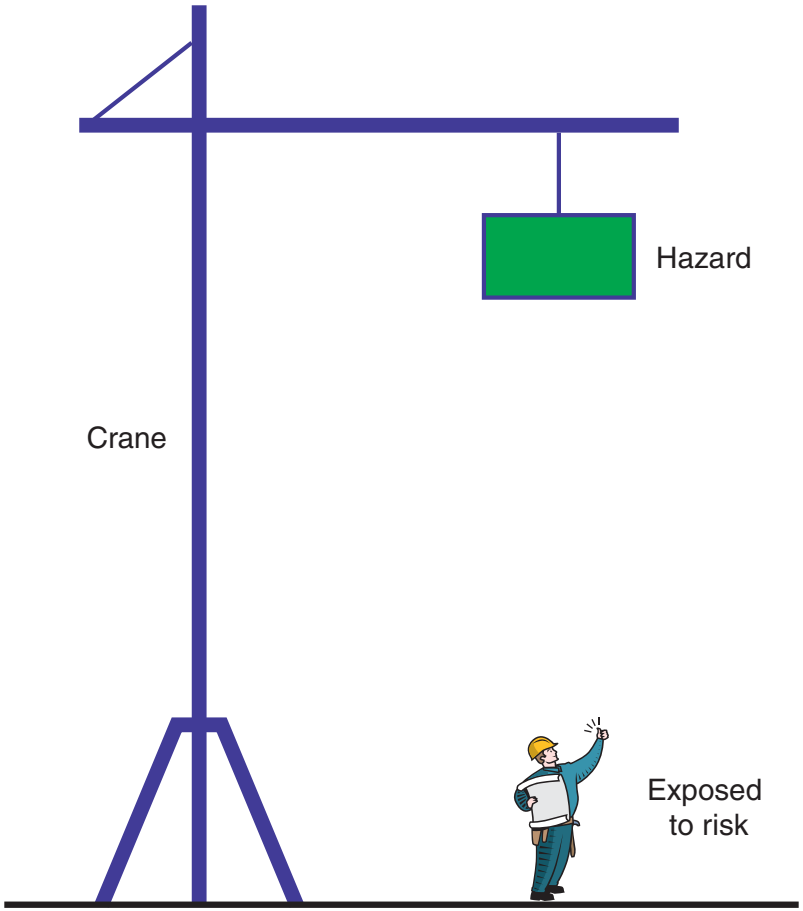
Classification of hazards

- Types of technological hazards
  - Mechanical, electrical, radiation, ...
- What are the effects (type of harm)?
  - Cancer, suffocation, pollution, burn, ...
- Where is the origin of the hazard?
  - Endogenous – "inside" the system
  - Exogenous – "outside" the system

