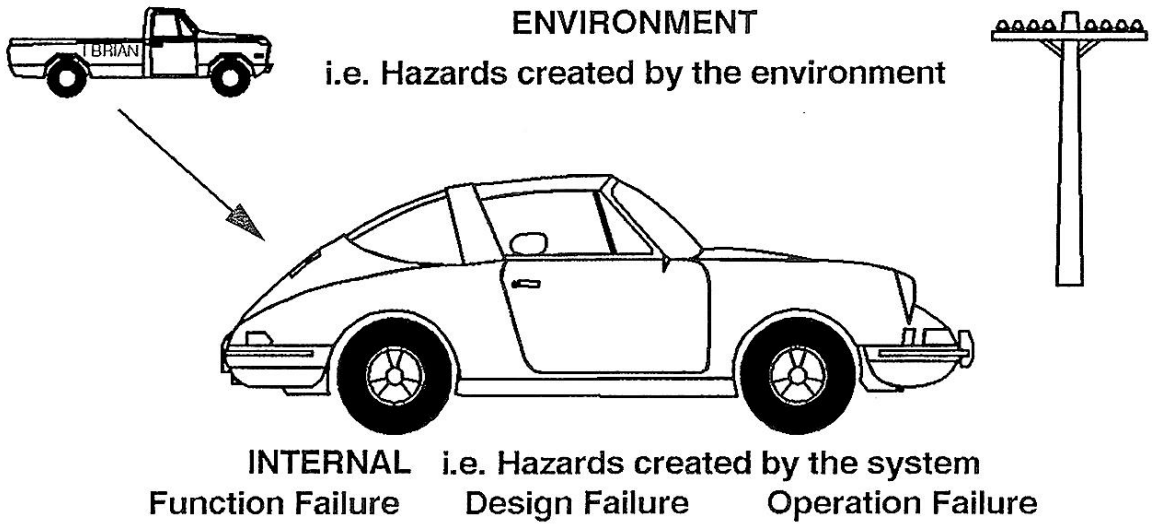
SAFETY

Safety is the protection from inadvertent risks while operating the system.

Safety is strongly linked in with reliability (a highly reliable system tends to also be a safe system) but it is not the same as many other factors come into account - both internal to the system and due to the external environment. Of these many factors that impact safety only "Function failure" is a question of reliability.



SECURITY

Security is the protection from deliberate risks while operating the system.

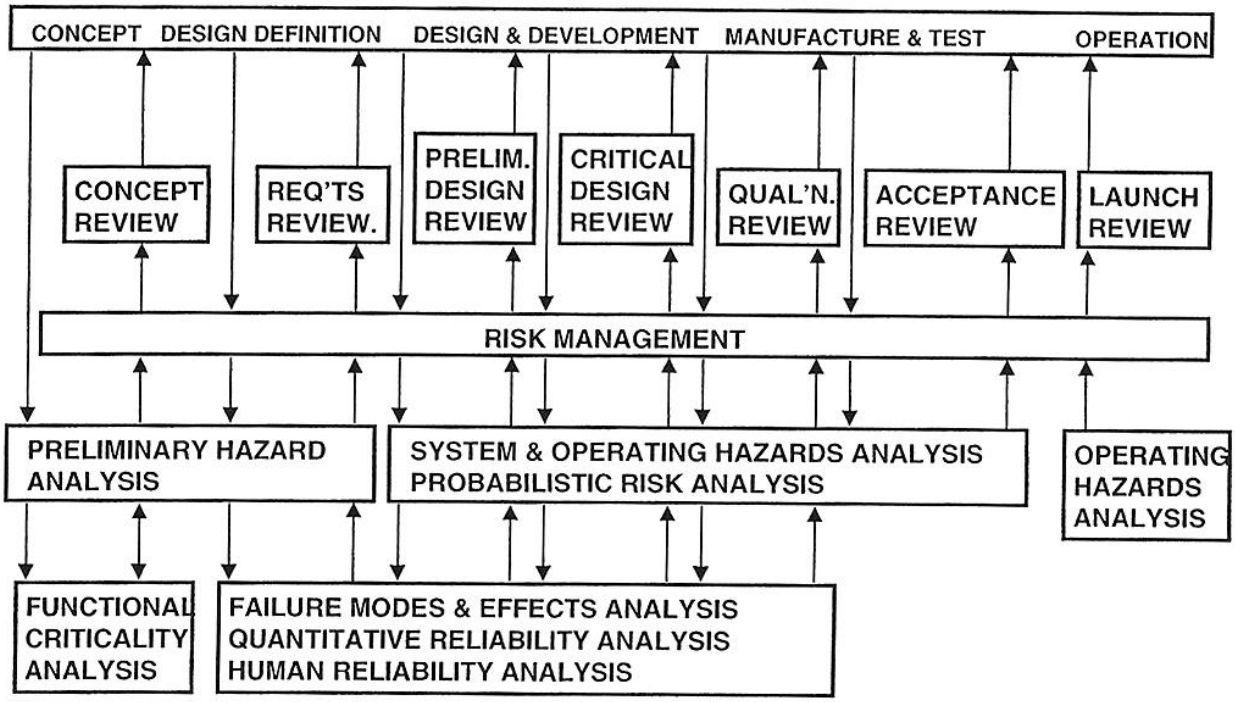
"Deliberate" - as in somebody taking action with intent to harm people while operating the system.

