

# Safety Analysis of Automotive Embedded Systems

**Peter H. Jesty**

Peter Jesty Consulting Ltd

**David D. Ward**

MIRA Limited

**Roger S. Rivett**

Land Rover

Copyright © 2008 SAE International

## ABSTRACT

This paper provides an overview of the new MISRA publication, Guidelines for Safety Analysis of Vehicle-Based Programmable Systems. It describes a process which needs to be incorporated into a company's or organization's management structure so they can manage safety effectively. The MISRA Safety Process comprises two principal phases: Preliminary Safety Analysis and Detailed Safety Analysis. The former identifies what needs to be done; the latter demonstrates that it has been done correctly.

## INTRODUCTION

In 1994 the MISRA project, which was part of the UK government funded program on safety-critical systems, published the *Development Guidelines for Vehicle Based Software* [1]. This document covered a number of topics, but, since it takes a goal-oriented approach, guidance is usually at a high level. It later became clear that additional guidance was required for the safety analysis of programmable automotive systems, and so MISRA decided to produce a supplementary document on this topic that incorporates the knowledge and experience gained over the intervening years. The result is the *Guidelines for Safety Analysis of Vehicle Based Programmable Systems* [2].

An important feature of these new MISRA Safety Analysis Guidelines is a revised approach to hazard analysis and risk assessment. The issues associated with these topics have been described in an earlier paper [3]. However, whilst these topics are of great interest to many people, they cannot be effective without a suitable management structure and safety lifecycle to support their use. This paper therefore describes the approaches to safety management and the MISRA safety process contained within the MISRA Safety Analysis Guidelines.

The fundamental approach that is taken by the MISRA Safety Analysis Guidelines is shown in Figure 1. It requires planning an analysis in order to find out what needs to be done. Then, whilst the development work itself is being done, evidence is collected to demonstrate, eventually, that it has all been done correctly and that it can be shown with a sufficient degree of confidence that the outcome corresponds to the results of the initial analysis.

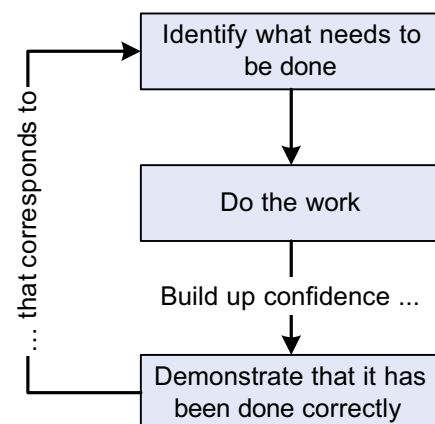


Figure 1: The Development Approach

## SAFETY MANAGEMENT

### OVERVIEW

In order to manage safety effectively, it is necessary that all the safety activities be performed with a basic framework that forms part of a company's engineering culture and structure, and that has its own organization.

Figure 2 shows how safety and quality fit together at various levels within an organization. The first three levels, *strategic*, *tactical* and *objective*, correspond to "identify what needs to be done" in Figure 1, whilst

*product-substantive* corresponds to “demonstrate that it has been done correctly”.

