The Role of Data in Safety-Related Railway Control Systems

Alastair Faulkner, MSc., MBCS, C.Eng; CSE International Ltd., Glanford House, Bellwin Drive, Flixborough DN15 8SN, UK

Neil Storey, Ph.D., FBCS, MIEE, C.Eng; School of Engineering, University of Warwick, Coventry, CV4 7AL, UK

Keywords: data-driven safety-related systems, data, safety, railway control systems

Abstract

In the production of a computer-based safety-related system, it is common to partition the hardware and software elements into a system architecture. The software part of such an arrangement will generally include both the instructions that are executed by the processor(s), and the data that is used and produced by these instructions. In some cases, a large amount of static or configuration data forms an essential element within the system and plays a vital role in ensuring its correct operation. While data is subject to errors, experience shows that it is often not subjected to safety analysis techniques such as hazard and risk analysis. Data is often treated in a totally unstructured manner (often making error detection difficult) and very rarely is fault tolerance used to protect the system from data errors.

To illustrate the role and importance of data in safety-related systems, this paper looks at the data associated with a railway command and control system. Such a system has a range of safety-related functions, and must also operate in the context of other safety, protection and business planning systems. The paper considers typical data errors associated with the railway environment and proposes the early definition of a system data architecture, which will allow the application of safety analysis techniques such as HAZOP.

Introduction

The systematic production, development and maintenance of configuration data for safety related systems receive little attention in both the literature and standards such as IEC 61508 (ref. 1). The safe operation of such systems is likely to depend upon the correctness of data. In particular, many safety-related systems consist, wholly or partially, of generic software elements which are adapted to a particular application by means of configuration data which describes the real world environment in which the system will operate. Configuration data is most conveniently regarded as "static" data in that it is created as part of the system development process, in contrast to "dynamic" data, which is created when the system executes.

Examples of such systems are found within the railway industry in the form of railway signalling and railway command and control systems. In the railway control environment safety-related systems are arranged as an interconnected suite of computer-based applications. Traditional protection systems are employed to reduce the risk of train collisions; an example being the use of low-level systems known as *interlocking*. These combine railway infrastructure elements such as tracks, points, signals and train detection equipment, to allow railway signalmen to set routes and receive indications.

Interlocking systems provide a good example of the distinction between static and dynamic data. A *track circuit* is a form of train detection equipment, and unchanging information about a range of track circuits (their identifiers, their relationship to other track circuits, and their input/output addresses) is described by *static* configuration data. The current status of the track circuits (whether they are occupied or unoccupied, or whether they are serviceable or unserviceable) is described by dynamic data, and is obtained by sensor readings and other inputs. Generally the configuration data and the dynamic status data are stored within a single data structure.

One of the functions of interlocking is to provide protection against the multiple occupancy of individual sections of track. However, it does not provide any protection where a train is 'out of gauge', for example, where a heavy goods train is to pass over a light railway bridge. Clearly, the railway command and control system needs

to provide protection against these out of gauge trains to ensure the safe operation of the railway.

Railway command and control systems range in scale from small signal boxes, which control a single control area operated by signalman, to large complex systems. These systems use a range of technologies from mechanical devices through electromechanical and electronic systems. This paper is particularly concerned with those railway command and control systems that are computer-based. These computer-based systems can range from limited installations that have control areas similar in size to traditional, manual signal boxes, to very large, potentially national command and control centres.

The purpose of these railway control systems in the UK environment is to deliver 'train paths'. A train path is a commercial agreement between the train operating company and the owner/operator of the railway infrastructure.

In the UK, information that identifies the trains to be run, is referenced in the railway timetable, which also describes the 'consist' of the identified trains. The consist is the description of the train to take a particular journey. The consist will comprise a list of each element of the rolling stock, in running order, starting with the locomotive. Each rail vehicle has a unique identifier, which is used to identify a classification known as 'route availability'. The concept of route availability is discussed in the section 'Out of gauge data errors' later in this paper.

Data is used to describe the geographical arrangement and capability of the rail infrastructure. Further data references to the journey to be taken by the train are contained within the timetable. The infrastructure data is largely static or slowly changing, whereas the timetable may be changed to overcome operational difficulties.