Can result in conflicts between safety and security.
For example:

> Security often drives for minimum access points under tight control (e.g. locks etc.) Safety drives for maximum exits easily to use. Leads to compromises like special exits which only work from the inside.
>
> Security often drives the control of critical functions to be by restricted (using access codes etc.) whereas in many cases safety drives for ease of access.

This lecture is only about safety - but given the prominence given of security it is important you understand the difference and the conflict issues.

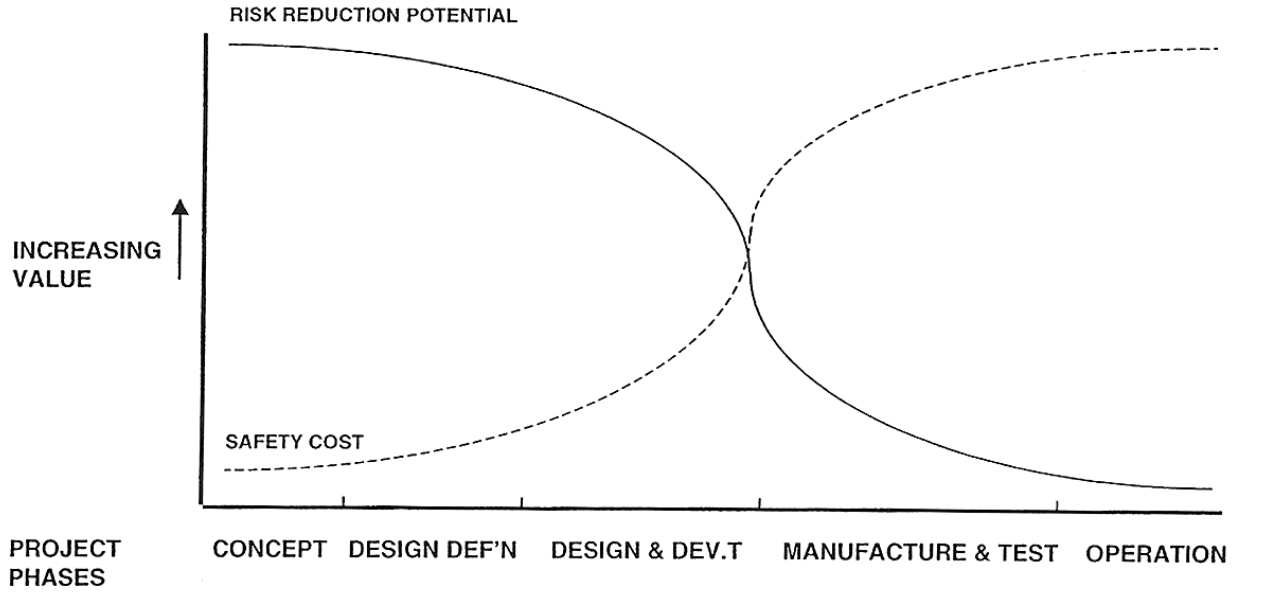
A TYPICAL PROJECT LIFE CYCLE.



Thanks to Keith Wright

SAFETY COST-RISK BENEFIT

Like almost all aspect of system design it is important to put early effort into getting the fundamentals right at the start of the programme. Starting with an inherently safe concept and system design is a cheaper and more certain of achieving a required level of safety than expensive "patches" on an inherently unsafe approach.



Thanks to Keith Wright

SAFETY POLICY

If safety is about protection then what is being protected? This is determined by safety policy.

