From regular threats to unexampled events: Risk, vulnerability, and complex systems

Erik Hollnagel
Professor & Industrial Safety Chair
MINES ParisTech
Crisis and Risk Research Centre (CRC)
Sophia Antipolis, France
E-mail: erik.hollnagel@crc.ensmp.fr

Professor II
Institutt for industriell økonomi og teknologiledelse (IØT)
NTNU

The meaning of safety

How can it be done?

How much risk is acceptable?

How much risk is affordable

SAFE SYSTEM = FREEDOM FROM UNACCEPTABLE RISK

What can go wrong?

Prevention of unwanted events

Protection against unwanted outcomes

Normal operation

Unexpected event

Unwanted outcome

LIFE
PROPERTY
MONEY

Accidents, incidents, …

Understanding what can go wrong

1 Is it possible to understand that there is a problem and further to describe what it is?

Recognise that there is a problem
NO SYSTEMS ARE INHERENTLY SAFE!
Understand the reasons for it (availability of examples)

2 Is it possible to imagine the consequences and to differentiate between risks with large and small consequences?

Envisage the consequences concretely
Understand failure "mechanism" (representativeness).
Intuitive feeling that the risks are real.

3 Are there are any known solutions by which the problem can be reduced or eliminated?

Are there concrete solutions, i.e., specific actions or precautions.
Are the solutions affordable?
Do solutions correspond to the "failure mechanisms"

Technical glitches hit T5 opening

Here are a few of the Terminal 5 features that make us the most proud:

- Terminal 5 offers seamless check-in, with 96 Check-in Kiosks designed to eliminate queuing
- There will be huge improvements in punctuality and baggage now that we've brought nearly all British Airways flights together in one terminal
- The state-of-the-art baggage system has been designed specifically for Terminal 5 using proven technology already in use at a number of global airports

During the first week of operation, BA cancelled ~350 flights and "lost" 20.000 pieces of luggage.

Willie Walsh (BA Chairman, referring to the prospects after the first three days): "I would expect some disruption tomorrow, but I think it will become better as we become accustomed to the building and the quirks of the systems."

Understanding what can go wrong

Smoking cigarettes

Problem is easy to recognise, and the risks are easy to understand.

Consequences are real, and the "mechanism" is well-known

Solution is concrete, although perhaps not very pleasant

See problem and the reasons for it → Consequences and failure "mechanisms" → Tangible solutions

Global warming

Problem is difficult to see, and causes or dependencies are complicated.

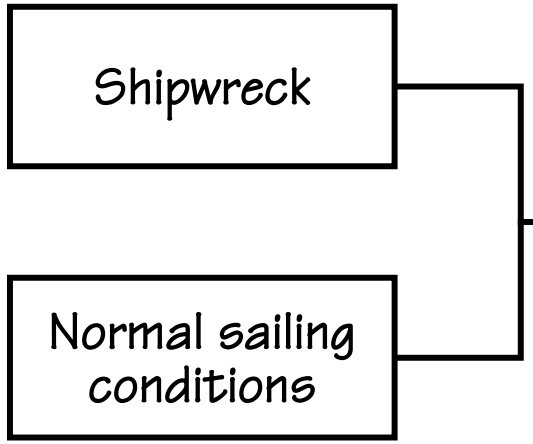
Both short-term and long-term consequences, but often difficult to comprehend

No obvious (!) concrete or effective solutions

Arrhenius, S. (1895). "On the influence of carbonic acid in the air upon the temperature of the ground", Presented to the Stockholm Physical Society.

The warship Vasa

Very serious consequence.
Known and dreaded.



and

Shipwreck during maiden voyage

Not conceivable,

but …

the Vasa did sink on her maiden voyage, Sunday august 10, 1628!

