

Barriers + Risk = Safety?

Erik Hollnagel
Professor, Industrial Safety Chair
École nationale supérieure des Mines de Paris
Pôle Cindyniques
Sophia Antipolis, France
E-mail: erik.hollnagel@cindy.ensmp.fr

What is safety?

The condition of being **PROTECTED** against failure, damage, error, accidents, or harm.

FREEDOM from those conditions which can cause injury or death to personnel, damage to or loss of equipment or property.

The expectation that a system does not, under defined conditions **LEAD** to a state in which human life is endangered.

The provision and **CONTROL** of work environment systems and human behaviour which together give relative freedom from those conditions and circumstances which can cause ... damage.

Protection
(passive)

Protection
(active)

SAFETY IS FREEDOM FROM UNACCEPTABLE RISK

↑
HOW?

↑
HOW MUCH?

↑
WHAT?

The links between risk and safety

The **conceptual** link:

Risk is defined as the probability that an unwanted event can happen.

Safety is defined as the absence of unwanted events, i.e., the absence of risk.

SAFETY IS FREEDOM FROM UNACCEPTABLE RISK

The **pragmatic** link:

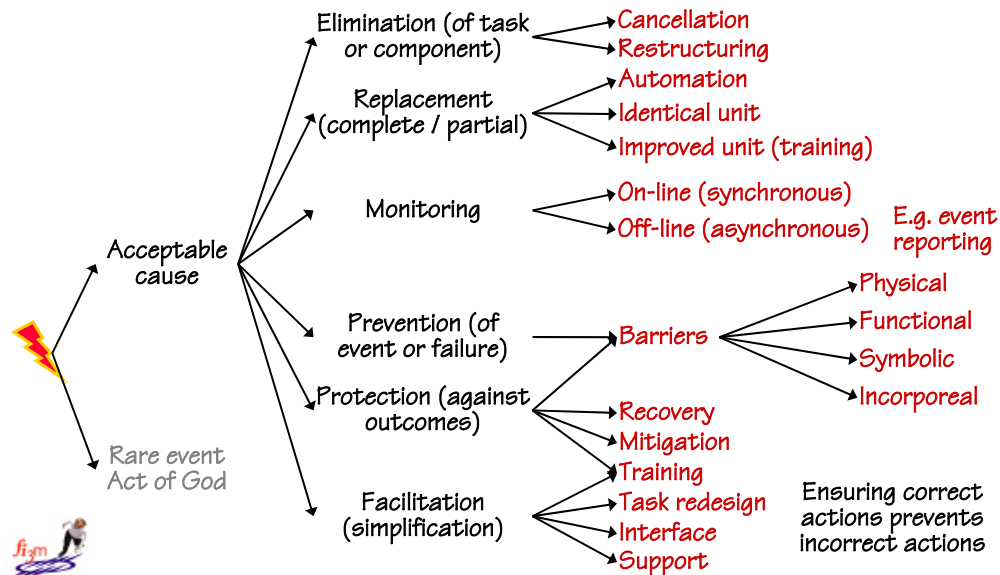
Safety – or rather, the lack of safety – is measured by the number of specified unwanted events, such as accidents and incidents.

A higher level of safety means a lower occurrence of such events and therefore a lower level of risk.

Safety can be achieved either by **preventing** something unwanted from happening or by **protecting** against its consequences. As it is impossible completely to eliminate risks, the two approaches are best used **in combination**.



Reactions to accidents / incidents



Safety through elimination

In order for elimination to work it is necessary that the risks are **known** or can be made known.

This can be achieved via common risk analysis methods + requisite imagination

It is further necessary that the specific risk source can be **removed** from the system without invalidating or markedly changing the system's functioning.

- True **elimination** – loss of primary function (grounding planes after 9/11, or Swedish change from left to right-hand driving)
- Replacement** by **new** but **identical** component/function (for HW only).
- Replacement** by **improved** component/function (upgrading, training).
- Substitution** by **alternative** component/function (upgrading, training).

The H-Day, September 3, 1967

All private traffic was prohibited between 01:00 and 06:00 on September 3. In most places private traffic was prohibited from noon September 2 to noon September 3.