Who determines safety policy? **Customer** - by safety requirements
Producer - by company policy
Society - by safety legislation

The policy determines what will be protected

People - always a preeminently important system requirement because of ethical considerations of the value of human life.
Animals & Environment - sometimes and probably not often enough
Property - Somebody always has liability for third party claims
The system itself - sometimes.

The policy also determines how much safety. Safety can never be infinitely good, so in the end the degree to which safety is implemented is influenced by secondary factors such as:

Ethical (what is reasonable within society's moral framework)
Cost (system replacement, litigation, clear up etc.)
Publicity (impact on marketing and public support)

In the end decisions on the degree of safety that is implemented within a system are based upon "Risk Analysis".

RISK ANALYSIS

A "Risk Analysis" is not the same as a "Hazard analysis" (see later in lecture). A Risk Analysis is basically a decision on whether it is worth taking the risk.

It has two components
1 - FACTUAL - Assessment of the level of the risk
This can be though a numerical Hazard Analysis, or historical statistics, or wild guess etc.

2 - ETHICAL - Assessment of the Value of the Risk
This normally involves placing a judgement on the value of a human life. Typical value is $1 - $2 million which corresponds both roughly to the earning potential over a working life, and the investment sum to create a reasonable western world income.

This sort of analysis can come up with such conclusions as -it is worth spending a million pounds, but not more, on central barriers on a stretch of road if statistically they will save one life.

In aerospace risk analysis conclusions is that investment in safety should be very high.

- Civil Airliners - The loss of a full 747 (passengers and plane) costs the best part of a billion dollars.
- Military Aircraft - Loss has much lower cost (tens millions of dollars) but risk much higher even with more safety related features.
- Space - Typical loss hundreds of millions but also very high publicity and hence political consequences. Together with other issues (discussed below) this leads to manned spacecraft having more specific safety effort than in general aeronautics.

LEGAL IMPLICATIONS

In theory not meeting the requirement specification can land you in court - but this is actually very rare. With safety issues, problems can quite often end up in court.

For most products - including aircraft - the most common person sued when injury or death is caused by a product is the manufacturer. He is normally the biggest and richest target and with civil aircraft the Warsaw Convention and Montreal Protocols both increase the liability of the manufacturer. To avoid liability a manufacturer must show that:

- the product is not defective or unreasonably dangerous,
- (in addition to the above) that the product is not dangerous (or adequate warning have been given that it is dangerous) when used in a way outside the design range but that could still be reasonably foreseen.
- he has not breached any statutory duties.

With aircraft the manufacturer proves these points before delivery in an issue generically known as "airworthiness".

With Space Systems the legal position is slightly different. The Government of the launching country is responsible for spacecraft. So far Governments have not taken the liability further and sued manufacturing companies but as space gets increasingly commercial this may change.

AIRWORTHINESS

Airworthiness is solely about safety not meeting technical requirements.

Who decides a system is Airworthy (i.e. gives it a certificate of Airworthiness)?

Civil Aircraft - Aviation Authorities
In USA the FAA (Federal Aviation Authority)
In UK the CAA (Civil Aviation Authority)
In Europe -inc UK - JAA (Joint Aviation Authority)

Military Aircraft and Space systems- The customer ministry
In USA DoD, in UK MoD etc.

Civil Space Systems - The Government Agenies
I.e. in USA NASA, in Europe ESA (through governments).

(Note when governments are the customer they also decided the airworthiness but non-government customers are not in control of the airworthiness process of the product they buy.)

These authorities set general airworthiness requirements but in practice these require interpretation on a product by product basis. So early on in the design process the manufacturer will discuss with the authority the interpretation and the test programme to prove compliance.

TRADITIONAL AIRCRAFT APPROACH

The Aviation Authorities method of generating rules primarily relies on historical accidents and incidents to establish good design and operational practice. Hence the importance of incidence reporting and accident investigation to maximise the lessons that can be learnt (compare with what happens after a car accident).

This is not a "systems engineering" method as it does not view the system "Top Down". It is closer to Darwinian natural selection as a process.