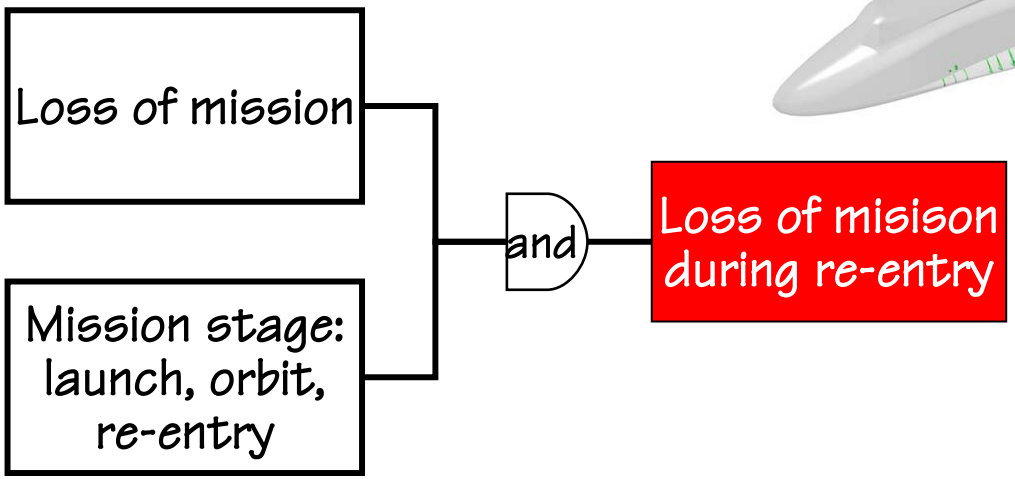
Highly unlikely event; p=0,0

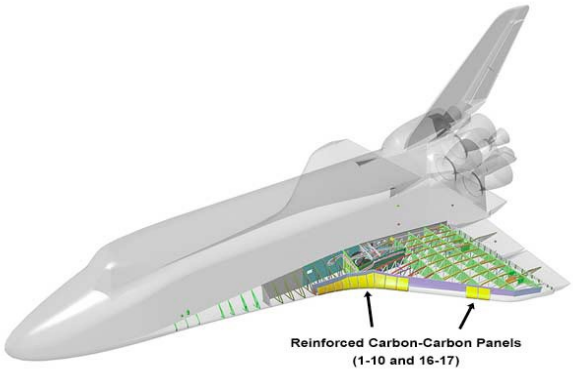
In practice impossible to imagine. No corresponding experience

Blaise Pascal and probability (1654)

Space shuttle Columbia

Most serious outcome.
Known and dreaded





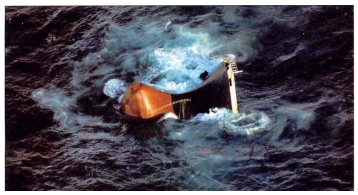
Similar event during first launch, April 14, 1981.

Challenger disaster, January 28, 1986.

February 1, 2003. Space shuttle Columbia: seven astronauts killed when the shuttle broke up on re-entry.

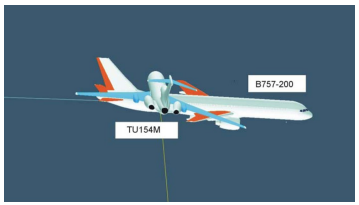
Three categories of threats (Westrum)

I: Regular threats



Events that occur so often that the system learns how to respond.
E.g., medication errors that only implicate a single patient, and potentially can be brought under control.
Effective and affordable responses can be prepared.

II: Irregular threats



One-off events, but so many and so different that it is practically impossible to provide a standard response. They are often unexpected although they are imaginable. (Example: Apollo 13)
Effective responses require improvisation and are not affordable.

III: Unexampled events

Events are virtually impossible to imagine and exceed the organisation's collective experience (Chernobyl, 9/11, subprime crisis)
Responses require the ability to self-organize, formulate and monitor remedial actions.

The necessary imagination

"It was not foreseen that it would be used for a purpose it was not intended for."

