

ACHIEVING AND DEMONSTRATING SAFETY OF PRT

Dr. Chris Elliott FREng

Director, Pitchill Consulting, Magalee, Moon Hall Road, Ewhurst, Surrey GU6 7NP, UK
t+44 1483 273793 m+44 7836 217901 www.pitchill.com

Abstract

The acceptability of PRT will depend crucially on safety – both how safe it is and how safe it is perceived to be. The qualities of a complex system like PRT that make it safe are the same as those that make it reliable. They are part of the way that it is designed and built, not add-ons to an otherwise unsound system. A systematic approach to design can be extended into a systematic approach to safety specification and verification. This is illustrated by the verification process used for ULTra, a process that satisfies the UK's regulatory regime that is derived from that used for railways.

Introduction

The safety of a guided mode of public transport will be subject to intense scrutiny. Although the public tolerates high rates of accidents on roads, including public services such as buses, any accident on guided mode attracts disproportionate attention. This is already clear for rail; a rail accident anywhere in the world is news.

The UK rail industry has investigated the attitudes of society to transport safety, using the tools of psychology, philosophy and opinion sampling with focus groups and structured questioning. A clear but inconsistent picture emerges in which people are satisfied with the level of safety that exists and not willing to pay to improve it, but are also outraged that accidents occur.

At the base of this inconsistency appears to be an expectation that public services will work reliably and safely. When they do not, trust is eroded – people feel that they have to place their trust in others when they step onto guided transport. They are placing themselves in the care of a large and impersonal machine whereas when they step on a bus or into a car they can see the driver and there is no hidden machinery of signalling and control.

There is also an innate distrust of the new. People may tolerate a lower level safety in a long-established service that they would not tolerate in a new mode, especially where there is clearly no human driver.

The consequence for PRT is that a very high standard of safety will be demanded, at least as high as that of rail and substantially higher than that of road transport. An accident, especially a fatal accident, would be a tragedy both for those involved and for PRT.

Safety by design

Safety is most easily achieved if the PRT is designed from the start as a system. This means that it is based on a proper analysis of the needs of short and medium distance public transport and the vehicles, guideway and control system are conceived within an integrated and systematic programme to meet those needs. It is much harder if the PRT is designed to use a pre-existing technology, product or infrastructure.

Safety can be an integral part of PRT if it is conceived and designed as a system. Safety measures are not “bolted-on” as afterthoughts; the safety of the system is an integral part of the design. Like reliability, availability and maintainability, safety is an emergent property of that system design. The commercial demand for a reliable system that provides an excellent service to passengers aligns exactly with the safety interests.

Another consequence of the system-led approach is that it allows the designers to minimize the use of new and unproven technology. By concentrating on the system, it is possible to use established and proven technology in novel ways. Again, this reduces the commercial and development risk as well as the safety risk.

Safety is most easily achieved if the system, or at least those parts of it that are safety-critical, is simple, using the minimum number of safety-critical components. One major component is the control system that schedules vehicles on the guideway. If there is a separate protection system, this control system can be designed to commercial rather than safety-critical standards. Of course, it must still be reliable; failures that present no safety risk (right-side failures) would cause the network to stop and greatly inconvenience passengers and operators.

A systematic approach design also allows a systematic approach to testing and verification. Hardware and software sub-systems may be tested independently, and using well-established existing technology wherever possible can reduce the risk and testing costs. An evolving programme of prototypes is obvious for hardware but the same concept can be applied to software; structured software design start with as a formal specification that can be tested by simulation before being translated, largely automatically, into executable code.

A systematic approach allows a PRT builder to be confident that the product has been designed to be, and will be, safe. It remains to verify that confidence, in two respects:

- verifying that the PRT as built does what its specification says it should
- verifying that the specification is complete and sufficient.

That verification has to meet the regulatory requirements of the country in which the PRT will be deployed. The UK’s requirements are probably at least as onerous as those of most countries, in part because they have been recently defined.

Regulation of PRT safety in the UK

All companies in the UK are subject to the Health and Safety at Work Act 1974. This imposes a duty on any employer to do all that is reasonably practicable to eliminate risk to others, including the passengers¹ of a transport company. This principle is used to define the acceptable level of safety for rail in the UK. It is not applied to transport operations for air and in practice is only just beginning to be applied to road transport. It is however the starting point for determining the acceptable level of safety for PRT.

The term “reasonably practicable” causes much debate. Where there is established good practice within an industry, it is presumed to define all that is reasonably practicable unless there are special circumstances. Where it is possible to make a quantitative risk assessment of the net costs and safety benefits of a safety measure, that safety measure is considered reasonably practicable if its cost per statistical fatality² avoided is less than around 2.3 million euro³.