Background

The railway industry in the UK has a history stretching back some 150 years. This paper does not intend to deal with the historical treatment of data for railway control systems.

The treatment of data by general standards such as IEC 61508 has, of necessity, grown out of the need to implement protection systems for well-defined operational circumstances such as individual process plant protection systems. These standards have been developed over a number of years, and in the case of IEC 61508 took over 15 years to produce the first issue.

IEC 61508-4 (ref. 2) defines software as an "*intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system*". This definition is not of great help in the management of data used by safety-related systems.

In some development standards, for example the draft IEC 61511 (ref. 3), programming languages are classified into Full Variability Languages (FVL), Limited Variability Languages (LVL) and Fixed Program Languages (FPL).

Examples of Full Variability Languages (FVL) include high-level languages such as Ada and C. The treatment and use of FVLs is extensively considered in IEC 61508-3 (ref. 4). FVLs are generally used to define the invariant part of the software.

An example of a Limited Variability Language (LVL) is an intermediate level language such as ladder logic. An LVL would allow "*the combination of a set of proven functions in limited proven variety of combinations to implement an application*" (ref. 3). The use of ladder-logic in a safety-related application is discussed in the SEMSPLC Guidelines (ref. 5). LVLs are used to provide configuration information for some railway interlocking systems.

A Fixed Program Language (FPL) is typically used to provide sensor scaling or is the output from a graphical configuration tool. Such a language might be used where a railway signalling design, in the form of a scheme plan, is translated into a data model for a railway command and control system. The graphical tool might incorporate some or all of the data checking rules. The configuration tool represents the data entered through a graphical user interface and expresses the output in the form of an FPL and associated data tables.

A system such as a railway command and control system may also use external data in the form of a timetable or references made from a timetable to train consist information. This form of data is not readily input by means of an FPL,

although its structure may be defined by a formal grammar.

European railway-specific standards such as references 6, 7 and 8 are, at the time of writing this paper, in the process of being issued. In particular CENELEC EN50128 section 17 "Systems configured by application data", (ref. 8) proposes the following:

1. that the development process should include a data lifecycle;
2. that the integrity of the tools employed should be appropriate to the Safety Integrity Level (SIL) of the system concerned; and
3. that the data lifecycle identifies a number of documents to be produced.

However the representation, in terms of the data model, and realisation, in terms of the population of the application data are not addressed.

Welbourne and Bester (ref. 9) identify several categories of data:

1. Calibration data, for example alarm and trip levels;
2. Configuration data, for example display screens for a specified area; and
3. Functionality data, for example control states to be taken up at failure.

Unfortunately, this categorisation does not assist in the management of data, as Welbourne and Bester (ref. 9) do not propose the definition of an overall system data model. Consequently, it is not clear how the analysis of data errors is to be achieved in the overall system context. Welbourne and Bester (ref. 9) do identify that the tools used in the manipulation and management of the data should be appropriate to the System Integrity Level (SIL), but fail to identify how this data integrity requirement is obtained.

A major weakness in the standards referenced in this section is that they do not identify a requirement for the definition of a data model. They also fail to give guidance on appropriate forms of data representation or the mitigation of identified system hazards through the selection of high integrity data model elements.

The identification of a system architecture *is* treated in the standards (refs. 1, 7 and 8) but is based simply upon the need to provide a vehicle for analysis of the proposed solution. The identification of the system architecture should recognize the role played by the configuration of the system components by data (FPL and LVL), as a majority of systems will contain these elements to a greater or lesser extent.

The System Architecture

A complete system architecture should be identified early in the development lifecycle. This architecture should clearly identify the elements of the system in terms of the functional and non-functional requirements, hardware, software and a data model.

The non-functional requirements should include timing and performance, capacity, robustness, safety properties, accuracy, reliability and maintainability. The system architecture should lend itself to analysis. Analytical techniques such as Fault Tree Analysis or HAZOPS (ref. 10) should be used to establish the safety properties of system components and the consequences of failure of each component.