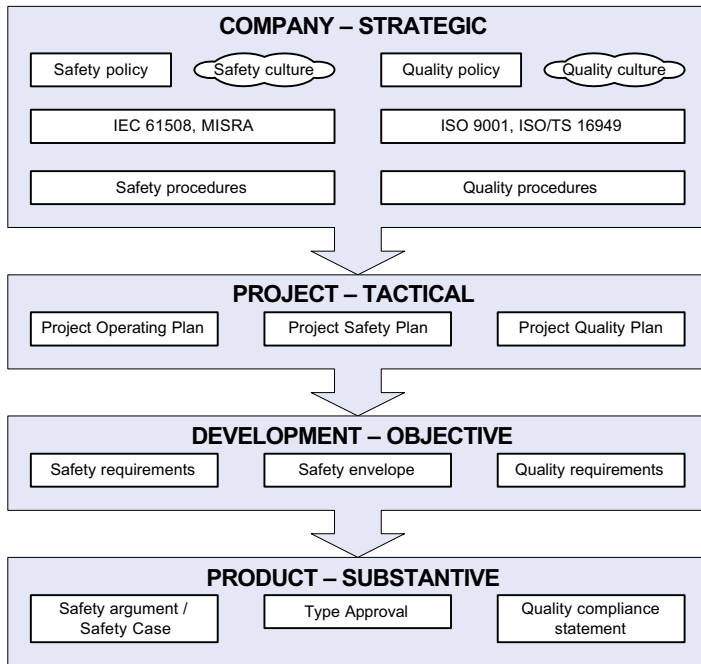


Figure 2: Safety Management Structure

In order to establish an effective safety management structure a company or organization requires a safety policy that defines the company-wide strategy for the management of product safety. This, like all top-level company policies, is the means by which the intent and commitment of the highest level of management is stated, though it must be supported by a suitable organizational structure and safety culture to be fully effective. From this policy a management structure is created to ensure that the policy statements are adhered to, and the means of their implementation monitored for effectiveness throughout the engineering lifecycle.

As with quality, each project should start with safety planned into it. A strategy alone is not effective: it depends on tactical decisions, objectives, and substantive actions to become effective. The safety policy establishes the strategy, and the individual project safety plans define the tactics in the form of engineering procedures that will be specific to individual projects.

In order to establish safety requirements for the system, the “expected” or “intended” use of the vehicle needs to be defined. These operational constraints are termed the Safety Envelope.

During the development of the system evidence is collected to demonstrate that it is safe for its intended use in a safety case. The strategy used to create a safety case is known as the Safety Argument.

An important part of safety management is that the engineering staff employed to manage safety should have professional competencies in safety engineering, appropriate to their level of responsibility.

## SAFETY CULTURE

A significant impact on the potential for harm that might be caused by a vehicle or its systems arises from the care, or lack of care, with which the product was engineered and developed. Where a safety culture exists, the members of an organization actively promote and pursue the achievement of safety as a primary objective for the product and its development. For an organizational safety culture to be successful, the promotion of safety must be actively pursued and supported at every level, starting at the top of the organization.

Thus a safety culture is not only about good attitudes in the members of the organization, but it is also about good safety management being established by an organization. It requires that the highest priority be given to safety and to a constant assessment of the safety significance of events and issues so that the appropriate level of attention can be given to them.

## SAFETY POLICY

A safety policy should define the company’s or organization’s strategy for encouraging and maintaining safety. The safety policy comprises a set of statements of commitment and intent from the board of directors of a company or organization. The statements should define, at a high level, the fundamental aims and responsibilities for managing product and process safety issues as specific, verifiable goals. The safety policy document is thus the top-level safety document, which stands at the apex of all other safety procedure documents, just as a quality policy document heads up a company’s quality procedures.

As with a quality policy, the safety policy should be monitored for its effectiveness, and improvements identified and implemented on an ongoing basis.

## PROJECT SAFETY PLAN

In addition to having a project quality plan, to implement effective safety management it is also necessary to have a project safety plan. This states all the specific actions, deviations, limits etc. that cannot be covered by the global set of procedures of the Safety Policy. It shows how and when all the elements required by the Safety Argument will be produced. A project safety plan should be assembled at the start of the project, but should be reviewed during the engineering lifecycle to ensure that it remains appropriate for handling the actions resulting from safety analysis and risk assessment. If any deficiencies are found, then all the activities that depend on the deficient process may need to be re-assessed.

Where the safety policy might state that safety issues should be examined and signed off at project milestones, the project safety plan would indicate which safety issues and which milestones relate to their sign-off.

