

Chapter 2

Active System Control and Safety Approach, and Regulation in Other Application Domains

Approach to Safety in Critical Systems

This chapter aims to analyse the currently available safety systems both in aviation and other fields where safety is considered to be a critical aspect.

In addition, this section reviews the currently available aircraft safety systems for general aviation (GA) operations and aspects affecting their design (including the associated economics).

Drawing on an analysis of these safety systems—their deficiencies as well as innovative concepts from fields other than aviation—a comprehensive basis for specification and a practical and more effective approach for the future is proposed.

Safety systems are already well established in other transport domains that share many characteristics with the GA domain. In this section, current approaches and trends in the automotive, space and railway domains are surveyed, particularly for on-board safety systems. The term “vehicle” is used to refer to a car/truck, spacecraft, train or plane, across all domains.

For a number of decades, the emphasis on safety systems in various fields of application has been “passive”, for example, protective bars in a car’s frame and data recorders for post-accident analysis. Increasing efforts have recently been made to introduce systems that will react in the event of an accident/incident, or the impending possibility of one, with the aim of minimising the effects of such an undesirable situation in terms of both human and material losses.

Although these systems are classed as “active” by each related industry, they are lacking in terms of both scope of application and capabilities when compared to the principles introduced for active safety. For example, a car’s airbag might be activated to minimise injury, but the vehicle immediately becomes undrivable. If the activation is erroneous, then the consequences can be disastrous.

Safety Approach in Industrial Systems and Machinery

Industrial systems span a wide spectrum of applications and sizes. From a safety management viewpoint they fall into two main areas: (1) systems that protect individuals from injury in the workplace and (2) systems that control dangerous processes that could cause serious loss of life and/or environmental damage. As with rail, space and aviation, major public accidents usually highlight the risks and harms; these have led to regulations being put in place, for example:

- Chemical process plant, Bhopal, India: a huge chemical explosion followed by a poison gas cloud drifting over a large city and its surrounding area. Hundreds were killed and thousands injured at the time, followed by years of blight on the local community and continuing environmental damage.
- Nuclear process plant, Chernobyl, Russia: nuclear reactor explosion and meltdown. Safety system overridden by operators for experimental purposes. Nuclear explosion and core meltdown, contamination over a wide area, thousands of casualties and continuing long-term environmental danger.
- Concorde, Paris, France: rupture of fuel tank from runway debris, leading to a crash and fire in a built-up area.
- Space shuttle, Florida, USA: launch attempted with rocket fuel seals below the recommended temperature, leading to a cataclysmic explosion of the vehicle in flight, killing the astronauts aboard.
- High-speed train, Eschede, Germany: a high-speed train derailed and crashed into a road bridge. A total of 101 people died and around a hundred were injured. The crash was caused by a single fatigued crack in one wheel, which, when it failed, caused the train to derail at a set of points (switch).

Approach to Safety in Process Plants

High-profile accidents have gradually led to a much tighter definition of responsibility for safety and also mandatory use of safety analysis and design techniques to prevent, avoid and/or mitigate harm. Typically, in safety-critical process control applications (e.g., chemical, nuclear) highly available systems are needed to support continuous (i.e., uninterrupted) operation of the plant.

This is often achieved by duplicated or triplicated systems, with voting being used to compare the results of each control channel, to guard against through-life software and hardware failures. Sometimes diversity of implementation of the control system is also used in an attempt to avoid common-mode failures (and to improve veracity rather than availability). However, a lack of clarity often exists on how these techniques are used, particularly when hardware design techniques (used to mitigate against random physical failures) are applied to software design. *A system view of hardware and software together is required, because both suffer from errors of implementation, but only hardware suffers from random failures.*

However, this may also affect software, for example, by radiation corrupting a value stored in a memory chip.

The Importance of Human Factors

Unfortunately, aspects of the human factor are less than adequately addressed in many systems. The classic example is the Three Mile Island nuclear plant accident in Pennsylvania (USA) in 1979, where over 50 sirens were simultaneously sounding in the control room—making it impossible for the staff to understand the significance of each siren or to concentrate on what to do next to mitigate the harm.

Three Mile Island is also a good example of added complexity inducing failure. The incident was triggered by a sensor, which was added to an existing safety sensor to check it, that is, with an intention to improve safety. The check sensor incorrectly indicated a fault in the main sensor, resulting in “preventative and corrective actions” by the control system and the control staff, which resulted in a cascade of errors—all predicated on the initial false indication. See the excellent book by John Gall (*Systematics*).

The Safety Lifecycle and Trends

Modern plants are now designed with safety in mind, rather than as an afterthought. The safety case for any new plant covers the operational process safety, the safety credentials of each piece of equipment and their interoperation as a whole control system. All phases of the plant lifecycle are covered including specification, design, construction, proving, operation, shutdown and decommissioning. It is conventional in safety critical plants to physically record a wide variety of significant operational data on a continuous basis—the “wall of chart recorders” being a familiar sight in production plants (e.g., chemical, oil, nuclear). Of course, these chart recorders are now being superseded by the equivalent of aviation’s black box recorder, which also has the advantage that it can be remote from the plant being monitored.

Approach to Safety in Small Industrial Systems

In small industrial systems, improvement has been driven by stringent workplace regulation and also the threat of litigation. All machinery that could cause injury to its operator, or to people working adjacently, must be designed to be safe. The normal reaction of such systems is to bring the machine to a safe state and/or disallow access to the operator in a particular area. The concept of “safety interlocks” is similar to that used in the rail sector, where all relevant preconditions need to be in an appropriate state before a potentially unsafe action is allowed to occur.

Most small systems (e.g., a lathe) do not keep through-life records of safety incidents or operational data. However, it is quite common now for larger automation systems to retain this data, which is then analysed to support “preventative maintenance” and recalibration at some convenient time.

The Trend to Design Standardisation

Over the past decade there has been a strong movement to standardise control systems. This has been spearheaded by the CiA (CAN in Automation), an organisation that promotes the CAN (controller area network) bus, which is now in widespread use in automobiles, trucks, trains and GA aircraft as it offers an effective method of collecting and distributing data over a robust and deterministically timed serial bus, a low-cost system originally specified by Bosch GmbH.

The CAN scheme has been adopted by the main US control system suppliers, such as Honeywell, using proprietary names. The original CAN communications protocol has now been joined by two additional abstractions:

The first is CAN Open which provides a standard model for interfacing devices within a system, making system configuration much easier and enabling a mass ‘plug and play’ market in CAN-compatible devices such as switches, lamps, level sensors, shaft encoders, stepper motors, etc.