Airbus Industrie communications director Clay McConnell (AA 587 Airbus crash, NY November 12, 2001)

"That was a risk factor for avian flu that we hadn't considered"

Epidemiologist Tim Uyeki of the US Center for Disease Control in Atlanta, after a man became infected by sucking a rooster's beak and swallowing the spit and mucus – a technique for clearing the bird's airway apparently common in cockfighting circles.

Cloned meat?

INTERNATIONAL
Herald Tribune

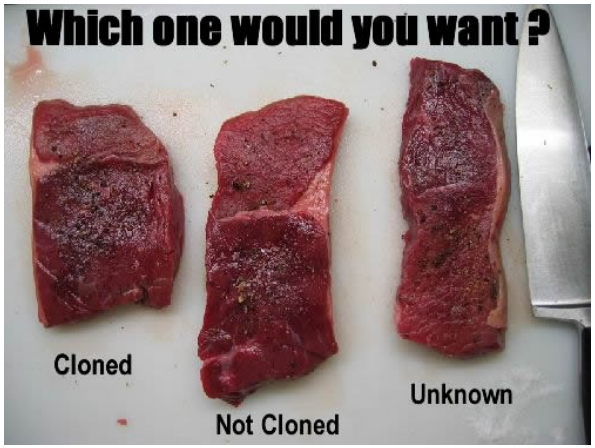
U.S. agency confirms food from cloned animals is safe

By Andrew Martin
Tuesday, January 15, 2008

After years of debate, the U.S. Food and Drug Administration on Tuesday declared that food from cloned animals and their progeny is safe, removing the last government hurdle before meat and milk derived from copies of prize dairy cows and superior hogs can be sold at grocery stores.

The decision comes more than four years after the agency tentatively declared that food from cloned animals was safe, only to face a backlash of criticism from consumer groups and some scientists who said the science supporting the decision was shaky.

On Tuesday, the FDA declared that further studies had confirmed its earlier decision.



"It is beyond our imagination to even find a theory that would cause the food [derived from clones] to be unsafe," Stephen Sundlof, the FDA's chief food safety expert, told reporters.

The disaster that could not happen!

"That 'perfect storm' of a combination of catastrophes exceeded the foresight of the planners, and maybe anybody's foresight" .

Comment by Homeland Security Secretary Michael Chertoff to the hurricane Katrina, September 3 2005

It's only a matter of time before south Louisiana takes a direct hit from a major hurricane. Billions have been spent to protect us, but we grow more vulnerable every day.

The Times-Picayune
"Washing away" - A five-part series of articles, June 23-27, 2002

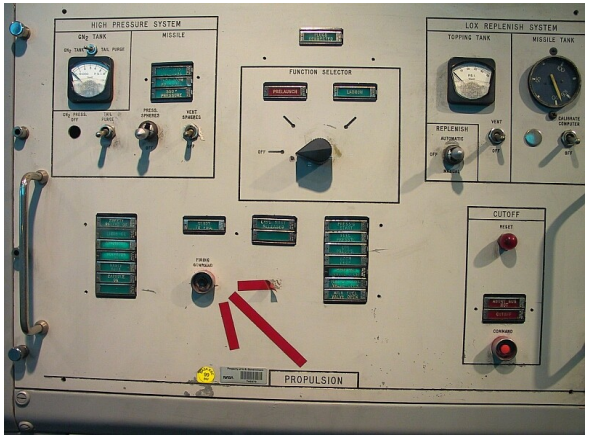
Requisite imagination

Redstone incident

Mercury mission MR-1, 21 November 1960,

(First manned flight with Alan Shepard on May 2 1961),

T - Lift-off
T + 2s Engine cut off, vehicle settled on launch pad after "flight" of a few inches



Escape tower rockets fired to separate the Mercury capsule from rocket, which deployed the re-entry parachutes and landed 1,200 ft. away.