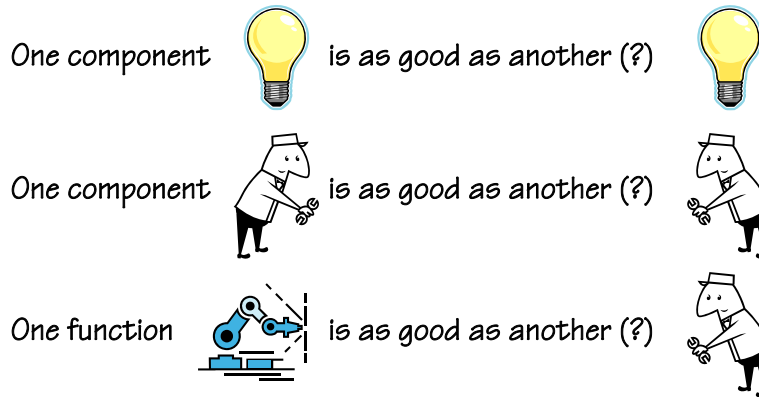


When traffic was allowed from September 4, the general speed limit was 40 km/h, gradually increasing through the following days.

The substitution principle

Elimination through substitution implies the correctness of the **substitution myth**:

Artefacts are value neutral and can be introduced in a system with only local (intended) and no global (unintended) effects.



Prevention and protection

A second option is to **prevent** the critical event from taking place, by hindering preconditions or initiating factors from having an effect.

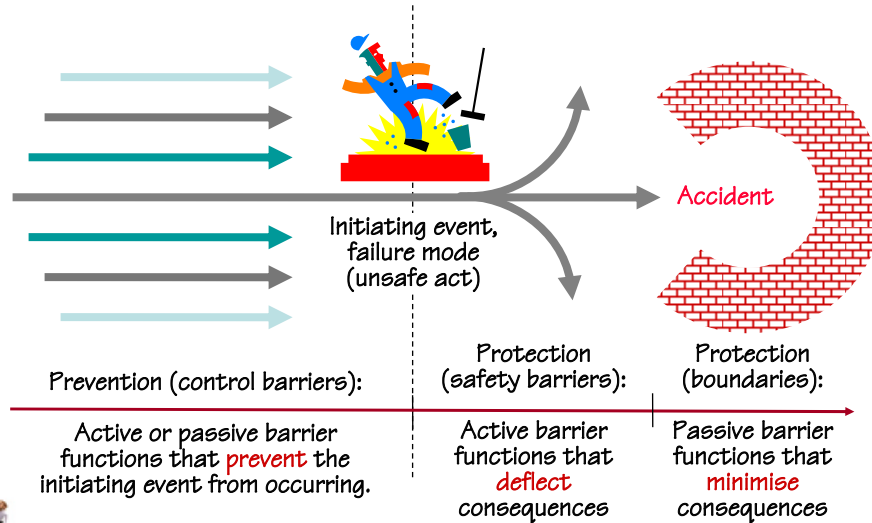
A third option is to **protect** against the consequences of the critical event if or when it happens, by reducing or weakening the consequences or by changing their direction either in a real or in a metaphorical sense.

Prevention tries to **maintain** the functioning of the system and to keep it going, but protection **does not** need to do that. **Protection may indeed require that the system is shut down for a time (e.g., NPPs), or that functioning is reduced until the situation again has returned to normal.**

This is because the primary goal is the safety of the larger system, such as the general population or the environment.

Both prevention and protection are achieved by means of barriers.

Prevention and protection



Barriers and safety

Barriers are obstacles, obstructions or hindrances.

Barrier purpose
(WHY)



- (1) To **prevent** an action or event from taking place,
- (2) To **protect** against the negative consequences if it takes place

Barrier function
(WHAT)



The specific manner by which the barrier achieves its purpose

Barrier system
(HOW)



The foundation or basis for the barrier function, the required organisational and/or physical structure. Barriers can be single or combined (**defence-in-depth**)

Barriers are effective even if the cause is unknown or uncertain

Types of barrier systems

Physical barrier system

A physical barrier system is always ON

Physically prevents an action from being carried out, or prevents the consequences from spreading

Functional (active or dynamic) barrier system

In this system, a barrier can be either ON or OFF

Makes an action impossible via **preconditions** and **interlocks**
May protect against consequences when **activated**.

Symbolic barrier system (perceptual, conceptual)

A symbolic barrier system is ALWAYS there

Requires an act of **interpretation** to work, i.e. an intelligent and perceiving agent (signs, signals, alarms, warnings)

Incorporeal barrier system (non-material barrier)

An incorporeal barrier system is NEVER there

Not physically present in the situation, rely on **internalised** knowledge (rules, restrictions, laws)