The second is a CAN safety protocol for data transmission of safety critical data. It is embedded in a chip, and based on the concepts of functional safety, it is certified by TÜV SÜD for SIL level 3 safety applications. With his radical innovation, for the first time safety support had been prepackaged into a standard integrated circuit. The users of the chip just need to add in an algorithm that customises the component for the specific safety requirements regarding the device and its context of use. It is interesting to note that the Bosch and CiA collect royalties on the CAN bus and safety chip by means of a royalty built into the cost of the IC components required to build CAN-based systems.

A variety of other connectivity standards are in use including Profibus. There is a renewed interest in a variant of Ethernet which provides a systemwide traffic management scheme to achieve determinism of message delivery timing (i.e., timed Ethernet).

Although industrial systems have tended to lag behind rail, space and aviation systems in terms of safety, there is now a strong motivation to design safe systems. This continues to be driven in the USA and Europe by regulations and the threat of litigation, and a systematic standards framework is in place to support it, based on ISO 61508 (ISO 61508, ISO 26262).

It should be noted that most of the standard data bus schemes and protocols currently in use have no security protection. In the new age of the Internet of Things, this is a major concern.

Safety Approach in the Automotive Industry

The automotive domain has many similarities to GA—the vehicle is relatively small, carries only a few passengers (or just the driver), and often the driver is the owner. There is great flexibility for the use of the vehicle and the variety of destinations and routes that can be used, but far more than in commercial aviation or railways.

Current On-Board Safety Systems

The automotive community has invested heavily in on-board safety systems, driven by an active customer base (spearheaded by Ralph Nader in the 1960s), the appetite for litigation in the USA (and now Europe) and the demands of government regulators. On-board safety improvements have taken many forms including those described in the following sections.

Physical Safety Systems

Physical safety systems are concerned with the physical safety of the driver, passenger(s) and other road users, for example, via passive systems such as seat belts, crumple zones, roll cages and laminated glass, or active systems such as airbags. Such systems seek to mitigate harm during or after a crash rather than preventing the crash in the first place. More recently, systems have been introduced that continuously monitor the state of wear/expected operational lifecycle of the safety-related components and subsystems within vehicles. These systems provide advice to the driver on the roadworthiness of the vehicle, but the driver is still responsible for the safety of the vehicle he or she is driving.

Route Safety Systems

Route safety systems are concerned with ensuring that the route being taken is safe, that is, within the vehicle's and driver's capabilities and free from risk of collision. These systems are in their infancy in the automotive domain, currently taking the form of navigation aids and marketing aids. This is partly due to the complexity of the task given the existing road infrastructure and immature technology (low-resolution positional tracking, lack of coverage in tunnels, etc.). Presently, navigation systems are *advisory* to the driver rather than contributing to the actual control of the vehicle. Some systems have recently been introduced, external to

vehicles, to dynamically control the flow of traffic, for example, adaptive speed restrictions on motorways. These systems are also preventative in nature.

Driving Safety Systems

Driving safety systems are concerned with improving the safety of the vehicle behaviour. This involves compensating for or enhancing the driver's control of the vehicle, for example, via traction optimisation, anti-skid compensation, anti-lock braking and speed governing. Some systems provide advice for the driver, while others actually control aspects of the vehicle directly, intervening in the way it is actually driven with the objective of improving on the driving capabilities of the driver.

Driver Safety Assurance

Driver safety is concerned with assurance that the driver can be identified, has the capabilities to drive the particular vehicle, and is currently able to drive the vehicle, that is, the driver's performance is not impaired by illness or intoxication. This may also have a security dimension, for example, with a bullion truck that may only be driven by specific drivers.

Currently there is no automotive equivalent of aviation's autopilot or the railway's "driverless train," as such systems (e.g., from Uber and Google) are still at the research stage. Some initial schemes are in place such as cruise control (possibly adaptive to local road conditions), safe braking distance control and cooperation schemes such as convoy management for creating "trains" of vehicles. Trials were held in Europe in 2016 to evaluate the practicality of "vehicle trains" and "self-driving" cars. Of course, these vehicles are not really "self-driving"; responsibility for driving has been taken over by a network of computers, programmed by programmers, some in the local environment and some by third-party providers. It is not yet clear how responsibility for incidents with self-driving cars, possibly causing injury or death, will be apportioned between the vehicle owners, vehicle manufacturers, guidance providers and navigation and safety system providers.

Safety Improvement

Safety in the automotive domain is improved mainly by regulation, litigation and competition. Regulation, as in the railway, space and aviation domains, has tended to be motivated by events. Really serious accidents have caused a tightening of regulations in an effort to prevent a recurrence of similar accidents, or at least to

mitigate the harm caused. Major accidents are analysed, the causes and hazards are identified, and reports are produced that offer recommendations for safety improvements to processes, systems and equipment. There have been some recent notorious examples where commercial gain has taken precedence over the safety of products and their users, for example, exploding petrol tanks, and lethal tires for 4×4 vehicles.

In some cases, new systems aimed at improving safety have actually led to increased harm, even fatalities. A recent example was an engine management system that, in attempting to protect the engine from over-revving, prevented a driver from completing a takeover manoeuvre, thus killing the driver. So it always needs to be borne in mind that safety must be considered pervasively, being the sum of effects of each system and all their inter-reactions.

A feature of the automotive market is that safety has been a major factor in building brands, good examples being Volvo and Audi. So far this kind of competitive advantage has been evident in the areas of physical safety and driving safety. So far, driver automation has been hampered by current technology and perhaps the drivers' own perceived need to remain "in control." Future systems may offer improved safety with features such as lane management and control of speed relative to the local environment and weather. Eventually full automation can be envisaged, the passengers simply specifying the destination and perhaps some interesting way-points to determine a desirable route. Of course, this could offer enormous safety benefits, eliminating collisions and the driver's mistakes, fatigue, illness and possible abuse of alcohol or other drugs. However, when accidents happen, as they surely will, then who will be responsible and therefore be held accountable? Will it ever even be possible to apportion blame?

Operational Safety Cycle

Operational checks for on-board safety are already widely used in the automotive domain. The typical life-cycle involves:

Maintenance

Here a wide variety of vehicle parameters is available that provide a basis for diagnosing faults, assessing wear on parts and how the vehicle has been used. Typically, the on-board computer records the absolute data, for example, brake pad wear, and summaries of operational data, for example, cumulative distance travelled and engine speed profile. This can be downloaded into a diagnostic computer and then analysed to provide guidance for the servicing and repair of the vehicle. The maintenance system may also upload parameters to the on-board system in order, for example, to improve its driving characteristics or enhance overall safety.