The safe operation of the system is likely to depend upon the correctness of the data model and the external data sources. Therefore the data model should lend itself to analysis, including hazard analysis techniques, and the populated data model should be susceptible to verification and validation. Here the term "populated" is taken to mean, "configured for a particular application".

Where data elements make reference to externally supplied data such as that contained in the railway timetable, these references should be identified and recorded. Where a railway timetable supplies information about a train whose characteristics are unknown to the railway command and control system, the latter should present this information for the operator to exercise his or her judgement.

The System Data Model

The structure and definition of the system data model are likely to have a significant impact on the operational safety of the system in question. Data elements are likely to be supplied across the system boundary from external sources, beyond the control of the command and control system. The validation, completeness and accuracy of these external data sources should be examined during the safety lifecycle. Estimates should be

constructed as to the likely error rate within the supplied data, as on the detection of any error the system will need to refer the command decision to the operator and as a consequence increase the operator workload.

Certain elements of the data are likely to be used by more than one function within the system. Data errors within the static data infrastructure description are likely to affect a majority of trains which pass over the route, whilst data errors within the consist references are likely only to affect one type of train or one instance of that train type.

The configuration of the system as a whole is likely to combine some element of LVL, FPL, populated data structures and external data, as noted above.

The populated data model will provide the system with a static or a slowly changing description of the application instance. In the case of the railway command and control system this will be the geographical and topological arrangement of the infrastructure elements and their capability, approvals and exclusions within the area of railway under control.

The system data model should be designed to support verification and validation of the populated data model. The data model should be self-consistent. The data model should demonstrated independence either in the form of a modular construction, or by the definition of strong data references so that changes to the populated data will not require the entire populated data set to be revalidated.

Where data references are made between data elements, the consequence of failure of these references should be identified, and measures taken to detect failed data references. Where the system integrity requirements demand, the data model should lend itself to automated error detection and correction.

The system data model should be specified and documented together with rules for data checking. In many instances a data model will contain many 'small' rules. These rules act on individual data elements to enforce properties. An example would be that where a railway signal is defined as having four aspects (combinations of coloured lights), it is necessary that all four aspects are represented in the data.

Data Errors

Data errors fall into two broad categories, *detectable* errors and *plausible* errors. Detectable errors are those data errors that can in principle be detected by the data rules. Plausible errors are those that produce a value, which is 'reasonable' (in that it cannot be detected by the data rules) but which is incorrect when validated with respect to the real world.

Emergency Speed Restriction Data Errors

An example of a simple data element would be an Emergency Speed Restriction (ESR) on a section of railway track. The intention of placing this speed restriction would be to reduce the running speed due to some track defect. The speed restriction would identify a location, a speed, and a distance over which the ESR applies. Examples of data errors associated with an ESR would be: the specification of the wrong speed, the wrong location, or an incorrect distance.

Speed is likely to be specified as a scalar value. As this is intended as a speed restriction its value will be less than the normal running speed; and will be positive. Simple rules such as these will allow the detection of gross errors, but will not detect plausible but incorrect values (for example an ESR of 60Km/h rather than the correct 54Km/h in a track section with a normal running speed of 90Km/h).

The location of the speed restriction may be specified in conjunction with an *existence* rule; that is, that this location 'exists' on the railway. This existence rule will not detect the wrong location, although it could be used to reject a wholly incorrect or non-existent location.

The use of physical distance, in the UK railway, is prone to error based on the continued use of a number of measurement systems and multiple datum points. For historical reasons, some of which are based in legislation concerning the placement of posts at one eighth of a mile intervals, distance, in the UK, has been expressed in a number of measurement systems. Railway records are based in the measurement system of the day that they are created, and are generally not updated until the area is re-signalled. The continued use of these measurement systems further confuses data structures, such as ESR, which rely on distance-

based measurements. The definition of the ESR may be changed to specify a start location and an end location to more reasonably resolve possible data errors.