Example of this approach see "Design for Safety" by David B Thurston.
His book starts with the statistics of accidents and then shows methods of designing to minimise the risks with amount of space devote corresponding roughly to the frequency of the problem

Pilot error biggest single cause (but getting better: 1948 - 75% of accident 1977- 58%). The book works through statistical causes and best way of dealing with them

In more detail: Failure to maintain flying speed 1948 - 7.25%; 1977 -5.78%
- book considers improving stall characteristics
Failure to see obstacles etc. 1948 5.5% ; 1977- 2.16%
- book considers instrument an cabin design.
Failure of fuel supply management 1948 - 2.97%; 1977 - 2.95%
- book has section on fuel system redundancy
Failure of power plant management 1948 - 4.18%; 1977 - 1.17%
- book considers engines and engine instrumentation

AND SO ON

SAFETY METHODOLOGY

In Aerospace systems engineering (especially space) safety is addressed by establishing methodologies. Examples:

European Space Agency - Uses a scenario approach based on a "scenario sentence"

HAZARDS in the SYSTEM DESIGN are manifest in HAZARDOUS CONDITIONS which depend upon the occurrence of INITIATOR EVENTS can cause UNDESIRABLE EVENTS that combined with EXPOSURE SITUATIONS result in CONSEQUENCES

The safety analysis aims to identify all the aspects in capitals in every hazardous scenario.

NASA - Uses a methodology to analysis safety with analysis stages linked to phase in the project lifecycle.

Identify all potential critical and catastrophic hazards (in phase A)
Identify all credible causes of these hazards (in phase A)
Identify methods of controlling the causes (Phase B)
Identify methods of verifying that the controls are intact (Phase C)
Verify that the controls are intact (Phase D)

REAL LIFE "EXPERIENCE" AND "SCENARIO" APPROACHES

System development programmes in practice use both but as we have seen in aircraft (and most other industries) the emphasis is on safety requirements based on experience.

Why? Because it works! People have been flying for over 90 years - Over a billion passengers fly each year - and aircraft are very reliable and safe. Large volume of experience and very extensive investigation of such incident that do happen lead to large body of rules, design guidelines and forbidden practices.

However in space systems (and other immature industries) where the background experience simply does not exist there has to be a greater reliance on scenario approaches. As the paper below from Keith Wright points out this is more expensive and not as effective.

The reason is simply the limitations of the human imagination - even large groups of experts putting considerable effort into scenario development will still miss things. Generally while the obvious points are covered the subtle and unusual are missed and these need to be addressed if aircraft like safety is to be achieved.

The risk of loosing the Space Shuttle was assessed as between 1 in 230 missions and 1 in 76 missions (5th to 95th percentile). Compare with civil aircraft risks of 1 in 2,000,000 hours in 1990.

Notes from
SPACEFLIGHT - REDUCING THE RISKS by Keith M. Wright
A paper presented at British Interplanetary Society symposium on The Popular Commercialisation of Space
September 2001

THE REASONS SPACE SAFETY IS EXPENSIVE AND LOWER THAN AIRCRAFT.

- THE CONTINUED APPLICATION OF "IMMATURE" TECHNOLOGY AS PART OF THE DEVELOPMENT OF NEW OPERATIONAL SYSTEMS (PARTICULARLY FOR SPACE TRANSPORTATION);
- PUSHING THE LIMITS OF PERFORMANCE RESULTS IN TIGHT DESIGN & OPERATIONAL MARGINS;
- THE PARTICULARLY HAZARDOUS CHARACTERISTICS OF SPACE SYSTEM TECHNOLOGIES & THEIR OPERATING ENVIRONMENTS;