This approach can and has been taken to extremes. In Formula 1 racing, telemetry is used to continuously monitor the performance of the vehicle and driver and then to optimise the vehicle systems on-line and interactively and advise the driver. The emphasis here is, of course, on performance rather than safety. For most automotive vehicles, however, there is only one mandatory vehicle maintenance per year to ensure that the vehicle is safe to drive.

Checks at Start-Up of Vehicle

Many safety-related checks are made during the start-up of the vehicle, for example, tire pressures, doors closed, oil pressure, coolant level, etc. In specialised applications where security is involved there may be additional automatic checks on the driver and passengers such as identity biometrics (e.g., iris scan, fingerprints, voiceprints), weight, alcohol in breath, licence validity and passwords.

The objective here is to ensure that the vehicle is safe to drive and that the driver is entitled and fit to drive it. There is no formal safety check of the vehicle during the start-up phase, at least not for car drivers. However, commercial and security vehicles do have safety checklists that must be successfully completed before the vehicle can be used.

Checks During Operational Use

Many checks recur during operation with feedback provided to the driver, normally as warnings or advice. Examples of on-going checks are oil pressure, water temperature, fuel level, fuel efficiency, impact detection (to deploy airbags), over-rev detection, etc. Insurance and litigation concerns initially ensured that the driver was in sole control of the vehicle. However, many ancillary systems, such as anti-skid compensation and anti-lock braking, are now well-proven enough that they are trusted to take some control from the driver. To put it another way, they enhance the driver's apparent performance and safety by compensating for his or her driving capabilities. Indeed, insurance premiums are now lowered in some cases to take account of the safety performance of specific models of vehicles.

Checks at the End of Operational Use

At the end of use the data acquired during the journey is accumulated and stored. If a journey ends exceptionally, for example, because of an impact, then safety systems such as airbags, fuel cut-off, door unlocking and electrical system isolation are activated. Additional detailed data related to the event may also be retained, rather than being accumulated in the normal way. During operation, tachometers and other instruments are used to record how long and in what way the vehicle has

been driven. This information can be inspected to ensure compliance with the law governing the use of different classes of vehicles.

In summary, on-board safety systems are well developed in the automotive domain and continue to develop at a rapid pace to meet the demands of customers and the regulators. On-board safety systems are seen as important and valuable benefits: by manufacturers, to protect themselves from litigation while making their products more marketable, and by customers to protect themselves and other road users from harm and to avoid litigation or legal sanctions. The issue of assigning liability for operational incidents and failures is an open topic, and will doubtless be gradually formed by legislation and case law.

Future Safety Systems in the Automotive Industry

The European Automobile Manufacturers Association has defined three objectives for the new “active” safety systems in the automotive industry:

- Reduce pedestrian fatalities
- Reduce pedestrian injuries
- Reduce societal costs

The twofold plan to achieve this is by:

- Avoiding collisions
- Reducing collision severity

The proposed solutions for the achievement of the above are summarised in the following concepts:

- Anticipate and steer
- Anticipate and brake
- Anticipate and warn

A number of technologies have been proposed for the improvement of safety associated with road transport. Depending on the nature of the proposed technologies and the characteristics associated with them, these can be categorised into the following three fields (according to the direction in which they provide enhancements in):

- Better visibility—*Current systems*: high-intensity discharge lamps, daytime running lights, UV lighting. *Future systems*: night vision systems (infrared), smart headlamps for steering and spotlighting, vision enhancement and analysis systems
- Better steering—*Current systems*: tire optimisation, ABS, enhanced stability and traction control, variable power assist, body control (active ride levelling and anti-roll). *Future systems*: smart steering, steer by wire, collision avoidance

- Better brakes—*Current systems*: ABS, ABS and electronic brake force distribution, brake by wire, emergency brake assist. *Future systems*: automatic precrash brake intervention, collision avoidance, adaptive cruise control stop-and-go

Further, there are concepts proposed by some automobile manufacturers that are of particular interest with respect to their applicability in the aviation domain, for example, the system proposed by Volvo for controlling unintended lane departure of the vehicle or the system under research by Ford and Autoliv which is to “combine vision and radar sensor technology to create a new type of auto safety system that will detect approaching hazards, measure their rate of motion, determine if and where a collision will occur, and trigger mitigating actions, such as applying brakes, pre-tensioning seat belts, and firing side airbags, with a near-zero false alarm rate.” Other such concepts, (for which applicability to the aviation domain should be investigated) include “Anticipate and Warn” and “Collision Avoidance.”

Safety Approach in the Rail Industry

Most of the safety concepts in use today have been developed gradually in the rail domain. Dating back to the 1850s, rail accidents and incidents have been investigated, the causes and hazards have been determined, and then systems have been improved to eliminate or mitigate them. Rail transport introduced a number of innovations—mass transport for the public, heavy vehicles with relatively poor braking performance travelling at high speed and the potential for major “man made” disasters (e.g., collapsing bridges) and collisions. Where rail routes intersect or end, there is the potential for collision, and from the earliest times safety systems have been employed (the first being a man on foot preceding the train and carrying a large red flag).

In the nineteenth century, semaphores were developed in the form of physical tokens carried on-board the train, to ensure mutually exclusive occupancy of track sections shared between multiple routes. More recently, in the twentieth century, dynamic routing and interlocking were developed, which guaranteed transient exclusivity of a route through the rail network in order to allow safe operation with more overall traffic. Safety standardisation for operations and equipment have also been pioneered in the rail domain, and this is reviewed more specifically in a later section. There is a distinct separation between on-board safety monitoring and operational control of trains.

Current On-Board Safety Systems

Rail safety systems cover a similar scope to aviation, including:

1. Control centres concerned with route management

2. Interlockings concerned with collision avoidance
3. Juridical recorders concerned with providing an independent trace of historical activity before an incident/accident, and covering signalling both on the track-side and on the train
4. Train protection systems, which either prevent unsafe train operation or safely curtail it
5. Automatic train operation, replacing functions of the human driver
6. “Info-tainment” systems for communication with vehicle users
7. Safety-driven maintenance systems for both trains and infrastructure (e.g., track, signals, etc.)

These are summarised in the following four subsections.

Physical Safety Systems

Physical safety systems are concerned primarily with the safety of the passengers and include physical containment (carriage design) but not yet seat belts. Rail travel is considered to be the safest mode of mass transport in terms of deaths per passenger per mile/kilometre and in the past, speeds have been moderate (<150 km/h); however, with the advent of modern trains running at speeds of 300 km/h or more, the physical safety of passengers is being reconsidered. Consequently, train and track infrastructure maintenance has come to be considered a safety-critical aspect and formal management and recording systems have become mandatory. In subway rail systems underground, additional safety systems are required both on- and off-board due to the increased risk of harm from fires and collisions in tunnels and enclosed stations.

