Design standards and third party approvals - why?

Sam Barrett, Senior Engineer, AEGIS Certification Services, continues the series of articles for Rail Infrastructure as he asks: Why do plant design standards and third party approvals exist?

Hazards

On-Track Plant (OTP) and On-Track Machines (OTMs) are, quite clearly, machines. They are, therefore, CE marked (after 1st January this will be a UKCA mark) as compliant with the Machinery Directive. Clause 1 of the essential safety requirements of the Machinery Directive says that the manufacturer must identify all the hazards that their machine poses, and then either eliminate the hazard or reduce the risk to acceptable levels. This is a big task. Identifying the hazards is onerous, establishing how to eliminate each of them, or reduce them to acceptable levels, is even more so. What, you may ask, is an 'acceptable level'?

Standards

This is where design standards have their biggest impact. If every manufacturer was told that they had to make machines that are 'safe', they would a) each spend a lot of money trying to determine what 'safe' is and b) each design machines with different levels of safety to one another. Take for example, the impact protection of side windows on an OTM. Most manufacturers would identify the need for the glass to resist impacts; but what impacts should they resist, and what type of glass is required to achieve this? Each manufacturer could conduct their own research, at great expense, and likely come up with a different answer to each other. Alternatively, they can look in the design standard and see that they should fit 6mm safety glass.

Ultimately, every safety decision constitutes an 'engineering judgement'. While each of us is competent to make such decisions, the subjective nature of 'safe' means that we will each make different decisions. Additionally, if we make an engineering judgement in isolation, it will be based on our individual experience. For the extremely experienced among us, this could be 50 years of railway experience although it is likely to be less. The engineering judgements made in a standard constitute the combined experience of the drafting panel, often multiplied over numerous iterations of a standard plus the large group of stakeholders who review the draft; not only is this collective experience larger, it is also broader.

Phase 1 of the enquiry into the Grenfell Tower fire found that the cladding likely did not comply with building regulations (i). The specific clause that the building is thought to not comply with states, 'The external walls of the building shall adequately resist the spread of fire.' (ii). What is 'adequate'? Most people would be in agreement that the fire resistance of Grenfell Tower cladding was not adequate, but at the time of installation someone made the decision that it was; furthermore, very similar cladding

has been installed on a number of other buildings, hence numerous different people made the decision that such cladding was 'adequate'. There are several failings that led to the tragedy in Grenfell Tower. One of them was the engineering judgement that the cladding offered adequate fire resistance. Another, arguably, is expecting each building contractor to make their own decision as to what constitutes 'adequate' - not only is this an extremely laborious task, but it has also failed to control the fire risk as intended. Phase 2 of the Grenfell Tower enquiry will be investigating whether the testing and certification of fire materials needs to be more prescriptive.

Third party certification

It is a fact of life that we all make mistakes. It is also well accepted that spotting mistakes in your own work is more difficult than spotting mistakes in someone else's. That is why most companies have a document approval process that requires the person checking a document to be different to the person who wrote it. By accepting that we all make mistakes, we can put processes in place to try to reduce the probability of these mistakes making it into service. This is where the need for third party certification through Notified Bodies, Designated Bodies and Plant Assessment Bodies, like AEGIS, arises. A third party provides an additional layer of checking, but also provides an impartial check that is not influenced by the thought processes and decision making that went into the development of the machine.

Those familiar with rail plant design and certification will be aware of performance level analysis, whereby the reliability of safety systems is assessed considering the architecture of the system. A simple input - logic - output, or sensor - logic - actuator, system provides a relatively low level of reliability, even with high reliability individual components. Reliability of the system can be improved by duplicating sensors and actuators (redundancy), automatically testing the system at regular intervals (monitoring) and using different types of sensor or actuator to prevent common cause failures (diversity). When the severity of system failure is higher, a higher level or safety reliability, and hence a more robust system architecture, is required.

A similar analysis is undertaken in the aerospace industry and was carried out by Boeing for its 737 Max aeroplanes. When designing a safety system that would be used to prevent aerodynamic stall, the engineers determined that the severity of failure of the system was either 'major' or 'hazardous', depending on the scenario in which it failed. As a failure of the system was not considered to be 'catastrophic', the analysis determined that a system with a single

sensor providing the input was sufficient. Following two instances of failure of that sensor, two 737 Max aeroplanes crashed killing everyone onboard; by almost anyone's measure, these were catastrophic events (iii).

