Electronic Data Interchange System for Safety Case Management

Alan Eardley[1], Oleksiy Shelest[2] and Saeed Fararooy[2]

[1] Staffordshire University, Beaconside, Stafford, ST16 3YL, UK.

[2] rcm2 limited, Cheltonian House, Portsmouth Road, Esher, Surrey, KT10 9AA, UK.

Abstract. In this paper the theory of Electronic Data Interchange (EDI) is applied to the safety case management domain in order to evaluate its benefits and to assess the potential issues which relate to data exchange within certain industry sectors. The work is undertaken to establish best practise and to examine successful techniques identified by other researches in the area of XML/EDI and to implement them in data transmission from a safety case management tool based on MS Visio to the Integrated Safety Case Development Environment (ISCaDE) residing on a Dynamic Object Oriented Requirements System (DOORS) database. Goal Structuring Notation (GSN) and its XML dialect Goal Structuring Mark-up Language (GSML) developed at the University of York is used as messaging specifications to represent the safety case model. Furthermore, these specifications are used to build EDI software to transport data across different safety packages.

1 Introduction

The growing popularity of the visual representation of evidence and arguments to promote safety has led to the development of a range of graphical safety case models, including

descriptions of the basic elements and relationships in the Goal Structuring Notation (GSN). The GSN model has been accepted in the safety management field and has been implemented in a number of computer-based tools (e.g. Wilson *et al* 1995*)*. Continuous development work on the model (Kelly 2003) has enabled the first XML representation of the safety case information Goal Structure Mark-up Language (GSML).

The aim of this paper is to identify the problems associated with the data interchange process in safety case management, to develop and evaluate a proposed solution, to demonstrate any advantage and to examine some potential issues. An XML data definition for a specific safety case model (GSN) is used to prove data interoperability between two software environments; Microsoft Visio and Telelogic DOORS.

Kelly (2003) recognizes the relative importance of re-using safety case data and therefore data interchange in safety case management. Safety cases for complete

Eardley A., Shelest O. and Fararooy S. (2006).
Electronic Data Interchange System for Safety Case Management.
In *Proceedings of the 3rd International Workshop on Computer Supported Activity Coordination*, pages 116-122
DOI: 10.5220/0002446901160122

systems are often decomposed into subsystems to manage the complexity of the models concerned. With this approach it is evident that well-structured safety cases can be used as templates for future safety arguments in certain application areas. This feature allows engineers to re-use the repetitive parts of safety arguments. (Kelly 2003).

A number of issues arise in safety case decomposition and potential problems with separating re-usable patterns and transferring data to other safety cases. It is vital to consider the interactions between subsystem safety cases, as a disproportionate amount of effort is devoted to the development of safety cases at a high or 'overall' level. Thus, problems may arise due to duplication of effort when carrying out safety tasks and to safety objectives 'falling through the cracks' when apportioning safety responsibilities. (Kelly 2003).

Industry based standards often realise the importance of carrying out safety case decomposition and understanding the relationship between subsystems. The current European Railway Standard (CENELEC 1998) describes three relevant types of safety case:

1 **A generic product safety case**

that provides evidence that a generic product is safe in a variety of applications;

2 **A generic application safety case** that provides evidence that a generic product is safe in a specific class of application;

3 **A specific application safety case** that is relevant to one specific safety application only.

The above categorization clearly reflects the need for the successful interchange of safety case data, which is the theme of this paper.

2 The XML/EDI Approach

With the importance of the exchange of safety case data being established, there is the opportunity to build a suitable EDI system to facilitate the exchange. The latest research in the area suggests the use of XML to take advantage of a new generation of protocols based on the Hypertext Transfer Protocol (HTTP). Such protocols offer flexibility and improvement to the use of existing 'legacy' EDI systems, exchanging the data in HTTP format via the medium of the Internet, using XML agents (Morrison 2000).

Research by the OASIS group, the UN/EDIFACT initiative, XML/EDI research group, and CEN Workshop have established that the core elements in building suitable EDI systems are; a global repository, a business processing logic unit and messaging specifications (Schmelzer 2002).