Route Safety Systems

Railways have the disadvantage that their route topology is fixed and is 2-dimensional. The cost of changes to track and infrastructure such as stations is huge and often socially contentious. As pressure mounts for more traffic to run on existing infrastructure, there has been a movement from static allocation of routes (protected by static interlocking logic) to dynamic allocation of route fragments based on current (and managed) availability.

The challenge has been to guarantee safety from collisions across the network while moving more trains at higher speeds through a fixed topology track network. Similar pressure is being experienced in the aviation domain, but without such severe constraints on route topology (3D rather than 2D).

The new dynamic train route management system being deployed throughout Europe (ERTMS) is based on the concept of providing a series of “movement authorities” (MAs) to individual vehicles as they proceed on their journeys. Each MA defines a safe forward speed profile for the train that either the driver or an automatic train operator (ATO) must conform with when driving.

This is similar to air traffic control in aviation, the grain of movement along each controlled route being much smaller for trains than aircraft.

Using MAs has the additional advantage that account can be taken of local environmental factors such as speed and noise restrictions, as well as providing the mechanism for guaranteeing exclusive occupancy of the track for the duration and location of the MA. Each operational train receives a stream of MAs from the control centre via an interlocking. This guarantees collision avoidance apart from unanticipated collisions with obstructions on the rail track, such as other vehicles (e.g., cars, trucks), animals or people (e.g., workmen, suicides). There are similar hazards in aviation such as parachutists, hang-gliders, chairlift cables, flocks of geese and drones.

Driving Safety Systems

Driving safety systems are well established in the rail domain; an early example is the “dead man’s handle” used to (hopefully) ensure that the driver is alive and conscious. Lately, particularly in subways, there has been a move toward driverless trains using so-called automatic train operator (ATO). Accidents in subways can cause extensive harm, for example, a fire can cause smoke that suffocates passengers and the public waiting at adjacent stations. The risk of a driver becoming ill, using drugs or even committing suicide can now be reduced using an ATO, so it is now perceived as safety-critical. ATO is widely used in the Far East, but its use in Europe has been tempered by social issues (e.g., trade unions). However, most new and refurbished rail schemes use ATO or have changed over to full automation with driverless trains. Note that such systems are much easier to control safely as the topology of the track limits the possibilities of movement. This is not the case with road vehicles where there are many more degrees of freedom, including a mix of driverless and human-driver-controlled vehicles.

Driver Safety Assurance

This is a rapidly changing area. Many current driver interfaces tend to rely on forcing the driver to acknowledge continuous stimuli from the driving console to confirm that the driver is aware of the current context and is active and alert. This scheme is not always desirable from a human factors viewpoint as drivers tend to

start unconsciously and automatically responding to the stimuli rather than the real and current driving situation.

This is believed to be a major contributing factor to the cause of the notorious high-speed train crash at Paddington, London, in 2003. This brought attention to the need to carefully consider human factors as a safety issue in the design of driver interfaces. Driver identification and confirmation of capabilities (e.g., knowledge, skills and relevant experience) has now become an important safety and security issue. After problems with alcohol and drug abuse with drivers and other rail staff, random testing of operational train staff has been introduced in Europe. The trend is towards mandatory checks before each workshift and also toward the use of an ATO to reduce dependency on the driver, based on the well-established use of autopilots in aviation.

Safety Improvement

Safety improvement in the rail domain is driven by regulation, approvals and inspection. At the infrastructure level, the equipment and operational standards are being harmonised across Europe, having previously been highly country-specific. At the same time, the signalling systems are being upgraded to ERTMS (European Rail Transport Management System). At the equipment level, there is a well-established and well-regulated framework (ref: EN ISO 50128) for defining, designing, verifying, validating and auditing the function and functional safety of individual products. The production and independent safety audit of safety cases is mandatory for all products and schemes, that is, the use of products together in operational systems.

The rail domain is very traditional and conservative in its approach to safety, for example, in the nineteenth century the route safety *interlocking* was originally a mechanical interlocking between the levers used to physically pull the signal arms via cables, and many are still in use today. In the early twentieth century, relay logic was introduced to emulate the mechanical interlockings, then subsequently programmable logic controllers (PLCs), which in turn emulated the relay logic. Only in the last decade or so has there been a movement toward using application-specific computer languages to define the signalling rules of the rail network and then interpret them in real time using journey scripts.

Operational Safety Cycle

Operational checks for on-board train safety are already widely used in the rail domain. The typical life-cycle involves the following.

Maintenance

For the most part, rolling stock (i.e., trains, wagons, carriages, etc.) are owned by investment companies and leased by train operating companies (TOCs) to serve specific routes. The owners are responsible for the safety and maintenance of the rolling stock, while the TOCs and infrastructure providers (i.e., track, signals, and stations) are responsible for operational safety on-board the train and within the rail network. Each train is considered to be a set of wearable parts and they are subject to a series of regular inspections and/or replacement according to a safety maintenance plan. The service intervals for each train are determined by elapsed time and also journeys made (i.e., distance travelled, speed profiles, route quality, etc.).

On-board monitoring for most trains is limited to the mandatory automatic train protection (ATP) system. However, the need to drive down maintenance costs and increase operational availability (which is crucial to the leasing companies) is fuelling interest in on-board monitoring and diagnostic systems.

Checks at Start-Up of Vehicle

The four main safety checks here are typically:

1. An approved route and a movement authority to proceed have been provided
2. A qualified driver capable of driving the train is available
3. A safety clearance from the on-board ATP system (driver and brakes approved, carriages coupled, etc.) has been provided
4. A safety clearance from the ATO system (doors all closed, guard on-board, etc.) has been provided

No rail personnel involved in any safety-related activity are allowed to consume intoxicants or drugs; incidentally this extends to the designers and maintainers of all the equipment, infrastructure and rolling stock. Mandatory random testing has been introduced for drivers. In many cases the driver's operational capability is still the "weakest link" in the safety chain (German Wings 9525 Tragedy).

Checks During Operational Use

The ATP system independently and continuously checks the vital aspects of the train during a journey, including braking, the physical integrity of the train, the emergency stop cord and the integrity of the ATP itself. Any compromise of safety automatically brings the train to a halt. With ERTMS it becomes possible to also ensure that the train remains within the speed/distance profile defined by the current movement authority at all times, and this to some extent also mitigates loss of control or erratic behaviour by the driver.

