

# New design targets for the Common Safety Method for Risk Evaluation and Assessment

## What are design targets?

The Common Safety Methods for Risk Evaluation and Assessment (CSM RA) regulation has been amended to introduce the concept of mutually recognised safety design targets for technical systems.

If the proposer of a change to a technical system can demonstrate that functional failures of the technical system are no greater than the design targets, then the acceptability of the failure rate of these functions is, by definition, mutually recognised in all EU member states. There are two classes of quantified design targets described in the amendment:

Class (a) design target; this is for functional failures that have the potential to lead to *catastrophic accidents*. In this case, the risk associated with a technical system does not

have to be reduced further if the frequency of the failures of the associated function is demonstrated to be less than or equal to  $10^{-9}$  per operating hour.

Class (b) design target; this is for functional failures that might lead to *critical accidents* affecting a small number of people and resulting in at least one fatality. For these failures the risk does not have to be reduced further if the frequency of the failures of the associated function is demonstrated to be less than or equal to  $10^{-7}$  per operating hour.

Design targets are intended to be used for the design of electrical, electronic and programmable electronic (E/E/PE) technical systems. They are not intended for the design of purely mechanical systems.

## What does this mean for me?

The new amendment came into force on 3 August 2015. When introducing a new technical system or implementing a change to a technical system, the proposer now has the option to use the design targets, provided that the system has the potential to lead to either catastrophic

or critical accidents. Using the design targets is mandatory if the proposer is using explicit risk estimation and wants to have the acceptance of the change mutually recognised in other member states.

## What does this regulation mean for those running railway projects?

If you are procuring technical systems that have been used in similar applications in other EU member states, then evidence from those projects that the relevant functional failures have met the design targets provides assurance that these failures have an acceptable level of

functional integrity. This reduces the need to repeatedly review safety evidence, reducing project costs and allowing for more flexibility in the choice of technical systems for railway projects across Europe.

## What would I expect to see in any initial demonstration that the requirements have been met?

The European Railway Agency has developed guidance which shows how the requirements can be met. This includes an indicative mapping of key functions of the railway to the class (a) and

class (b) requirements. The guidance points to certain levels of design process that are required in each case, and acceptable standards to apply, eg the RAMS standard EN50128.

## Is this all that I need to do to assure myself that a technical system is safe in use?

No. Meeting of these requirements is only one part of the safety demonstration that is needed and is concerned only with the acceptability of anticipated failure rates of technical systems. The need to understand the broader hazards of the use of a technical system, and the acceptability

of any resulting risk still remains. Note, in particular, that if the introduction of a technical system represents a 'significant change' in accordance with the CSM RA, then the full risk management framework from the regulation must be applied.

## Where can I find more information on the Common Safety Methods for Risk Evaluation and Assessment?

The original regulation was published on 30 April 2013 as [402/2013](#). This was amended by regulation [2015/1136](#) of 13 July 2015, which introduces the design targets. Guidance on applying the regulation has been produced by both [ORR](#) and [RSSB](#). A good starting point is the [management of change](#) page on RSSB's website which contains links to detailed guidance. More general guidance on how companies in the rail industry take decisions that affect safety can be found on the website in the document [Taking Safe Decisions](#).

In-depth training courses on the application of the regulation are available, run by rail industry consultants. In addition, we will continue to give industry briefings and workshops, as appropriate.

For details on RSSB briefings on Common Safety Methods for Risk Evaluation and Assessment contact [wayne.murphy@rssb.co.uk](mailto:wayne.murphy@rssb.co.uk).

For feedback on your experience with the regulation contact [david.griffin@rssb.co.uk](mailto:david.griffin@rssb.co.uk).