'Out of Gauge' Data Errors

This paper has already introduced the 'out of gauge' concept. In the UK, the railway timetable identifies a passenger train to run at a certain time, and to take an identified route, stopping at a number of stations. The timetable identifies the train. The train 'consist' is obtained by an enquiry to an associated information system. Through this mechanism the railway command and control system has identified the train journey, its start, destination and its waypoints, together with each element of the train, from locomotive to individual carriages.

The static configuration data defines the topology of the route to be taken, together with the approvals and exclusions for the use of the route infrastructure.

The generation of the timetable and the information systems, which maintain consist information, are outside the system boundary of the railway command and control system.

The data that defines each item of rolling stock is maintained in the Rolling Stock Library (RSL). The data, which comprises the RSL, is defined within reference 11. To ease the identification of rolling stock and infrastructure capability a 'Route Availability' index is used (ref. 12). The infrastructure is assigned a *Route Availability* and provided that each element of rolling stock has the same or lower Route Availability the train may pass over the route. Route Availability is based upon individual axle weight. Additional information may be required from the individual type approvals of the rolling stock, such as physical clearances (structure gauge) and traction type of the locomotive. The capability of the infrastructure is defined in the 'Sectional Appendix' (ref. 13). A further standard identifies 'Information for Safe Train Operation' (ref. 14). This document identifies a minimum set of information available to the train crew and to Railtrack.

Although this is a complex example it does represent the real world. The data errors to which this example could be subject are considered in the next section.

Static Data Description Errors

Harrison and Pierce (ref. 15) identify the following classifications of errors in the data used to describe the railway infrastructure for several layers of railway control systems.

1. omission, an infrastructure entity is not present in the control system data set;
2. spurious data, a non-existent entity is present in the data set, this may also include duplicated entities;
3. positioning errors, for example an entity is represented and addressed correctly, but its physical position is incorrect;
4. topological errors, all entities are present, but they are connected in a way which may be plausible, but incorrect;
5. addressing errors, an entity is correctly located and labelled but is connected to the wrong field devices;
6. type errors, an entity is connected and labelled correctly but is recorded with an incorrect type identifier;
7. labelling errors, an entity is located and addressed correctly, but is assigned the wrong label in the data model; and
8. value errors, a scalar attribute of some entity in the configuration data has the wrong value.

External Data Errors

The railway timetable and the train consist information system, although external to the railway command and control system, are used in the execution of the timetable. The model uses a number of references to other information systems and is reliant upon these systems to provide timely, consistent, complete, and accurate information upon demand. Additionally, train position information will be provided for train movements that are outside the control area of the command and control system, but will enter the control area in the short term.

In addition to static data description errors the external systems may provide data with the following error types:

1. existence, a data reference provided by one external information system cannot be fulfilled by another information system;
2. reference error, the wrong data reference is provided resolving information which does not represent the required train;

3. availability, an external information system is not available (off-line) at the time the information is requested;
4. inconsistent, data requested from more than one external information systems is inconsistent – which data will be used? and
5. timely, data is not supplied until after the event.

Data Representation Errors

Where multiple information systems are to be used it is almost inevitable that pre-existent systems will represent similar information in a variety of data models. These data models will have been created to fulfil the requirements of the individual information system, rather than information models in the context of all the potential uses of the information systems data. This is particularly the case for legacy systems where the original design and design intent are often not documented.

Management of Data Errors

Throughout this paper the importance of the early identification of the consequence of data errors has been stressed. The definition of a system architecture early in the system lifecycle is intended to facilitate analysis. This system architecture should identify not only hardware and software components but recognise the importance of data. In the example of a railway command and control system this configuration data may be extensive.

This configuration may be through the use of FVL, LVL, FPL and data. The development lifecycle should make clear the identification of the non-functional, as well as the functional requirements of the system and the consequence of errors, including data errors.

The development life cycle should also ensure the production of a data model that is self-consistent, clear, analysable and unambiguous. Where data is to be used from external systems, the accuracy, completeness, availability and timeliness of this should be determined and documented.

Data Maintenance and Change Control

A number of associated issues that relate to data completeness and consistency are concerned with aspects of change control and configuration management. Where maintenance is undertaken on the railway infrastructure and physical devices are either modified, upgraded or replaced, the characteristics of those changed devices should be consistently represented in the data used by a number of systems.