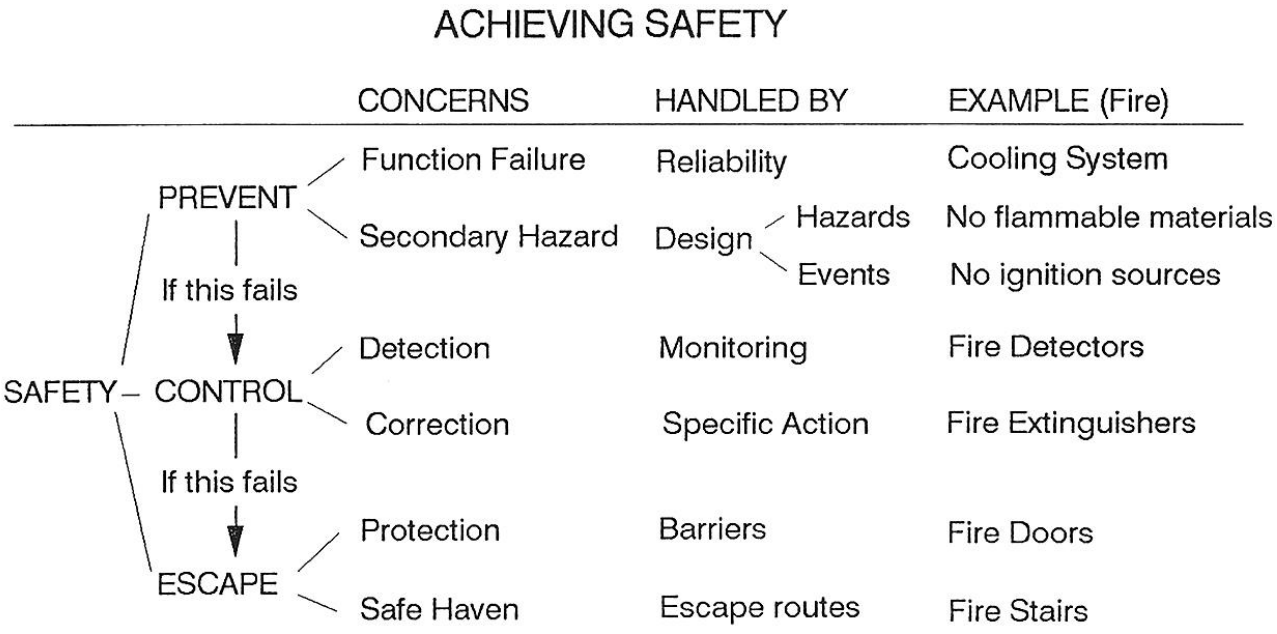
THIS RESULTS IN A VERY COMPLEX SPACE SYSTEM DESIGN, DEVELOPMENT & VERIFICATION PROCESS.

DISADVANTAGES OF THE CURRENT PRACTICE.

- THE PROCESS IS COMPLEX AND EXPENSIVE;
- RELIABILITY & SAFETY ANALYSES ARE BASED ON A MODEL OF THE SYSTEM DEVELOPED BY THE ANALYST BASED ON THE DESIGN DATA AVAILABLE, & HIS/HER UNDERSTANDING OF THAT DESIGN;
- THE SAFETY & RELIABILITY ANALYSES TEND TO LAG THE DESIGN PROCESS RATHER THAN DRIVING IT OFTEN RESULTING IN LESS THAN OPTIMUM DESIGN SAFETY (LEAST HAZARDOUS TECHNOLOGY AND SYSTEM CONFIGURATION).

RECOMMENDATIONS .

- SEPARATE TECHNOLOGY DEVELOPMENT FROM OPERATIONAL SYSTEM DEVELOPMENT (USE "OFF-THE-SHELF" TECHNOLOGY);
- INCREASE PERFORMANCE MARGINS BY THE CONSERVATIVE APPLICATION OF PROVEN TECHNOLOGY;
- DEVELOP A STANDARDISED SET OF RELIABILITY & SAFETY REQUIREMENTS & PRACTICES;
- PROVIDE JUSTIFICATION RATIONALE FOR ALL TECHNICAL REQUIREMENTS AND PRACTICES;
- INTRODUCE AN INDEPENDENT OVERSIGHT PROCESS.



PREVENTION

Obviously the first and most desirable approach to achieving safety is not to have a hazardous situation develop in the first instance. So the first line of defence is to minimise the systems ability to create hazardous situations.

For each component of the system two questions must be asked corresponding to the two ways a component can become a hazard.

1. What happens if the component fails to perform its function? Sometimes this is a safety question (brakes on a car) sometimes it isn't (car radio). It is this aspect of safety that is a question of reliability.

2. Does the component represent a secondary hazard. This can range from having some exposed sharp edge to containing a couple of kilograms of Plutonium. Example a car radio may be a fire ignition risk due to shorting even though it is not a function hazard.

Having identified the possible failures, the system can then be designed to either eliminate them or to minimise them. With function failures the only way to improve safety is to improve the reliability. With secondary failures, practices like using non-flammable materials, rounding sharp corners, "leak before burst" pressure vessels etc. are the methods used to improve safety.

A WARNING: FUNCTION FAILURES

Systems can often be dominated by one class of hazard and the safety practices for different types of system often reflect this.

Dynamic systems (e.g. cars planes) tend to emphasise Function Failures - this leads to reliability and redundancy as major concerns.

Static systems (e.g. buildings) tend to emphasis secondary failures – this leads to hazard control being the prime concern.

The Warning: - A common problem when function failures dominate is to forget about secondary hazards.

An example Apollo 13: redundant oxygen tanks gave adequate reliability to minimise risk due to function failure. Problem was the tanks were placed side by side so when one tank exploded (the most likely failure mode) the second tank was taken out as well.