Currently, this is considered to be an ATO function but it could easily cross over to being an ATP function. External systems can also affect safety, for example, trackside transponders used to detect whether a rail signal has been “passed at danger” that is, the driver has ignored or missed it. Presently, this is presented as a driver warning, so as not to lower traffic throughput in the rail network; in the future it may come within the scope of the ATP system.

Passenger information systems are now being more widely used to inform passengers of safety features and so are becoming part of the on-board safety system (following the long-established aviation practice). In the case of hazard conditions or an impending accident, the passenger information system is used to give advice designed to minimise impending harm, the other safety systems being focused on accident prevention and mitigation.

Checks at the End of Operational Use

The journey data for each train is accumulated by the ATO (if fitted) and at least by the train operator and leasor. It is highly likely that as further data is sensed and recorded during journeys that diagnostic systems will be used to identify and anticipate developing safety conditions and emerging hazards. This is particularly relevant for high-speed trains where huge amounts of kinetic energy are involved and safe braking distances are anything up to 5 km.

Future Safety Systems in the Rail Domain

It will take at least 10 years to fully introduce the new ERTMS system throughout Europe, probably longer while Europe continues to expand. In the meantime it will coexist, inter-operate with and gradually displace the existing melange of “traffic light”-based signalling and safety systems.

The increased risk of harm due to high operational speeds, high mass trains and increased passenger volumes (e.g., double-decker carriages) will increase the need and market for on-board safety systems to monitor, predict and mitigate safety-related conditions and avoid hazards. New systems to reduce the dependence on human drivers are already being introduced. It is anticipated that systems for driver identity and capability assurance will also be developed and deployed in the next few years, particularly in the light of the spread of terrorism.

Safety Approach in the Space Domain

In the space domain, safety is the critical issue. At present, safety systems on-board spacecraft are split into two main categories—the flight safety systems (FSS) and the integrated vehicle health management (IVHM) systems:

- FSS are the systems, which are concerned with the protection of the public from off-nominal launch vehicle flight, and nontraditional FSS will expand this protection via new methods and to vehicles that re-enter as well as launch.
- IVHM systems form the basis for safe operation of launch and re-entry, especially with regard to vehicle maintenance and interaction with future nontraditional FSS.

The kinetic energy of an out-of-control spacecraft and the hazard associated with such a large volume of fuel as is normally carried may have catastrophic repercussions for both the general public and the environment in the event of an accident. This is the reason why FSS are very much mandatory for spacecraft.

Five distinct FSS methodologies can be identified:

1. *Range containment*: Flight trajectory is constrained to a chosen range, which is perceived to contain in its entirety a vehicle or its debris in a case of possible malfunction. If the vehicle is to stray out of this range, its destruction is commanded. This may be done remotely or by on-board means, depending on whether the vehicle is manned or not.
2. *Vehicle destruct*: Certain boundaries are set along a vehicle's trajectory such that the vehicle's continued operation within those boundaries will not negatively affect public safety. However, should the vehicle stray outside of those boundaries or become uncontrollable within those boundaries, the vehicle is destroyed via an active command. The boundaries are defined such that the propagation of debris to Earth's surface will not bring harm to the public.

Such systems may be placed on an element of the spacecraft, depending on its operational characteristics, (e.g., if the vehicle is of the reusable type, the system may be placed on the rocket boosters so as to assure safe recovery of the main body of the craft). For a reusable launch vehicle (RLV) carrying people on-board, the use of the system would be a last resort, a highly undesirable situation.

3. *Flights safening*: This is a flight safety methodology presently employed by UAVs that is applicable for any non-crewed vehicle capable of sustained powered flight in the atmosphere. Within the general methodology of flight-safening are several modes, which are dependent upon the degree of autonomy of the vehicle; all of these modes require a minimum autonomous flight capability. The first mode entails a cessation of the attempt to fly a course and the commencement of flight around a fixed point. The mode would be entered automatically if the command-link is lost, and might be entered by command if the pilot observes a control problem (however, the control problem could easily hamper the ability to maintain flight).

For the very lowest level of autonomous capability, the mode would entail circling of the vehicle's present position. The next level of capability would be a circling of the present position while gaining altitude in an attempt to reacquire a lost command-link. The next level of capability beyond circling a "present" location would be for the vehicle to fly to a preprogrammed waypoint. The highest level of capability is one where it is possible for the craft to be equipped with an auto-land system that would allow it to fly to a suitable landing area designated by a waypoint and then land.

4. *Thrust termination*: This system consists of an on-board computer that determines, via inertial measurements, when the craft is straying from its course sufficiently so as to place public safety in jeopardy. If public safety would be placed in jeopardy by continuing operation of the craft, the on-board system would terminate the vehicle's thrust and the vehicle would continue on and impact Earth along a planned ballistic trajectory. This system may often be combined with some other FSS, so as to allow recovery of the vehicle.
5. *Vehicle recovery system (VRS)*: A vehicle recovery system is defined as any system which, either given a launch-abort or a re-entry anomaly, allows the vehicle to come to a "soft" landing (i.e., a landing after which one can reasonably expect to recover the vehicle relatively intact such that it would need only moderate repairs before being returned to flight status). In the case of NASA UAVs, this is simply a parachute system. A VRS may be employed as a method of allowing the vehicle to descend to a "soft" landing in the case that the vehicle cannot land at an alternate or acceptable landing location. A "soft" landing in this case will hopefully allow the vehicle to be recovered intact and protect the occupants, if any. Moreover, it protects public safety by restricting the impact velocity to a value much lower than the value would be if the vehicle were in free-fall.

On the other hand, IVHM systems have two separate areas of emphasis. The first area is the use of IVHM to support vehicle maintenance. In this role, IVHM is used to record data in-flight; that data is not accessed until post-flight, at which time it is used to help determine when vehicle systems are in need of repair or replacement. These systems are normally referred to as "post-flight IVHM."

The second area of emphasis is the use of IVHM to support vehicle flight operations. In this role, IVHM actively manages (and therefore is also monitoring) the vehicle during flight, and is intended to take action in the case of component or system degradation, imminent failure, or failure. Ideally these IVHM systems would act so as to prevent component or system failure that in any way would affect the safety of a mission. These systems are referred to as "in-flight IVHM" and resemble the active safety concepts explained in this book.