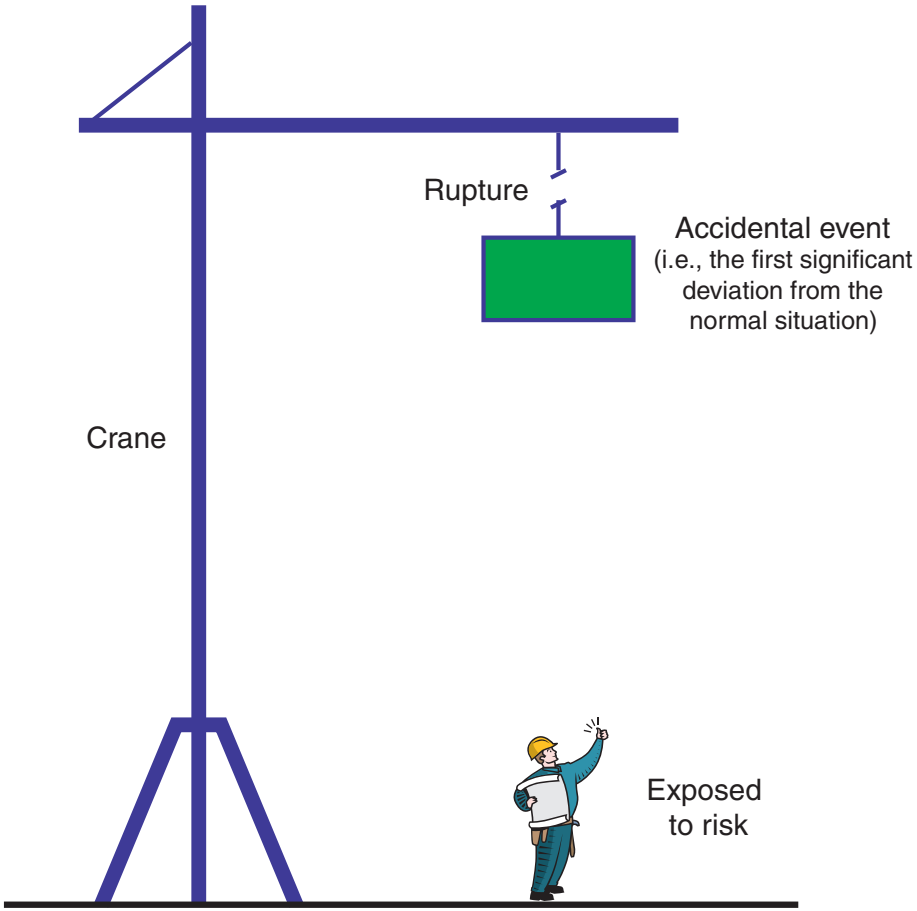
Specific hazards

- Mechanical hazards
  - Kinetic energy
  - Acceleration or retardation
  - Sharp edges/points
  - Potential energy
  - High pressure
  - Vacuum
  - Moving parts
  - Rotating equipment
  - Reciprocating equipment
  - Stability/toppling problems
  - Degradation of materials
- Dangerous materials
  - Explosive
  - Oxidizing
  - Flammable
  - Toxic
  - Corrosive
  - Carcinogenic
- Electrical hazards
  - Electromagnetic
  - Electrostatic
  - Short circuit
  - Overload
  - Thermal radiation
- …and so on