It can also lead to inappropriate system design practice. For example designing space stations as if they were launch vehicles.

An Example of how system overall function can alter the emphasis between Functional failures and general hazards.

COMPARISON OF SAFETY IMPACT OF SUBSYSTEM RELIABILITY
LAUNCH SYSTEMS Vs SPACE STATIONS

The most likely impact of a subsystem failure during the mission.

	MANNED LAUNCH SYSTEM			SPACE STATION		
SUBSYSTEM	IMPACT	CREW ACTION	TIMESCALE	IMPACT	CREW ACTION	TIMESCALE
Structure	Complete Loss	Attempt escape	Seconds	Performance	Repair	Days
Electrical power	Complete Loss	Attempt escape	Seconds	Data Loss	Repair	Hours
Propulsion	Complete Loss	Attempt escape	Seconds	Orbit Decay	Repair	Months
Guidance	Complete Loss	Attempt escape	Seconds	Pointing Loss	Repair	Indefinate
Communications	Various	Mission Abort	Minutes	Data loss	Repair	Indefiniate
Life support	Crew health	Mission Abort	Hours	Crew health	Repair	Days
Thermal Control	Complete Loss	Attempt escape	Minutes	Performance	Repair	Days
Control Actuators	Complete Loss	Attempt escape	Seconds	Pointing	Repair	Indefinite
Data Handling	Complete Loss	Attempt escape	Seconds	Data loss	Repair	Indefinite

Conclusions: Launch systems functional failures are safety significant therefore reliability needs to be high. On Space Stations safety is dominated by general hazards, so hazard control rather than reliability is the issue.

HAZARD ANALYSIS

The Hazard analysis is the key part in a systematic implementation of a safety methodology. Mostly used to identify the method the system designer will use to eliminate or minimise a potential hazard.

It is similar in form to a FMECA

Aims to identify every potential hazard (functional and secondary) in the system and any remedial action to be taken about it. It should follow the safety methodology being used to control safety.

The example here is from HOTOL shows part of analysis of Electrical Ground Support Equipment (EGSE). Note this analysis follows the ESA methodology and also the way hazards are categorised.

CATEGORIES OF HAZARDS

During a Hazard analysis potential Hazards are normally categorised in some way. This is used to determine the action to be taken. The following is an example (practice can vary).

Catastrophic - Potential loss of human life

Critical - System loss, Human injury

Marginal - Damage to system, Minor injury to humans

Typically rules that might apply during system design/hazard analysis is no two system failures shall lead to a catastrophic hazard. i.e. Three things must go wrong for life to be at risk. This rule was supposedly used on the Space Shuttle but the Solid Rocket boosters joint did not meet this requirement, that lead to the Challenger accident.

Another rule might be no single failure should lead to a "contingency situation". A contingency situation is where one or two more failures leads to a catastrophic hazard. This requires a departure from nominal activity to correct the situation.

CONTROL

If prevention fails then the next step normally is some specific action to control the hazard and eliminate its consequences.

E.G. If you have fire - put it out.

Control nearly always means adding special hazard control elements in to the system

E.G. Fire extinguishers.

If there is a system element those function is to control a specific hazard it must have a means to triggering it. That is there must be a method of detecting the hazard which feed back into the hazard control equipment.

E.G. Fire alarms as well as fire extinguishers.

NOTE: a common mistake - insufficient concentration on detection process.

ESCAPE

The last resort - if prevention and control fail - get out! To do that there needs to be a safe place to go to.
Buildings etc.- normally easy outside.
Ships - more difficult as the sea dangerous therefore lifeboats etc.
Aircraft - even more difficult leaving aircraft only achievable with a Parachute otherwise the plane must land first.
Space - Long term manned facilities need lifeboats and safe haven areas. Short term system normally have escape systems during launch (except the Space Shuttle which most needs it).

But you need to be able to reach these "Safe Havens". This means: - Planned escape routes - that work during the emergency conditions. This means:- Protection Systems

Protection means barriers between what you are protecting (normally a person) and the Hazard. These can be:

Specific to the hazard - Local protection around a likely hazard source
General - general blocking such as a fire wall or door
Specific to the person - Gas masks, protective clothing

Another point about escape routes: Two separate routes is always desirable (and in some cases specified). Many hazards like fire can cut off one route trapping the people trying to escape.

(Footnote: Escape has acquired an unfortunate connotation within NASA - "Assured Crew Return" is current jargon)