It should be noted that it is necessary to ensure a degree of independence between those who are responsible for the design of a system, and those who are responsible for implementing the project safety plan. The higher levels of safety integrity should require greater independence of assessment to ensure that there is neither bias from the development team, nor misplaced pressure from management [1].

## SAFETY ENVELOPE

It is necessary to identify a consistent set of conditions that will be assumed when undertaking a safety analysis on a system. Indeed it is often the case that these conditions will relate to the type of vehicle, rather than the type of system. Exceptions to these conditions may be incorporated in a project safety plan for an individual project, system, or product. For example, a dynamic vehicle control system may be introduced into a vehicle design for a number of reasons, including:

- As an aid to normal driving, and introduced to mitigate hazardous driving conditions due to the driver misunderstanding the situation, or overestimating his or her driving skills, e.g. ABS or Active Yaw Control.
- To ensure that a vehicle is stable for all rated load and driving conditions, e.g. Electronic Stability Enhancement.
- To provide assistance to the driving task, e.g. Adaptive Cruise Control, Intelligent Speed Adaptation.

A Safety Envelope defines the operational and environmental limits within which the system is expected to behave in a safe manner. It defines the "expected" or "intended" use of the vehicle with the system fitted and operational, so that risks associated with the system can be evaluated under defined conditions, should it fail to perform an intended function correctly. A Safety Envelope will normally only apply to hazards associated with the movement of the vehicle, because the others will be covered by existing regulations.

When the system under consideration is an aid to "normal driving", i.e. only to come into operation when driving conditions are abnormal, or to provide additional information to the driver concerning the environment, then the Safety Envelope may need to consider the widely recognized phenomenon of risk compensation, where drivers rely on extra features for part of their normal driving behavior. Particular examples of this are relying on the ABS to provide improved braking characteristics, and relying on Electronic Stability Control to compensate for what would otherwise be unsafe modes of driving. The Safety Envelope will need to be defined in a manner that will take into account this example of reasonably foreseeable misuse, as required by IEC 61508 [4].

It should be noted that, although most nations have a standard of driving that would normally be expected of a reasonable, prudent and competent person in all the associated conditions, a company may wish to extend the Safety Envelope beyond this limit to cover unintentional excursions due to short-term misjudgments of the current conditions.

## SAFETY ARGUMENT AND SAFETY CASE

The ultimate goal of a safety management approach to systems engineering is some form of evidence that the system is safe within specified limitations (the Safety Envelope). This evidence may be collected together into a Safety Case.

A Safety Argument is the logical explanation that ties together the evidence from the system safety analysis with the safety requirements, and shows that all the hazards have been mitigated. It is essential for the creation of the project safety plan because it specifies the evidence that will be required to support the Safety Case, and therefore what processes and procedures are required in order to produce that evidence. The Safety Argument may, of course, iterate as the project proceeds. The Safety Case shows that the Safety Argument has been fulfilled, and is supported by the necessary evidence.

In non-automotive industries, a Safety Case is normally assessed by an independent party. The final output from the third party assessor, or auditor, will usually be a report accompanied by a certificate. While the latter is not currently a legal requirement for road vehicles, a Safety Case is useful to confirm that everything necessary has been done, and may be used as evidence of due care for the purpose of defending a legal action. Advice on when to use independent assessment in the automotive industry can be found in [1].

## THE MISRA SAFETY PROCESS

### THE SAFETY LIFECYCLE

The MISRA Safety Analysis Guidelines are intended to be compliant with the requirements of the overall Safety Lifecycle defined by IEC 61508 [4] (see Figure 3). However, the safety lifecycle of IEC 61508 does not align well with the typical product development processes followed for vehicles. In particular, automotive systems are usually subject to a Type Approval process, whereby the system is fully developed and validated, then approved, then released for series production. In contrast the safety lifecycle in IEC 61508 assumes that the final validation of the system is carried out once it has been installed on the plant as part of the commissioning process.