

The paradox of ultra-safe systems

Rene Amalberti

SAFETY is driven by a simple principle: complete elimination of technical breakdowns and human errors.

But is there a limit for reduction of error within the present system?

Clearly, the main operating principles of systems bear within themselves a maximum safety potential.

The commonsense approach to safety has been successful over decades, but is now beginning to lose relevance.

The commonsense approach involves three principles:

- Designs which generate systems with high safety potential, subject to technical and human failings.
- Improvements in machine reliability.
- Reporting systems which identify and address failures.

Reduction of errors and breakdowns is effective in systems where the risk of disaster is one failure for 100,000 events (10^{-5}). In these systems improved procedures, staff training, automation and error blocking solutions are effective.

Over-stretched? In ultra-safe systems, such as airline travel, where the risk of disaster approaches one accident per 10 million events (10^{-7}), accidents usually occur in the absence of any serious breakdown or error. They result from a combination of factors, none of which will cause an accident on its own.

Most of today's human-



machine systems were designed in the 1960s. These systems may not be able to reach safety levels higher than the record of 10^{-7} .

As a system approaches "ultra-safe", investments tend to stop being directed at safety and are earmarked towards improving performance.

The system can then find itself subject to the risk of a disastrous accident because it's over-stretched performance has given rise to new risks. Beyond a certain threshold comes a reduction of margins and recovery opportunities in degraded conditions.

Optimising safety around 10^{-7} requires priority to be given to safety rather than to performance improvement.

When safety has nearly reached its maximum level within a given system, the objective becomes to contain the system within its optimised limits as long as possible.

A comparison with geriatrics illustrates this point. Very old persons are not medically cared for in order to be cured using intensive treatment, but only to prevent suffering and prolong life with maximum effectiveness. The drugs used are less potent and interactions between different ailing organs need to be taken more seriously than with younger patients.

Ultra safe systems have reached today's level of safety through a lengthy, extensive

and crisis-ridden optimisation process, during which these systems have aged and matured.

These systems will eventually be replaced by others having a different safety potential (such as complete datalink); so goes the development of technical cycles.

We must recognise that these systems are nearing the end of their life, and should not be placed off-balance by requiring operations to take place within unreachable performance and safety objectives.

Increased performance beyond a certain threshold can result in an increased risk of reduction of margins and recovery opportunities in degraded conditions.

Optimum safety: Optimum safety is achieved through the careful monitoring and the tolerance of a minimum number of incidents.

The message is twofold:

- It is essential to fully understand system behaviour.
- Such a system must be treated with methods allowing it to remain simultaneously at the edge of safety and at a sufficient performance and competitiveness level to resist market constraints.

Edited excerpt from "The paradoxes of almost totally safe transportation systems." The full paper will be available in the last Safety Science journal of 2000.

Professor Rene Amalberti is Chief of the Cognitive Science Department at IMASSA, France.