Measures for Structuring Data

Software tools and techniques identified in IEC 61508-3 guide the developer in the creation of software artefacts and systems. No such guidance exists for the development and management of the data model and its population.

Indeed the data model is commonly populated and maintained outside the development environment. The structure of the data model should, at least in part, be determined by the system integrity requirements. Where the system requires a high degree of integrity from the data model and its populated data set, the data model should lend itself to verification and validation.

A set of rules should be created and documented which address the task of detecting, and where appropriate correcting data errors.

Where the system places reliance upon external data sources, the consequence of failure of external data should be documented.

Data Sources

The railway command and control system uses a number of data elements, which can be generalised into the following data types or sources:

1. a static or slowly changing description of the application instance, the railway infrastructure;
2. a command schedule or set of instructions, the railway timetable;
3. a description of the current status of the system either from indication (sensors) or external information systems; and
4. a set of operational conditions based upon equipment failures or external factors such as flood.

These data sources are presented as a generic model. Small-scale systems may only incorporate a small subset of such sources, for

example a set point and actual temperature to implement a protection system. As the size and complexity of the systems under consideration grow, the consequences of data errors increase.

Discussion

The paper has discussed the role of data in a safety-related railway command and control system. It has also identified a number of distinct components of a generic system. These are:

1. a command schedule, the railway timetable;
2. a static or slowly changing description of the infrastructure for the application instance;
3. a description of the instantaneous status of the system either through sensors or external information systems; and
4. a set of operational conditions based upon equipment failures or external factors.

This paper identifies a number of data error modes for static and external data. These error modes can be used to analyse the system, the data design, and the data population processes. This can be used to determine the severity of each possible error and the necessary means to reduce the likelihood of errors to a tolerable level.

Conclusion

The safe operation of data-driven safety-related systems is likely to depend upon the correctness of its data. However, tools and techniques, which would assist in the creation of data models for such systems, are not treated in the literature, or in standards such as IEC 61508.

This paper has illustrated some of the issues related to the production and use of data, through a brief example - a railway command and control system. Through this case study this paper has identified a number of data error modes in the static description of the railway infrastructure and the command schedule (timetable).

The production of any safety-related system should include the development of a system architecture that contains not only hardware and software elements, but also components representing its data. All these elements should be analysable and should lend themselves to verification and validation.

Although a number of data error modes have been identified, further work is required to provide guidance on tools and techniques that are suitable for the production of high integrity data-driven systems.

References

1. IEC 61508-1 Functional Safety of electrical / electronic / programmable electronic safety-related systems – Part 1:1998 General Requirements. Geneva: International Electrotechnical Commission, 1998.

2. IEC 61508-4 Functional Safety of electrical / electronic / programmable electronic safety-related systems – Part 4:1998 Definitions and abbreviations. Geneva: International Electrotechnical Commission, 1998.

3. IEC 61511-1 Functional safety: Safety Instrumented Systems for the process industry sector – Committee DRAFT for Vote: 2000, Geneva: International Electrotechnical Commission, 1998.

4. IEC 61508-3 Functional Safety of electrical / electronic / programmable electronic safety-related systems – Part 3:1998 Software Requirements. Geneva: International Electrotechnical Commission, 1998.

5. IEE. SEMSPLC Guidelines – Safety Related Application Software for Programmable Logic Controllers. IEE Technical Guidelines 8:1996. Stevenage: Institution of Electrical Engineers, 1996

6. CENELEC EN50126 Railway Applications – The specification and demonstration of dependability – reliability, availability, maintainability and safety (RAMS). Comite European de Normalisation Electrotechnique, Brussels.

7. CENELEC prEN50129 Railway Applications – Safety related systems for signalling. Comite European de Normalisation Electrotechnique, Brussels December 1999.

8. CENELEC prEN50128 Railway Applications – Software for railway control and protection systems. Comite European de Normalisation Electrotechnique, Brussels May 2000.