Works in and of itself

Requires someone to respond

Barrier systems / barrier functions

Barrier system	Barrier function	Examples
Physical, material	Containing	→ Walls, fences, tanks, valves
	Restraining	→ Safety belts, cages
	Keeping together	→ Safety glass
	Dissipating	→ Air bags, sprinklers
Functional	Preventing (hard)	→ Locks, brakes, interlocks
	Preventing (soft)	→ Passwords, codes, logic
	Hindering	→ Distance, delays, synchronisation
Symbolic	Countering	→ Function coding, labels, warnings
	Regulating	→ Instructions, procedures
	Indicating	→ Signs, signals, alarms
	Permitting	→ Work permits, passes
	Communicating	→ Clearance, approval
Incorporeal	Monitoring	→ Monitoring
	Prescribing	→ Rules, restrictions, laws

Physical barrier systems

Physical or material barrier system:



Physically prevents transportation of matter/energy, or prevents consequences from spreading



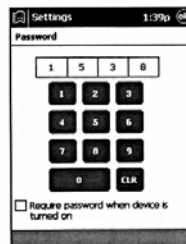
Functional barrier systems

Functional barrier system:

Mechanical (interlocks);
logical (spatial, temporal)



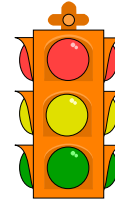
Hinders an action via preconditions (logical, physical, temporal) and interlocks (passwords, synchronisation, locks)



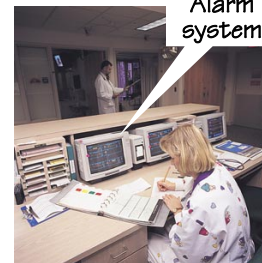
Symbolic barrier system

Symbolic barrier system:

Signs and signals;
procedures; interface
design



Requires an act of interpretation to work, i.e. an intelligent and perceiving agent (signs, signals alarms, warnings)

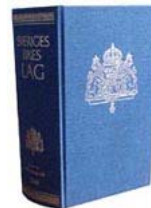


Incorporeal barrier system

Incorporeal (or non-material) barrier system

Rules, laws, norms, principles;
Ten Commandments, Laws of
robotics, "lessons learned"

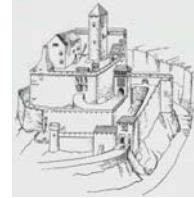
Not physically present in the situation, relies on internalised knowledge (rules, restrictions, laws)



Composite barrier systems

Effective barriers normally rely on a mixture of barrier systems, with the possible exception of specialised physical barrier systems.

Several barriers may be used together to increase the robustness, not least for safety critical applications. Typical examples are the use of *defense-in-depth*, such as in nuclear power plants and in modern automobiles.



Having more than one level of barriers obviously reduce the probability that an accident will happen, although it can never completely eliminate it.

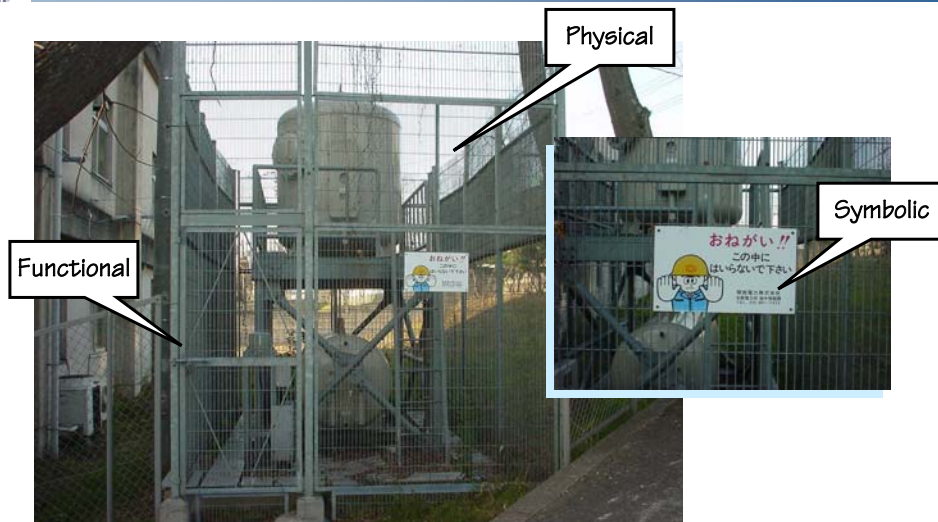
It is important to be able to assess the vulnerability of the barriers that are put in place as well as how they may fail – singly or in combination.

Accident analysis does that by determining which barriers failed and why they failed.