Once again, out of all the systems described in this section, there are some of particular interest with respect to the active safety and the applicability of the associated concepts in the field of aviation. Depending on the associated conditions, the "range containment," "vehicle destruct," "flight safing," "thrust termination" and "vehicle recovery system" concepts, or a combination of those, may be of

interest with respect to their application in aviation. In light of the events of 9/11 and some previous crashes of civil aircraft in residential areas (e.g., a cargo 747 EL-AL crash in Amsterdam in 1992), future implementation of such systems in aviation may be worthy of investigation at least at the conceptual level.

Existing Standardisation

In the domains examined above, there are a number of standards that specify the requirements associated with the safety systems installed on-board the vehicle in question.

Of these standards, those that bear some relevance with respect to active safety are discussed in the following sections.

Standards in the Industrial Domain

The range of applications of industrial systems is very diverse. Consequently, there has been a two-level approach to standardisation. Firstly within a sector (e.g., chemical) there are regulations regarding the safe operation and use of specific products and systems. These tend to be drafted by either manufacturing associations or the manufacturers themselves. Secondly across all sectors there is a single standard (IEC 61508), which covers the specification, design and implementation of safety-related products and systems themselves.

The 61058 standard is concerned with “Functional Safety of Safety-Related Systems”. It is also the basis for safety standards in a wide variety of other sectors (e.g., chemical, nuclear, rail).

Safety Definitions of IEC 61508

A full set of definitions and abbreviations can be found in Part 4 of the standard. The main concepts are outlined below to explain what functional safety is and how it can be achieved:

- *Safety*: freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment
- *Functional safety*: the part of overall safety that depends on a system or equipment operating correctly in response to its inputs
- *Safety-related system*: systems that are required to perform a specific safety function, or functions that ensure that risks are kept at an acceptable level

- *Safety function*: an individual function of a safety-related system
- *Safety function requirements*: what the function does
- *Safety integrity requirements*: the likelihood of a safety function being performed satisfactorily in terms of the probability of failure of the function:
 - Per year of continuous operation
 - Its required function on demand

Functional Safety Analysis

To assess safety and clarify requirements, the following techniques are used:

- *Hazard analysis*: identifies potential hazards and the conditions that led to them
- *Risk assessment*: determines the nature and performance requirements for the safety function needed to prevent conditions leading to a hazard; the aim is to ensure that safety integrity of the safety function is sufficient to ensure that neither people nor the environment exposed to unacceptable risk associated with a hazardous event

The purpose of functional safety analysis is to prevent dangerous failures or to control them when they arise; examples of such failures are:

1. Incorrect specifications of the system, hardware and/or software
2. Omissions in safety requirements (failure to develop all relevant safety functions for all modes of operation)
3. Random hardware failure mechanisms
4. Systematic hardware failure mechanisms
5. Software implementation errors (logic, sequence, temporal)
6. Common cause (mode) failures of sensing, computation and actualisation
7. Human error
8. Environmental (e.g. electromagnetic, nuclear radiation, temperature, mechanical)
9. Power supply disturbances (blackout, brownout, reduced voltage, reconnection, etc.)

The system life-cycle is laid out in a similar way to the safety life-cycle; however, they cover separate aspects and concerns of the same entity.

Because the 61508 standard is large and comprehensive, it is split into seven parts, each related to an area of concern:

1. General requirements for any system
2. Requirements for electrical/electronic/programmable electronic safety-related systems
3. Software requirements (to develop software that is safe in operation, auditable in design and implementation and maintainable in the long term)
4. Definitions and abbreviations

5. Examples of safety integrity level determinations (SIL1 to SIL4)
6. Guidelines on appropriate techniques and measures used to achieve different SIL levels
7. Overview of measures and techniques

Further details can be found on the IEC website in the functional safety zone section at: <http://www.iec.ch/functionalsafety>.

The 61508 standard has now been used as the basis for many other industry/sector-specific standards, for example, the well-established ISO EN 5012× family of specifications in the rail sector already referenced.

Standards in the Rail Domain

Safety techniques are well established in the rail sector as this was the first sector to introduce mass travel with the attendant potential for disaster. A series of standards has been defined to provide detailed guidance on how railway systems can be specified, designed and implemented to be safe to some defined level of integrity. The basic philosophy behind this group of standards is concisely reviewed and the standards are based on the concepts defined in the functional safety standard EN 61508 previously mentioned. These standards together cover all aspects of railway safety from wide-area signalling systems at a high level, down to component-level design and reliability at the equipment level.

The Safety Case

Railway systems are gradually enhanced and changed over many decades, often with new subsystems having to interwork with existing systems as well as replacing their functions as technology has changed. In order to ensure that the overall subsystem will remain safe when a new system is deployed, a documented safety case needs to be produced. Typically, this is comprised of the following:

1. The definition of the new subsystem in the context of the existing system
2. A quality management report on the implementation, verification and validation of the new subsystem
3. A safety management report detailing evidence of the safety management of the project and product (e.g., safety plan, results of audits such as “vertical slice” audits of documentation and V&V evidence of requirements, design, implementation and testing)
4. A technical safety report detailing evidence of functional and technical safety
5. Related safety cases, such as for the bounding system(s) or any pre-existing or commercial off-the-shelf (COTS) sub-subsystems embedded in the subsystem being considered

6. A conclusion that summarises the evidence provided and makes the argument that the system/subsystem/equipment is adequately safe subject to compliance with the specified conditions of use

These points are all described in detail in Section 10 of EN ISO 50129.

Development Life-Cycle for Safety-Related Systems

The life-cycle activities for overall development of safety-related systems can be represented conveniently in a V shape. The top of the V has higher levels of design abstraction (e.g., system requirements specification), whereas the bottom of the V is the hardware design itself, with its corresponding software runtime support. The left-hand side deals with the specification and the right-hand side deals with the implementation of the verified and validated system.

Clearly the key document is the system requirements specification because this addresses the scope of the subsystem, its interfaces to its bounding system and environment, what it does (i.e., functional and nonfunctional requirements) and its functional safety requirements. As explained in the section on industrial safety above, the product development life-cycle closely corresponds to the safety life-cycle with a change of emphasis on product functionality rather than functional safety; both are essential and intertwined.

The standards also outline the approaches required for hazard analysis, risk assessment, safety integrity level assessment and failure mode analysis (typically, failure mode effects and criticality analysis, FMECA, and fault tree analysis, FTA). Note that active safety may require these or similar techniques, but the principle of active system safety (PASS) concept *dynamically extends the scope of safety analysis beyond these techniques* using analysis of real-time operational data, not just static “design time” FMECA and FTA data and assessments.