9. D. Welbourne and N. P. Bester. Data for Software Systems important to safety. GEC Journal of Research, Vol. 12, No. 1, 1995.

10. UK Ministry of Defence, HAZOP Studies on Systems Containing Programmable Electronics, Interim Defence Standard 00-58, Issue 1, July 1994, reprinted by IEE London. See also www.dstan.mod.uk

11. Railtrack PLC. Railway Group Standard GM/RT2211: Issue Two. Mandatory Data for Rail Vehicles. London Railtrack PLC, 1996.

12. British Railways Board. Group Standard GC/TT0138 Issue. A, Rev. 1: Route Availability System. British Railways Board 1993.

13. Railtrack PLC. Railway Group Standard GO/RT3206 Issue. One: Format and Content of the Sectional Appendix: London. Railtrack PLC, 1995.

14. Railtrack PLC. Railway Group Standard GO/RT3436 Issue One: Information for safe Train Operation. London. Railtrack PLC 1998

15. A. Harrison and R. H. Pierce. Data Management Safety Requirements Derivation. Railtrack: West Coast Route Modernisation Internal report. June 2000. Railtrack PLC, 2000.

Biography

Alastair Faulkner, MSc., MBCS, C.Eng; CSE International Ltd., Glanford House, Bellwin Drive, Flixborough DN15 8SN, UK. Telephone +44 1724 862169, facsimile +44 1724 846256 email - agf@cse-euro.com

Alastair Faulkner holds an MSc degree in Computer Science from Salford University and is a Chartered Engineer. His background is in software development mainly concerned with computer based command and control systems.
Alastair works for CSE International Ltd. as a Senior Engineer and is currently engaged on a large UK Rail command and control project. Alastair's research interests are in the data management of data-driven safety-related systems. He is also a Research Engineer with the University of Warwick and is studying for an Engineering Doctorate.

N. Storey, B.Sc., Ph.D., FBCS, MIEE, C.Eng. School of Engineering, University of Warwick, Coventry, CV4 7AL, UK. Telephone - +44 24 7652 3247, facsimile - +44 24 7641 8922, email - N.Storey@warwick.ac.uk.

Neil Storey is a Director within the School of Engineering of the University of Warwick. His primary research interests are in the area of safety-critical computer systems. He is a member of the BCS Taskforce on Safety-Critical Systems and has a large number of publications including both journal and conference papers. Neil is also the author of several textbooks in the areas of electronics and safety, including "Safety Critical Computer Systems" published by Addison-Wesley.

Paper Release Form
19th International System Safety Conference

Title of Paper: The Role of Data in Safety-Related Railway Control Systems

I hereby authorize the System Safety Society to publish the paper listed above in the Proceedings of the 18th International System Safety Conference. Further, I agree to the following policy and notice regarding copyrights.

It is the policy of the System Safety Society, the sponsor of the International System Safety Conference, not to copyright the proceedings in order to provide the widest access for academic and educational use. Authors are free to copyright their papers as long as they agree with this policy. The policy to be contained in the proceedings is as follows:

Permission to print or copy: The copyright of all materials and commentaries published in these proceedings rests with the authors. Reprinting or copying for academic or educational use is encouraged and no fees are required; however, such permission is contingent upon giving full and appropriate credit to the author and the source of publication.

Author: Neil Storey

Address: School of Engineering
University of Warwick
Coventry
CV4 7AL
UK

Work Phone: +44 24 7652 3247
Home Phone: +44 24 7641 5517
FAX: +44 24 7641 8922
E-Mail: N.Storey@warwick.ac.uk

Signature Date

Author: Alastair Faulkner

Address: CSE International Ltd
Glanford House
Bellwin Drive
Flixborough
DN15 8SN
UK

Work Phone: +44 1724 862169
Home Phone: +44 161 338 2682
FAX: +44 1724 846256
E-Mail: agf@cse-euro.com

Signature Date

Mail to: John Livingston
Boeing Reusable Space Systems
555 Discovery Drive
Mail Code ZA-12
Huntsville, AL 35806-2809
(256) 971-3005, fax (256) 971-2699
john.m.livingston@boeing.com