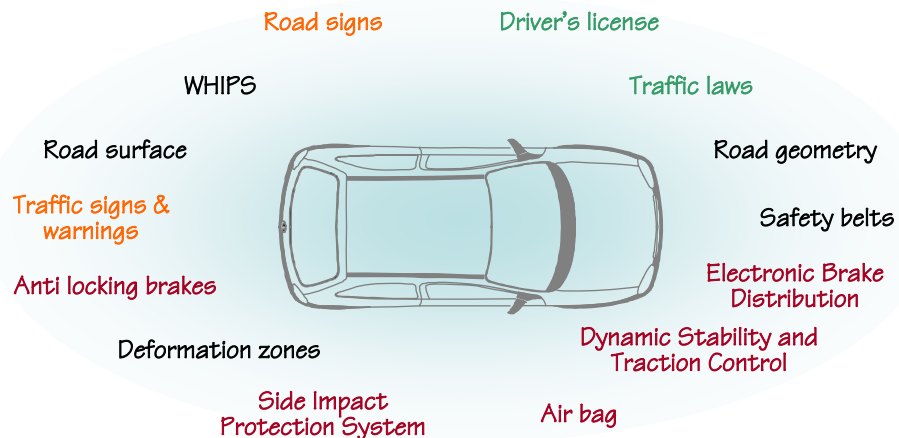
System design and risk assessment do that by identifying how barriers may potentially fail, i.e., what the weaknesses of the system are.

An assessment of the reliability of different barrier systems may be a valuable input to system design.

Physical + functional + symbolic barrier



Multiple barriers in driving



Relative advantages



Incorporeal barrier systems are attractive to managers both because the resource needs are low and the delay in implementation short; but they generally score low on all evaluation categories because they completely depend on the users' willingness to abide by them (safety culture).

Symbolic barrier systems are also relatively inexpensive and can be put in place rather quickly. But their efficiency is low since people can choose simply to ignore them. They are therefore ill-suited for safety critical tasks, at least as the only barrier system.

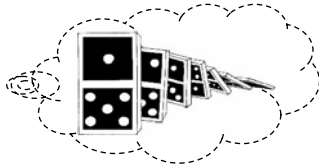


Functional barrier systems are on the whole very efficient, but often require complex preparations and are therefore both costly and lengthy to implement. They can be very reliable, although they may require extensive maintenance.

Physical barrier systems are generally efficient, robust, independent of humans, and easy to verify. But they can be very costly and time-consuming to establish may require considerable maintenance. They are best suited for risks that have been identified as part of the system design process, or that warrant a significant system redesign.

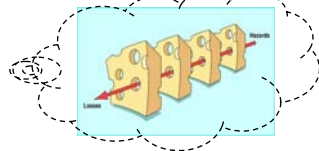


Accident models and barriers



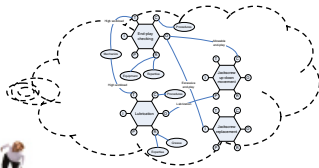
Simple linear model (domino)

Prevention by erecting barriers against harmful external influences.
Barriers a primary means of prevention



Complex linear model (Swiss cheese)

Prevention by maintaining / strengthening barriers, and by hindering the propagation of effects.
Barriers a means of protection but also a concern.



Non-linear model (functional resonance)

Prevention by monitoring and dampening performance variability.
Barriers of limited value ad either prevention or protection.

Different views on the nature of risk

← Looking at the past

Accident model

Simple linear

Complex linear

Non-linear (emergent)



→ Looking into the future

Risk model

Component failures

Regular threats

Combination of failures and degraded defences

Irregular threats

Performance variability, resonance

Unexampled events

Three categories of threats (Westrum)

I: Regular threats



Events that occur so **often** that the system can learn how to **respond**.
E.g., medication errors that only implicate a single patient, and potentially can be brought under control.
Solutions can be based on **standard responses**

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)
Solutions require **improvisation**.

III: Unexampled events



Events that are **virtually impossible** to imagine and which exceed the organisation's collective experience. (E.g. Chernobyl, 9/11)
Solution requires the ability to **self-organize, formulate** and **monitor** a series of responses.

Conclusion: Barriers + Risk \neq Safety!

Barriers are mostly used to prevent something from occurring again, i.e., as a reaction or a response.

The initial responses to accidents/incidents are often symbolic or incorporeal barriers.

Safety can however not be guaranteed only by considering what has happened. It is equally important to **look ahead**, to identify potential new risks, and then to devise barriers against them.

Barrier design must not become entirely reactive, since in that case safety will become a game of constant fire fighting or catching up.

Safety cannot genuinely be improved by looking only to the past and by guarding against accidents that have happened.

Safety must also be **proactive** and look to the future. That requires taking a risk of investing in something that is uncertain. This creates a **safety dilemma**:

If the investment is right, there will be nothing that justifies it or strengthens proactive safety..

If the investment is wrong, there will be plenty of evidence. This strengthens reactive safety.