The global repository and business processing logic unit are outside the scope of this paper, but will be discussed briefly in the next section of the paper, which then focuses on the messaging specification element.

3 Technical Implementation

The global repository is briefly discussed with some suggestions made about its technical implementation. The importance of the business processing logic unit is also mentioned in this paper. A list of functional requirements for this subsystem was derived from Tim Kelly research papers and it was suggested to implement the unit in a form of intelligent agents.

Message syntax is discussed in perspective of XML mapping.

3.1 Global Repository

In practice, global repositories can be databases containing meta-information. A dedicated repository can contain lists of XML files and their corresponding descriptions. They can be stored on the Internet or implemented as a web service accessed through thin and thick clients. In this context Universal Description, Discovery and Integration (UDDI) technology has potential for improved safety case data interchange.

Repository maintenance should have a standard organization and processes, although individual businesses may want to use local copies of a repository to manage their mission-critical functions (CWA 13993:2000, 2000). In relation to safety management systems, a repository can be a place to find information about safety case modelling techniques including Goal Structuring Notation (GSN), Claim Weighted Factor Analysis (WeFA) and Argument Notation (ASCAD) by Adalard. Goal Structuring Mark-up Language (GSML) is a representation of GSN safety case modelling that can use XML dialog data to form XML objects in the proposed system. The system may contain GSML templates and industry best practices such as successful safety case arguments represented in GSN.

3.2 Business Logic

The business logic unit should aid the system decomposition process, offer advice on identifying the subsystem interdependencies and ensure that the system boundaries are drawn correctly with no unwanted ‘gaps’. Business processes can also be modelled with various tools (e.g. BP Win and Oracle Process Modeller) and are applicable to a broad range of services and a common approach is to implement business logic with the aid of intelligent agents. Such agents can interpret the existing templates to perform the work needed, interact with the transaction and the user to create new templates for each new specific task, or identify and obtain alternative templates for existing jobs. Overall, the business logic should as a minimum take care of links to system requirements, should ensure there are no unwanted interdependencies, that there are subsystems and that the boundaries between subsystems are drawn correctly.

3.3 Messaging Architecture

The proposed architecture allows the importation of GSML files into ISCaDE by MS Visio using GSN with added-on VBA scripts through a DOORS database using the DOORS Extension Language (DXL). Visio GSN creates a GSML document and passes it to the ISCaDE GSML ActiveX control. The ActiveX component inherits the MSXML interfaces and uses them to check if this document is well-formatted and is a valid XML file. A number of internal operations are performed to map the XML DOM tree to the GSN model and to derive the resulting GSN objects, attributes and their relationships. Any GSN-specific information is then passed to the DOORS database DXL Type library, which communicates directly with the DXL script through a Windows Component Object Model (COM) interface. The DXL script stores the data in a DOORS database and creates the relevant modules.

Third party software providers can create industry specific XML subsets and parse them with ISCaDE GSML objects by querying the ActiveX components for the supported interfaces. They can incorporate ISCaDE GSML into any software package that supports the Windows COM architecture or use DXL API to retrieve data from components and store it in a DOORS database, as in Figure 1

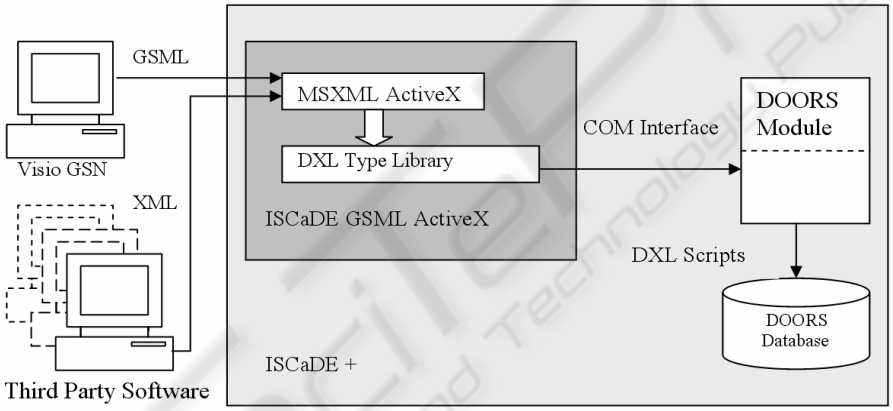

Fig. 1. ISCaDE GSML System Architecture.