Safety Integrity Levels (SILs)

At some point, the question has to be asked, “How safe is safe?” That is, how can safety be made measurable objectively? The safety integrity level, or SIL, defines the level of safety. Depending on the SIL level required for the subsystem, in the context of its system(s), the EN 61508 standard and the rail standards set out various minimum technical methods for system, hardware and software design and implementation recommended for use to achieve each SIL level (1–4). The SILs for railway applications are defined as follows (Table 2.1).

Non-life threatening systems are usually implemented to SIL 2, (e.g., a data preparation system for track layout information). Potentially life-threatening systems and ultra-high-availability systems are normally implemented to

Table 2.1 Typical safety integrity level characterisation for railway applications

SIL level	1	2	3	4
Probability of failure to perform its design function on demand	$\geq 10^{-5}$ to 10^{-4}	$\geq 10^{-6}$ to 10^{-5}	$\geq 10^{-7}$ to $< 10^{-6}$	$< 10^{-7}$
Dangerous failure rate per hour per system element	Function on demand $\geq 10^{-7}$ to 0.3×10^{-5}	$\geq 0.3 \times 10^{-8}$ to 10^{-7}	$\geq 10^{-10}$ to 0.3×10^{-8}	$< 10^{-10}$

SIL 4 (e.g., the automatic train protection system and parts of the automatic train operation system). In the active safety context, the passive device used to monitor active safety would most probably be implemented to SIL 2 as a product (not for the prototype). If this device were extended in scope to include control of some aspects of an aircraft, then it would definitely be classified as SIL 4. New systems for controlling railways are being introduced (ERTMS); however, the basis for systematic safety assessment, design and assurance remain the same, based on the existing standards.

Standards in the Space Domain

One of the standards that govern the specification of flight safety systems for space vehicles is ISO/WD 14620-3. This international standard sets out the requirements for space-borne operations with respect to the safety of the exposed people, property and environment for those countries and/or organisations conducting scientific commercial or civil launch activities. In addition to standard requirements regarding the availability of the flight safety systems in question, under the worst predicted environment, the adherence to component storage and operational life-cycle requirements, the prevention of system unavailability attributable to electromagnetic interference, the following requirements have been highlighted so as to provide an overview of the requirements associated with space-born Flight Termination System FTS, Range Tracking System RTS and Telemetry Data Transmitting System TDTS.

Under the section “General Requirements” of the standard:

1. Clause 5.2 requires that: “All guided launch vehicles shall incorporate a means of tracking that enables real-time monitoring of vehicle position and prediction of instantaneous impact points from launch through orbital insertion or mission completion.”
2. Clause 5.3 requires that: “All launch vehicles shall incorporate telemetry data transmitting systems for monitoring critical vehicle performance data, flight termination system and tracking system status that are capable of functioning throughout the launch phase until the end of range safety responsibility.”

3. Clause 5.4 requires that: “Any launch vehicle having a stage, motor or component capable of violating the defined safety envelope shall be equipped with a flight termination system (FTS) that shall be capable of interrupting the flight of the vehicle if it diverts from its predicted flight trajectory and has sufficient energy to become a threat to public safety.”

Under the section “Flight Termination System Requirements” of the standard:

4. Clause 6.1.1 requires that: “Any launch vehicle where a malfunction of the vehicle or any stage, motor, payload or component may generate an unacceptable hazard to public safety shall contain flight termination systems.”
5. Clause 6.1.2 requires that: “All launch vehicle stages capable of violating the defined flight safety envelope shall contain flight termination systems.”
6. Clause 6.1.3 requires that: “FTS reliability shall be set at 0.999 at the 95% confidence level, or shall be compliant with the quantitative flight safety objectives if the later are more stringent. The reliability should be established by analysis of all components and supporting test data.”
7. Clause 6.1.4 requires that: “The FTS shall be capable of rendering all powered stages and any other propulsive system of the vehicle nonpropulsive.”

Under the section “Range Tracking System Requirements” of the standard:

1. Clause 7.2.1 requires that: “All expendable launch vehicles and suborbital vehicles shall have an approved means of tracking the vehicle’s trajectory throughout flight. The RTS may use various ground-based or vehicle-incorporated tracking modes to provide accurate tracking information.”
2. Clause 7.2.2 requires that: “The RTS shall provide real-time data from which position and velocity can be determined.”
3. Clause 7.2.5 requires that: “The RTS shall be capable of providing real-time indications of malfunctions of any components compromising operation of the system.”
4. Clause 7.2.8 requires that: “Transponder systems used on vehicles shall be capable of operating within the parameters established for operation of the tracking facilities.”
5. Clause 7.2.9 requires that: “Space-based translators or receivers, such as GPS, shall be independent of any on-board guidance system.”
6. Clause 7.2.10 requires that: “Design RTS reliability shall be 0.995 at the 95% confidence level for transponder systems and 0.999 at the 95% confidence level for space-based systems such as GPS, or shall be compliant with the quantitative flight safety objectives if the later are more stringent. The reliability should be established by analysis of all components and supporting test data.”

Under the section “Telemetry Data Transmitting System Requirements” of the standard:

- Clause 8.2.1 requires that: “All launch vehicles shall have a TDTS to provide vehicle performance data to flight safety operators.”

Clause 8.2.2 requires that: “The TDTS shall be capable of providing uninterrupted data from lift-off through orbital insertion, mission completion or until range responsibility for safety has been fulfilled and terminated.”

Clause 8.2.3 requires that: “The TDTS shall be capable of acquiring, storing, processing and providing data in real-time.”

Clause 8.2.4 requires that: “Telemetry data shall include data relevant to position and tracking, FTS status, RTS status, vehicle performance, engine and control information.”

Clause 8.2.5 requires that: “The TDTS shall be capable of providing real-time indications of malfunctions of any components compromising operation of the system.”

Clause 8.2.6 requires that: “Sufficient TDTS data shall be obtained to determine the adequacy of the flight safety system throughout flight and to support pre-flight and post-flight analyses.”

Clause 8.2.7 requires that: “The airborne telemetry system shall be compatible with the ground-based telemetry stations.”

Clause 8.2.12 requires that: “Design TDTS reliability shall be 0.995 at the 95% confidence level, or shall be compliant with the quantitative flight safety objectives if the later are more stringent. The reliability should be established by analysis of all components and supporting test data.”

Note that the real-time data during flight is not stored on-board in a “black box” recorder. Instead, it is transmitted from the vehicle and analysed independently of the vehicle itself. The above requirements would be of interest with respect to addressing the hazard associated with aircraft crashes (mostly into a populated area), whether because of a terrorist act or because the pilot had been incapacitated, or because of some system failure, etc. These requirements need to be considered as guidance and the basis for the possibility for incorporation of such safety systems in future aircraft whether in general, civil or military aviation.