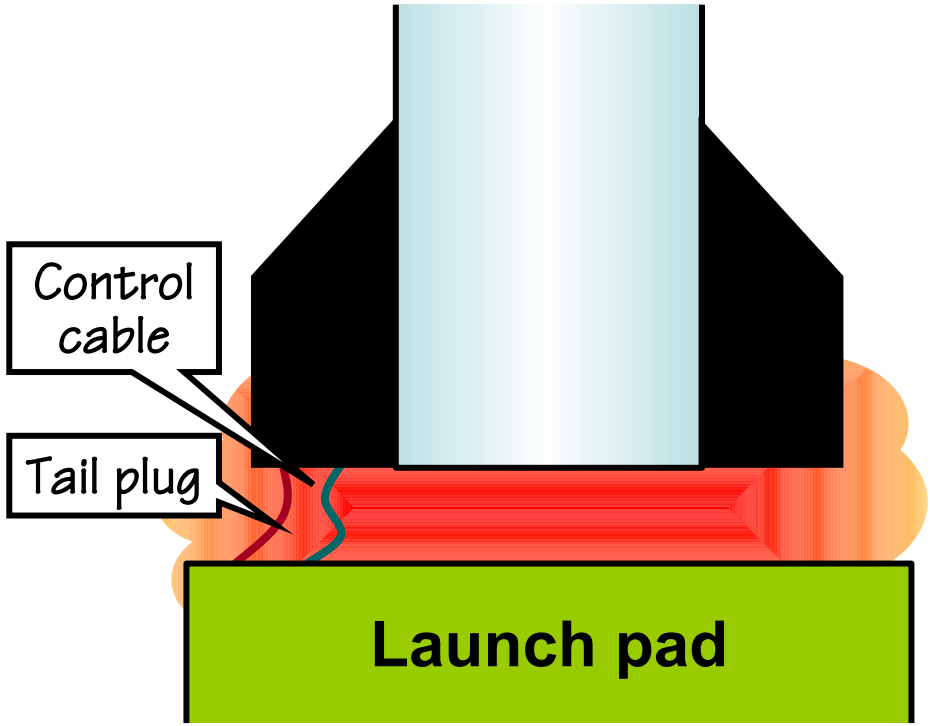
Whole area was cleared for 28 hours as the cause of the engine shutdown was not known and to allow the Redstone batteries to drain down and liquid oxygen to evaporate.

The sneak circuit

The tail plug that connects the rocket to the launch assembly was prematurely pulled out before the control cables.

The tail plug was rebuilt after every launch by cutting back the burned wire and insulation and reinstalling the connector.

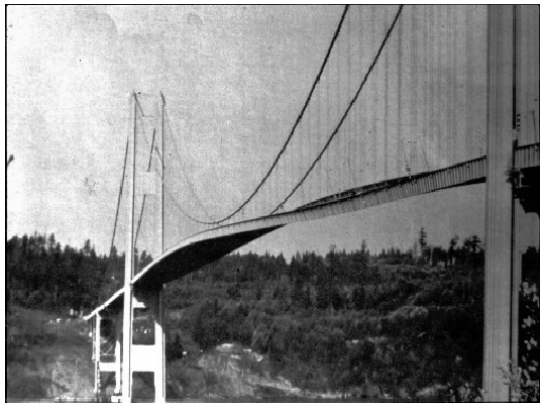
As a result of this, the cable one day became too short and pulled out as soon as the rocket lifted off the pad while the control cables were still connected.



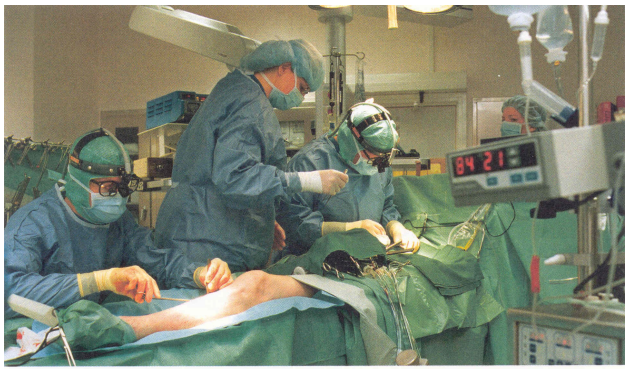
This condition created a sneak circuit, defined as an unintended current path, which causes an unwanted function to occur or which inhibits a wanted function.