4 Case Study

Figure 2 shows an example of a safety case model depicted in MS Visio software. The safety goal is to prove that fail-safe design will ensure at least 90% of potential failures that are due to systematic faults are fail-safe. This can be achieved by breaking the safety case down into sub goals, making relevant assumptions. If sub goals are proved subsequently the main goal has been proved. Three sub goals are used:

- Flaws in ADC, application software, configuration trip limits and trip logic will be revealed by dynamic on-line tests;
- Compiler, loader and processor flaws are protected against by the reversible computing technique;

- Double thermocouple disconnection or veto will cause a trip.

These are used in conjunction with three respective assumptions:

- A14 On-line tests detect 90% of systematic failures;
- A15 Tests indicate a 99.995% fail-safe bias;
- A13 Thermocouples fail low in 90% of cases.

From Figure 2 it can be demonstrated that within the context of the safety problem and given assumptions about the system, the main goal is proved

Although MS Visio software is effective as a drawing tool it does not depict the evolution of the safety case within the timeframe, nor does it indicate the resources used or the changes made to the safety system. However, if the XML structure can be applied to a safety case, GSML can be used to represent it, as follows:

```
<goal xlink:type="resource" xlink:label="G.PFD.SYST.2__goal">
  <name>G.PFD.SYST.2</name>
  <summary>Fail-safe design will ensure
    that at least 90% of failures due to
    systematic faults are fail-safe
  </summary>
</goal>
```

This is how a goal object will look within this frame:

```
<solved_by xlink:type="arc" xlink:from="G.PFD.SYST.2__goal"
     xlink:to="G.CHECKS__goal" />
```

This object represents the link:

```
<assumption xlink:type="resource"  xlink:label="A1. __assumption">
  <name>A1.</name>
  <summary>A15 Tests indicate a
   99.995% fail-safe bias
  </summary>
</assumption>
```

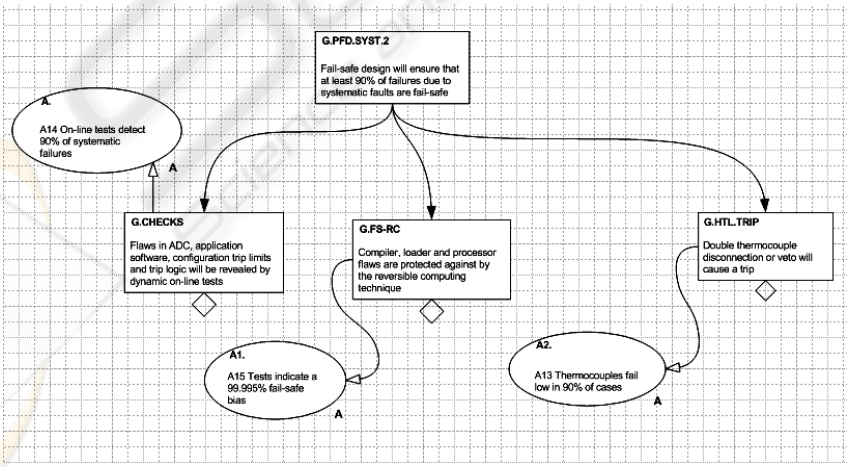

Fig. 2. GSN model in Visio.

New GSN Safety Case Model	Object Type	Context Type	Assumption
1 G.PFD.SYST.2 Fail-safe design will ensure that at least 90% of failures due to systematic faults are fail-safe	Goal		
1.1 G.HTL.TRIP Double thermocouple disconnection or veto will cause a trip	Goal	Assumption	A2. A13 Thermocouples fail low in 90% of cases
1.2 G.FS-RC Compiler, loader and processor flaws are protected against by the reversible computing technique	Goal	Assumption	A1. A15 Tests indicate a 99.995% fail-safe bias
1.3 G.CHECKS Flaws in ADC, application software, configuration trip limits and trip logic will be revealed by dynamic on-line tests	Goal	Assumption	A. A14 On-line tests detect 90% of systematic failures

Fig. 3. GSN model in DOORS.