Conclusions

In this chapter we have briefly covered problems of safety and existing solutions, regulations and trends in:

- Space systems
- Railways
- On-ground transport

We have discovered:

- The role of functional safety analysis based on fault tree analysis
- Requirements for life-cycle for safety (based on the V-scheme)

We have described standards for safety in the space domain.

This short overview has indicated that apart from initial steps of implementation of an in-flight vehicle health monitoring system for aerospace, there is no evidence so far that active system control and its application for active system safety. In spite of the fact that fault tree analysis has been proven to be ineffective, static and inapplicable for real-time safety, this analysis still predominates in safety system designs.

Additionally, design and management of safety systems so far has been approached using a V-diagram, while nonfunctional requirements such as active safety or active system control should be maintained at each level of design with minimisation of feedback between phases or levels of a project.

Thus, the activeness of system controls or system safety should be introduced at first theoretically and then further implemented through existing systems, changing the requirements for the system we design as needed.

Active system control and active system safety, therefore, should be illustrated by the positive impact of our approach on the schemes, regulations and maintenance. This advantage should be shown quantitatively and address gains in reliability, performance, and energy efficiency with and without implementation of our concept.

Functional Safety Standards Based Upon IEC 61508

Functional Safety	
IEC 61508	Standard on functional safety, see https://en.wikipedia.org/wiki/IEC_61508
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related system
Machinery	
IEC 61511	Safety instrumented systems for the process industry sector (in USA: ANSI/ISA S84)
IEC 62061	Safety of machinery
Railways	
IEC 62278 / EN 50126	Railways—Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
IEC/EN 50128	Software, railway control and protection
IEC/EN 50129	Railway signalling
Nuclear	
IEC 61513	Nuclear power plant control systems
Avionics	
RTCA DO-178C	North American avionics software “Software considerations in airborne systems and equipment certification”
RTCA DO-254	North American avionics hardware
EUROCAE ED-12B	European flight safety systems

(continued)

Automotive	
ISO 26262	Automobile functional safety
ISO26262-1	Road vehicles—Functional safety—Part 1: Vocabulary
ISO26262-2	Road vehicles—Functional safety—Part 2: Management of functional safety
ISO26262-3	Road vehicles—Functional safety—Part 3: Concept phase
ISO26262-4	Road vehicles—Functional safety—Part 4: Product development at the system level
ISO26262-5	Road vehicles—Functional safety—Part 5: Product development at the hardware level
ISO26262-6	Road vehicles—Functional safety—Part 6: Product development at the software level
ISO26262-7	Road vehicles—Functional safety—Part 7: Production and operation
ISO26262-8	Road vehicles—Functional safety—Part 8: Supporting processes
ISO26262-9	Road vehicles—Functional safety—Part 9: Automotive safety integrity level (ASI) oriented and safety-oriented analyses
Medical	
IEC 62304	Medical device software
ISO14971	Medical devices—Application of risk management to medical devices
EC/EN 50402	Fixed gas detection systems
DEF STAN 00-56	Accident consequence (UK military)

References

Active Safety

1. AOPA United States GAO (General Accounting Office), GAO-01-916 (2001) General aviation status of the industry, related infrastructure, and safety issues. U.S. General Accounting Office, Washington, DC

2. ARINC_653. The avionics standard based on the concept of partitioning the processor time, memory ranges and I/O access. http://en.wikipedia.org/wiki/ARINC_653, also: “ARINC 653 An Avionics Standard for Safe, Partitioned Systems,” www.computersociety.it/wp-content/uploads/2008/08/ieee-cc-arinc653_final.pdf

3. German Wings 9525 Tragedy. Suicide by pilot. https://en.wikipedia.org/wiki/Germanwings_Flight_9525

4. Bhopal. Gas leak tragedy in India. https://en.wikipedia.org/wiki/Bhopal_disaster

5. CAN Bus. Using software protocols to mask CAN BUS insecurities, B R Kirk, IEE colloquium on the electromagnetic compatibility of software, Thursday, Savoy Place, London, 12 November 1998, IEE document reference 98/471, available from the IEE Library at Savoy Place, libdesk@theiet.org, or archives@theiet.org

6. Castano V, Schagaev I (2015) Resilient computer system design. Springer International Publishing. ISBN 978-3-319-15068-0

7. Chernobyl. Nuclear reactor explosion and meltdown. https://en.wikipedia.org/wiki/Chernobyl_disaster

8. Concorde. Rupture of fuel tank from runway debris. https://en.wikipedia.org/wiki/Air_France_Flight_4590

9. EMC Guide. Guide on EMC for functional safety, published by the IET in 2008, PDF download. www.theiet.org/factfiles/emc/index.cfm, colour-printed book: www.emcacademy.org/books.asp
10. EN ISO 50128. Software assurance standard for railway applications. https://de.wikipedia.org/wiki/EN_50128
11. IEC 61508. Standard on functional safety. https://en.wikipedia.org/wiki/IEC_61508
12. Kaegi T, Schagaev I. System software support of hardware efficiency. eBook from: www.it-acs.co.uk/book.html
13. Overtoon E, Miloslavina S, Schagaev I (1999) In: Proceedings of the international system safety society ASGA: active safety for GA, ISSS99. Orlando, 16 August
14. Schagaev I (2001) CASSA: concept of active system safety for aviation. In: 15th IFAC symposium on automatic control in aerospace, 2–7 September 2001. pp 303–309. ISBN 0-08-043684
15. Schagaev I (1998) The concept of dynamic safety for aeroplanes, ISSC98. Seattle
16. Shuttle. Launch attempted with rocket fuel seals below specified temperature. https://en.wikipedia.org/wiki/Space_Shuttle_Challenger_disaster
17. Susskraut. Safe program execution with diversified encoding. Martin Susskraut et al. Embedded World 2015. www.embedded-world.eu
18. Systemantics. A book and thesis by John Gall on why systems fail. <https://en.wikipedia.org/wiki/Systemantics>
19. Three Mile Island. Nuclear plant accident. https://en.wikipedia.org/wiki/Three_Mile_Island_accident
20. Timed Ethernet. http://www.ieee802.org/802_tutorials/2012-11/8021-tutorial-final-v4.pdf
21. Train. High-speed train derailed and crashed into a road bridge. https://en.wikipedia.org/wiki/Eschede_derailment

<http://www.springer.com/978-3-319-46812-9>

Active System Control

Design of System Resilience

Schagayev, I.; Kirk, B.

2018, XVI, 295 p. 139 illus., 110 illus. in color.,

Hardcover

ISBN: 978-3-319-46812-9