Guided modes of transport are usually subject to specific licensing regime. In the UK this was based in the Transport and Works Act 1992. This regulated road-based and rail-based modes with either cable or side guidance. Cable guidance means “guided wholly or mainly by means of a cable, wire or other device which is not in direct physical contact with the vehicles” and side guidance means “guided wholly or mainly by means of wheels bearing outwards against fixed apparatus”. PRT that uses neither wire guidance nor side wheels was not regulated. The only legal basis for deciding if such a PRT was sufficiently safe was, until recently, the general provisions of the Health and Safety at Work Act.

The European Union is pursuing a policy of transforming railways from their historical position as effectively elements of the State into independent and competing companies subject to regulation (including safety regulation) by the State. A critical part of this is the Rail Safety Directive 2004/49. This requires that every railway company has a Safety Management System that includes specified elements, a Safety Certificate or Safety Authorisation issued by the State, and procedures for ensuring that new rolling stock and track are verified as safe.

Directives have to be transposed into national law by each Member State. The UK implemented the Rail Safety Directive by creating the Railways and other Guided Transport Modes (Safety) Regulations 2006, known as ROGS. As its name implies, this was an opportunity to bring PRT within a regulatory framework. Unfortunately, it is a framework designed to regulate trains so requires adaptation to be applicable to PRT. In particular, much of the framework is designed to accommodate several independent train

¹ Section 3 (1) It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety.

² The rail industry uses an estimate of Fatalities and Weighted Injuries, where 10 major injuries or 200 minor injuries are given the same weight as one fatality.

³ This figure is issued by the UK government, derived from Willingness to Pay studies of the value attached to an incremental reduction in risk. It is NOT, as is often claimed, the “value of a life”.

operating companies (“Railway Undertakings” in the jargon) operating on infrastructure operated by another company (the Infrastructure Manager) – circumstances that are unlikely for PRT.

The Regulations include several exemptions for systems that operate with a permitted maximum speed less than 40 kilometres per hour. What remains requires that:

- before bringing a PRT into service, the operator of a vehicle or the person responsible for developing and maintaining infrastructure must establish a satisfactory Safety Management System (SMS)
- the general requirements of the SMS are defined but there is no requirement for it to be approved and no certificate is required
- one of the requirements of the SMS is that, before any new or altered vehicles or infrastructure are placed into service, the operator must:
 - establish a written compliant safety verification scheme
 - appoint a competent person and the competent person must undertake that safety verification
- the “competent person”:
 - has sufficient skills, knowledge, experience and resources to undertake the safety verification in relation to which he is appointed;
 - has not borne such responsibility in relation to any of the matters he has to consider in undertaking that safety verification that might compromise his objectivity; and
 - is sufficiently independent of a management system, or a part thereof, which has borne responsibility for any of the matters he has to consider in undertaking the safety verification, to ensure that he will be objective in carrying out the task for which he is appointed.

It is apparent that this is effectively self-certification, since the competent person is appointed by the builder or operator of the system.

An approach to safety verification within UK regulations

There are two parts to the approach:

- a systematic definition of safety requirements
- a review of every part of the system (vehicles, guideway, control system and, crucially, operations) to ensure that it satisfies those requirements.

Safety requirements can be defined by a suite of documents:

- Safety Policy or Safety Concept: this sets out the duties of the builder of the system, the operator of the system and the operator of the site within which it is deployed.

- Safety Management Plan: this is the project planning document for the development of the safety system. It shows how each of the duty holders will develop their safety management systems and ensure that they are mutually consistent.
- Safety Management System: this is the SMS demanded by ROGS. It consists of the organisational structure, processes, procedures and methods used by the duty holder to direct and control the activities required to define and meet the safety requirements and the Safety Policy objectives.
- Safety Requirements Specification: this starts by identifying all hazards and setting acceptable levels for each. Given public attitudes to transport safety, the levels should be at least as high as the aspirations of the national railway system. One convenient way of codifying them is to use Goal Structured Notation, which allows goals to be linked to the evidence that shows that they have been satisfied.
- Safety Cases: each Safety Case is a structured argument, supported with evidence, that the PRT is safe for its application in the operating environment. A Safety Case must demonstrate that the safety requirements defined are complete, correct and have been met. It will set out an argument for safety i.e. the safety claims and sub-claims made which are linked to evidence to support them. Evidence can include; risk assessment results; test/trials data; emergency arrangements; safety audit/inspection results; system/sub-system specification; ‘CE’ or similar markings; standards compliance evidence etc. In general the volume and type of evidence will be proportional to the level of risk or safety criticality of the components.