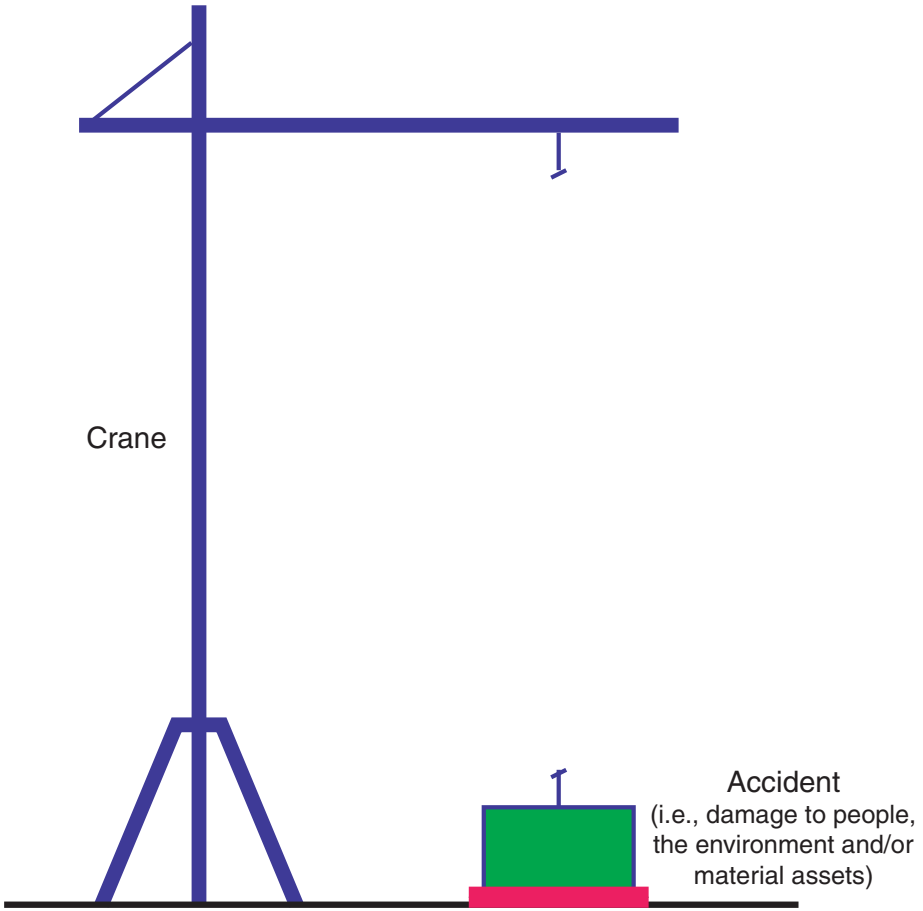
Hazard



Hazardous event



Accident


Crane
Accident
(i.e., damage to people,
the environment and/or
material assets)

Threat

☞ Threat: Anything that might exploit a vulnerability.

- Any potential cause of an incident can be considered a threat
- Closely related to hazard
- A threat is a hazard, but a hazard need not be a threat

☞ Threat agent: A person, organization, thing, or entity that acts, or has the power to act, to cause, carry, transmit, or support a threat.

- *Who* could want to exploit vulnerabilities, and *how* they might use them against the system
- *Intention, capacity*, and *opportunity*

Information security concepts

- Availability: The accessibility of systems, programs, services, and information when needed and without undue delay
- Confidentiality: The sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of 'loss' should unauthorized disclosure occur
- Integrity: The accuracy and completeness of information and assets and the authencity of transactions
- Compromise: Unauthorized disclosure, destruction, removal, modification or interruption.

Vulnerability

☞ Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threat agents, for example, to gain access to the asset and subsequent destruction, modification, theft, and so on, of the asset or parts of the asset.

- The weaknesses may be physical, technical, operational, and organizational.

Technical failure

☞ Failure: The termination of the ability of an idea to perform a required function.

- In other words: A failure is the non-fulfillment of a functional (or performance) requirement.

Example

Consider a water pump:

- A required function of the pump is to “pump water.
- The functional requirement related to this function is that the output of water should be between 100 and 110 liters of water per minute.
- The pump has failed if the output of water is outside this interval.

Failure mode

☞ Failure mode: The effect by which a failure is observed on a failed item.

- A failure mode is a state and specifies the actual deviation from the performance requirements of the item.

This definition is not totally clear, but a failure mode should tell us in which way an item is no longer able to fulfill a required function.

General failure modes

- Failure during operation
- Failure to operate at a prescribed time
- Failure to cease operation at a prescribed time
- Premature (spurious) operation

Failure modes

Example: Failure modes of a water tap

- Fail to open (on demand)
- Fail to close (on demand)
- Cannot fully close
- Leakage through (dripping)
- Leakage out (from tap seals)
- Too high temperature
- Too low temperature
- …and so on

Failure mechanism

☞ Failure mechanism: A physical, chemical, or other process that leads to failure.

Examples of failure mechanisms include

- Corrosion
- Erosion
- Fatigue

Failure classification

According to cause of failure

- Primary failure: Caused by natural aging that occurs under conditions within the design envelope of the item.
- Secondary failure: Caused by excessive stresses outside the design envelope of the item.
- Command fault: A failure caused by an improper control signal or noise (sometime referred to as a *transient* failure).

Failure classification

According to degree of failure (from OREDA)

- Critical: A failure that causes immediate and complete loss of the system's capability of providing its output.
- Degraded: A failure that is not critical but that prevents the system from providing its output within specifications.
- Incipient: A failure that does not immediately cause loss of a system's capability of providing its output, but which, if not attended to, could result in a critical or degraded failure in the near future.