The certification process by the Federal Aviation Authority (FAA) placed a large amount of the technical review and approval work of the aeroplanes under Boeing's responsibility, including the review of the safety analysis. While the technical content was reviewed, the third party element of the review was removed or reduced. Boeing was placed in a position where it was required to design a product and then spot its own mistakes. It made the mistake, for example, of assigning the 'hazardous' failure category based on the system being able to apply a 0.6 degree change to the plane's tail when, in fact, the system could apply 2.5 degrees. While the resulting congressional enquiry notes 'faulty technical assumptions' made by Boeing, it also describes 'grossly inefficient oversight by the FAA' (iv).

The Boeing 737 Max disasters are a stark reminder of the need for a third party review of safety systems. While the engineers designing the systems are highly competent, mistakes are inevitable and asking someone to spot their own mistakes is setting them up to fail.

Deviating from standards

While standards are an essential component to plant safety, they are not perfect; they cannot account for every design of plant, particularly highly innovative types of plant. Each clause in a standard exists to mitigate a certain risk, but a manufacturer may choose to mitigate that risk in a way more appropriate to their design of machine. It is essential that manufacturers are able to do this and that is why the derogation process exists; the manufacturer can make a justification to the mandating authority, either Network Rail or the RSSB, and they will, where they agree, grant permission for the machine not to comply with specific clauses. While standards are often cited as a barrier to innovation, the derogation process aims to allow manufacturers to develop novel solutions whilst ensuring that the risks the standards were designed to mitigate remain controlled.

Improvements made and further improvements to make

Plant, and in particular OTP, have historically been viewed as one of the higher risk assets on the railway. However, with iterative improvements to standards, plant safety has improved significantly. According to the RSSB's annual workforce safety report (v), 'machinery/tool operation' is currently the lowest risk posed to the workforce when on or about the line, with a risk score of 0.7. This is compared to a risk score of 4.3 for 'slips, trips and falls' and 1.5 for 'struck/crushed by train'. Unfortunately, some plant incidents have been counted in 'contact with object' (risk score 2.8) and 'other' (risk score 1.9) so the total risk score associated with plant is higher than the headline figure of 0.7. However, when considering the inherently dangerous nature of plant, and the number of high consequence incidents historically associated with plant, the figures are encouraging.

Although significant advances have been made in plant safety, the 'state-of-the-art' - the technology available to manufacturers at a price proportionate to the product value and risk - continues to evolve. As the state-of-the-art evolves, so too must the standards that govern plant design; as an industry, it would be negligent of us not to take advantage of new technologies, or existing technologies available at lower prices.

Safety improvements can also be achieved by seeking to identify the causes of incidents occurring on machines that comply with current standards, and then closing the gaps. Any incident is the consequence of a chain of decisions; whilst it is easy to identify the decisions made by the operator, the root cause perhaps exists in a much earlier stage of the decision-making tree - at the design, standardisation or approvals stage. 'The operator turned the RCI off' - why was the operator able to put the machine in dig mode when the machine was being used for lifting? 'The operator see-sawed the machine when on-tracking' - why was the machine able to become unbraked? Those of us with the luxury of making our decisions from a desk, inside, during daylight hours, should be ensuring that safety systems are robust enough to account for decisions made in the heat of a tight timescale shift, in the middle of the night, in adverse weather and ever-changing site conditions. The more risks we can mitigate at the standardisation stage, the greater chance we have of preventing that risk occurring in the design, construction and, ultimately, the use of a machine.

Sam Barrett, Senior Engineer, AEGIS Certification Services.

Closing the final gaps

While standards can be used to mitigate a high proportion of risks, they cannot account for all risks posed by a particular piece of machinery. The requirement of Clause 1 of the Machinery Directive, that manufacturers identify hazards and eliminate or control them, is not satisfied in full by standards compliance. Manufacturers must still undertake the hazard identification and management exercise, and any residual risks present after standards compliance has been achieved must be managed. Ultimately, the management of product design risk is the manufacturer's responsibility; standards and third party certification are tools designed to help achieve this objective.

References

- i: *https://assets.grenfelltowerinquiry.org.uk/ GTI%20%20Phase%201%20report%20 Executive%20Summary.pdf*
- ii: *https://www.legislation.gov.uk/uksi/2010/2214/contents/made*
- iii: *https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lion-air-crash/*
- iv: *https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf*
- v: *https://www.rssb.co.uk//media/Project/RSSB/Platform/Documents/Public/Public-content/Improving-Safety-and-Health/ashr/2019-20-Workforce-Safety.pdf?la=en*