This should not be just a “paper chase”, generating reports and documents only to satisfy an administrative need. Each document should be tightly focused on ensuring that the PRT is safe and can be shown to be safe. By using a systematic structured approach, it is possible to review and challenge any part of the safety system and to revise it in the light of emerging experience. There is another justification for this approach: safety emerges from exactly the same qualities of the system as reliability. Ensuring that the system is safe also ensures that it is reliable, a critical commercial requirement.

Having specified safety requirements, the next step is to verify that the system meets them both as designed and in practice.

Case study: verification for ULTra

The ULTra PRT has been extensively described elsewhere so will only be summarized here. ULTra uses electric vehicles running at up to 25km per hour on dedicated guideway. Each vehicle takes up to four passengers from a station to another station that they have specified. Vehicles always move in the same direction along a section of guideway and stations are off-guideway to allow vehicles to pass. Vehicles self-navigate and self-steer, using dead-reckoning backed up by sensors detecting the edges of the guideway.

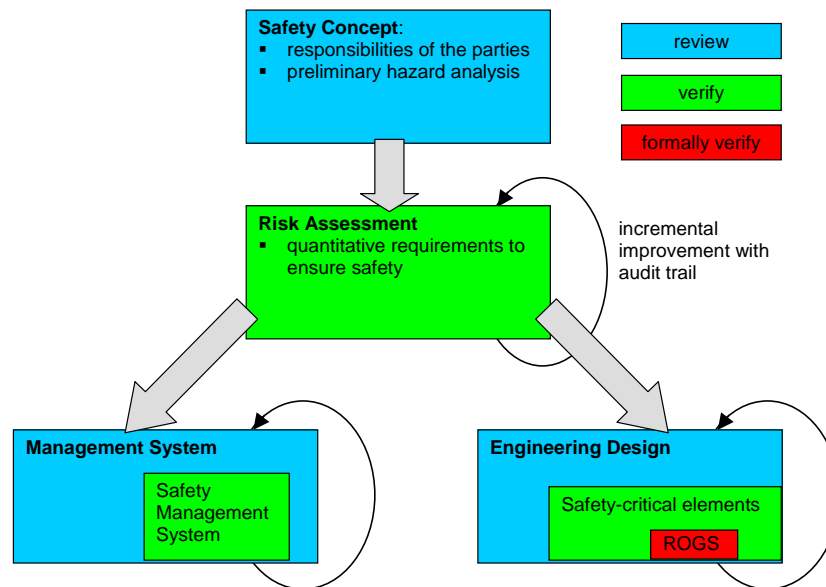
ULTra’s developer has established a Safety Verification Team (SVT). This is a group of independent experts who review the design, implementation, trials and operations of

ULTra to ensure that it is compliant. ULTra is expected to be first deployed in the UK at Heathrow Airport so its verification has to meet the UK regulations; SVT is the “Competent Person” required by ROGS and includes expertise on airport operations as well as PRT.

The members of SVT are:

- Dr Chris Elliott FREng: system engineer and lawyer working in health and safety and regulation of technology
- Paul Fairbairn: civil engineer and former Director of BAA (the owners of Heathrow and 7 other UK airports), bringing expertise on the design and operations of airports
- Steve Firth: former railway inspector and rail accident investigator, now specializing in trams and metros in the UK and Ireland
- Dr John May: Director of the Safety Critical Systems Centre of the University of Bristol, specialist in high-integrity software for the nuclear and transport industries.

The duties of the SVT are summarized in the diagram. The scope is wider than that demanded by ROGS (which for example does not require that the SMS be verified as compliant) or even of safety. Because safety and reliability emerge from the same qualities of the system, SVT provides an independent review of all aspects of ULTra.



SVT verifies each element of the ULTra system by considering and, if appropriate, certifying, Safety Cases. Although the members of SVT have wide knowledge of ULTra, verification is based only on the information presented in the Safety Case for that element, judged against the Safety Requirements document (which SVT also verifies).

Conclusions

Safety is critical for the success of PRT. It presents a challenge to safety regulators because it is novel – the UK solution of extending rail regulations to cover PRT avoids developing a dedicated regime but is not tailored to the specific hazards not to the measures needed to manage them. It also represents a challenge to the designers, builders and operators of PRT, because the level of safety that will be demanded is very high.

This requires a systematic approach to safety that incorporates:

- explicit analysis and statement of safety requirements
- safety as an implicit feature of design, not a “bolt-on”
- formal, independent verification that the design delivers the requirements.

These three steps together ensure that PRT will satisfy the regulators that it is safe and, which is even more important, be safe.