After XML code has been generated, the tool that was described above can transport the data into the DOORS database. DOORS is a document-based database that allows its users to trace its objects and view their history or 'lifecycle'. In other words if Visio is a graphic approach to safety system specification, then DOORS is a data-centred approach.

Figure 4 shows how the data was interpreted by ISCaDE that resides on top of DOORS. As can be seen the communication was complete and effective - no data was lost or was misinterpreted.

Therefore, by applying this technique companies can benefit from both environments. Should they require ease of use they can develop their models in MS Visio or should they be more concerned about traceability features, they can migrate the same data to ISCaDE or they can use both tools where issues of time or effort are over-ruled by the demands of safety.

The features of both tools are compared in Figure 5.

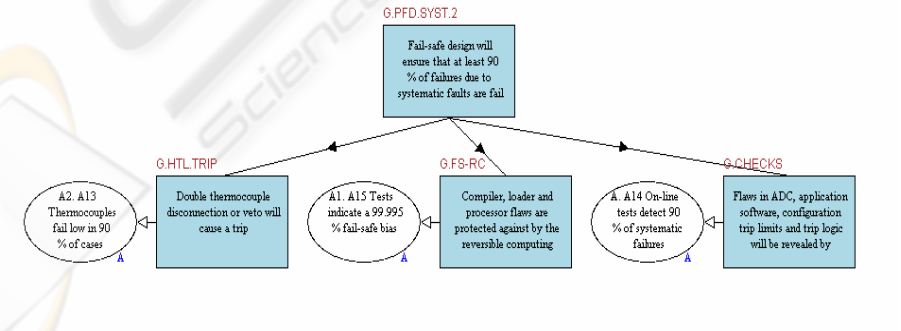

Fig. 4. GSN model in ISCaDE.

Benefits	MS Visio	ISCaDE/DOORS
Ease of graphical use	Yes	No
Enhanced report facilities	Yes	No
Traceability	No	Yes
History of events	No	Yes

Fig. 5. A Comparison of the Features of MS Visio and ISCaDE/Doors.

5 Conclusions

The research highlights the importance of data interchange within the safety-critical industry and provides sufficient proof of concept to demonstrate that data transfer can be carried out effectively between existing safety development environments, using existing EDI systems having the minimum set of components, namely a global repository, a business logic processing unit and supporting messaging specifications.

The research concentrates on the message processing and building a XML specific data channel for efficient EDI. GSML is used as a starting point, as its principles can be expanded to cover all aspects of the safety management industry. These standards can include ASCAD, the WeFA model, hazard logs and risk analysis matrices. To ensure future standardisation, it is possible that a regulation body will have to be set up to validate and authorise proposals for XML representations within EDI structures in relation to safety cases.

Future work may involve the formation of an independent initiative group across the industry to research and propose a set of XML-based safety case standards. This will provide the safety management industry with scientific knowledge that can be used to develop XML/EDI safety systems.

If approved by the British Standards Committee or ISO (International Organisation for Standards), these could become industry standards.

References

1. CENELEC (1998) ENV 50129 Railway applications – Safety related electronic systems for signalling, European Committee for Electrotechnical Standardisation.
2. CWA 13992:2000 (2000) Recommendations for standardisation in the fields of XML for electronic data interchange, British Standards
3. CWA 13993:2000. (2000) Recommendations and guidance on the use of XML for electronic data interchange, British Standards.
4. Kelly, T. P. (2003) Managing Complex Safety Cases, Proceedings of the Eleventh Safety-critical Systems Symposium, Bristol, UK. Springer Verlag.
5. Morrison, M. (2000) XML Unleashed, Sams Publishing
6. Schmelzer, R. (2002) XML and Web Services Unleashed, Sams Publishing Ltd.
7. Wilson, S.P., Kelly T.P. and McDermid, J.A. (1995) Proceedings of the 12th Annual CSR Workshop, York University.