How do we know that this is safe?

Design principles:	Clear
Design:	Explicit
Components:	Known
Architecture, composition:	Known
Models:	Formal, explicit
Analysis methods:	Standardised, validated
Mode of operation:	Well-defined, simple
Structural stability:	High
Functional stability:	High
Tractability:	High



How do we know that this is safe?



Design principles:	High-level
Design:	Partially explicit
Components:	Known and unknown
Architecture, composition:	Partly known, partly unknown
Models:	Informal, implicit
Analysis methods:	Ad hoc, unproven
Mode of operation:	Partly defined, complex
Structural stability:	Good
Functional stability:	Good
Tractability:	Low

How do we know that this is safe?

Fully automated
Controlled environment
Flexible only as programmed
Reactive only
But is it safe?

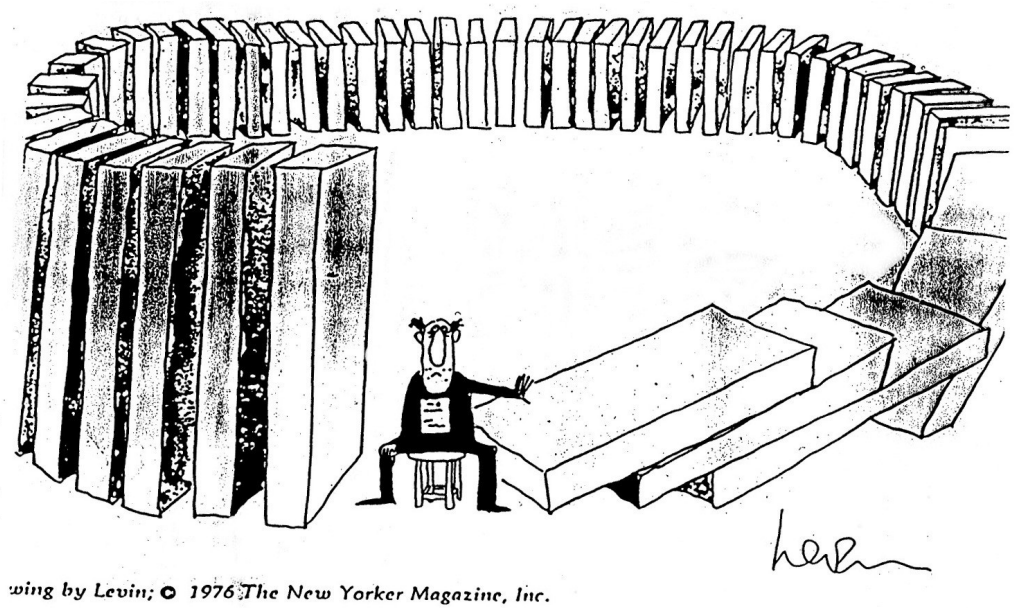
Partly automated
Semi-controlled environment
Flexible and adaptable
Reactive and proactive
But is it safe?

Conclusions

Requirements to understand if something can go wrong:

1. Ability to see that there is a problem and describe what it is.
2. Ability to imagine the consequences and differentiate between large and small risks.
3. Ability to think about solutions that can reduce or eliminate the risks.

Today's socio-technical systems are underspecified, and therefore challenge traditional risk analysis approaches. Today's systems require models and methods that can explain how adverse events can arise from performance variability, as well as from failures and malfunctions. This is the focus of resilience engineering.



wing by Levin; © 1976 The New Yorker Magazine, Inc.

"Deep thought"

I believe that it is important that we recognize that although it is impossible to predict the future, the one thing that is certain is the uncertainty of it.

Tony Blair, Parliamentary debate, March 14 2007
(on whether the UK should maintain a nuclear deterrent.)

We can never avoid the dilemma that all our knowledge is of the past, while all our decisions are about the future

Livet forstås baglæns, men må leves forlæns.

1813 - 1855