Assurance of open systems dependability: developing a framework for automotive security and safety

Robin Bloomfield[1,2], Eoin Butler[2], Kate Netkachova[1,2]

[1]Centre for Software Reliability, City University of London

[2]Adelard LLP
London, UK
{kn,eb,reb}@adelard.com

***Abstract*—We describe how a security informed analysis of the open systems dependability model of DEOS can be used to frame the problem of open systems and security. Together with an approach for analysing industry objectives based on claims, arguments and evidence (CAE), we develop a set of principles and rationale for the security and safety of road transport systems. The associated CAE will provide a generic template for a security informed safety case and supports standardization activities for security-informed safety.**

Keywords—security-informed safety; automotive systems; DEOS; assurance cases

I. INTRODUCTION

In this paper and associated talk, we describe how the open systems dependability model of DEOS can be used to frame the problem of open systems and security. Together with a framework for analysing decision based on claims, arguments and evidence (CAE), we are developing principles for security and safety for an automotive standard.

II. FRAMING THE PROBLEM

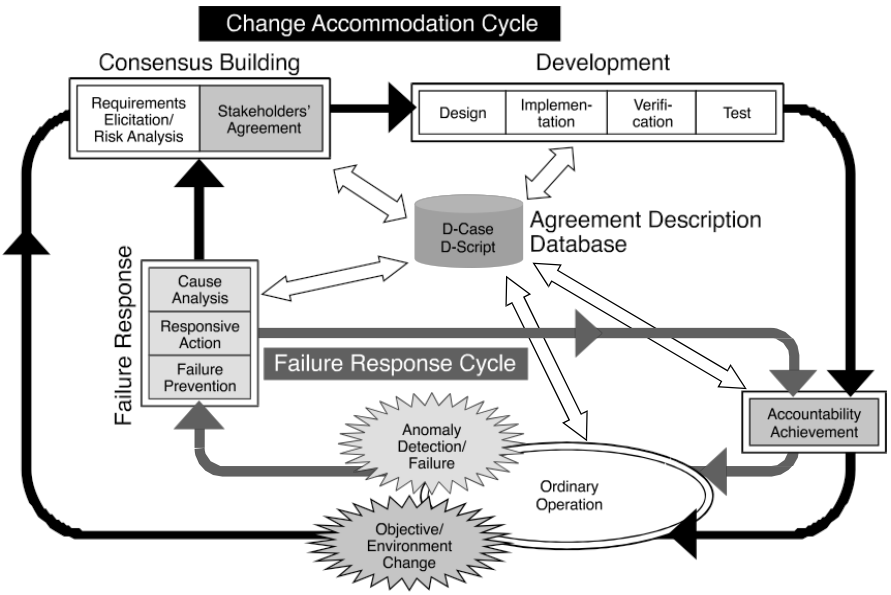
Open systems dependability is the ability to accommodate changes in purpose, objectives, environment and actual performance and to achieve accountability continually, so as to provide expected services as and when required.

The DEOS process provides a reference model for an open system. It consists of two cycles:

- Change Accommodation Cycle to adapt system according to requirement changes;
- Failure Response Cycle to provide failure prevention, failure response and analyse the causes of failures.

We use a CAE framework for analysing engineering decision, particularly those concerned with dependability but also wider issues such as regulatory strategy [1]. We can assess the role for the different parts of the DEOS process (see Fig.2) [9] by examining their contribution to different claims and arguments and evidence for a generic dependability claim. Fig. 2 shows how the CAE framework can be mapped to the DEOS process (and vice versa).

A preliminary analysis will show that there will be two major changes from a security perspective. The adaptation process needs to consider non-benign events (see Fig. 3) and attacks on the change infrastructure. The change infrastructure will also need to be adapted in the fact of threats and other changes so the diagram and DEOS approach [9] will be deepened as it is applied recursively. In addition the requirements on the confidentiality of information need to be captured in an appropriate policy. The overall impact of security can be assessed by applying security informed Hazops, STRIDE or STPA to the DEOS process.



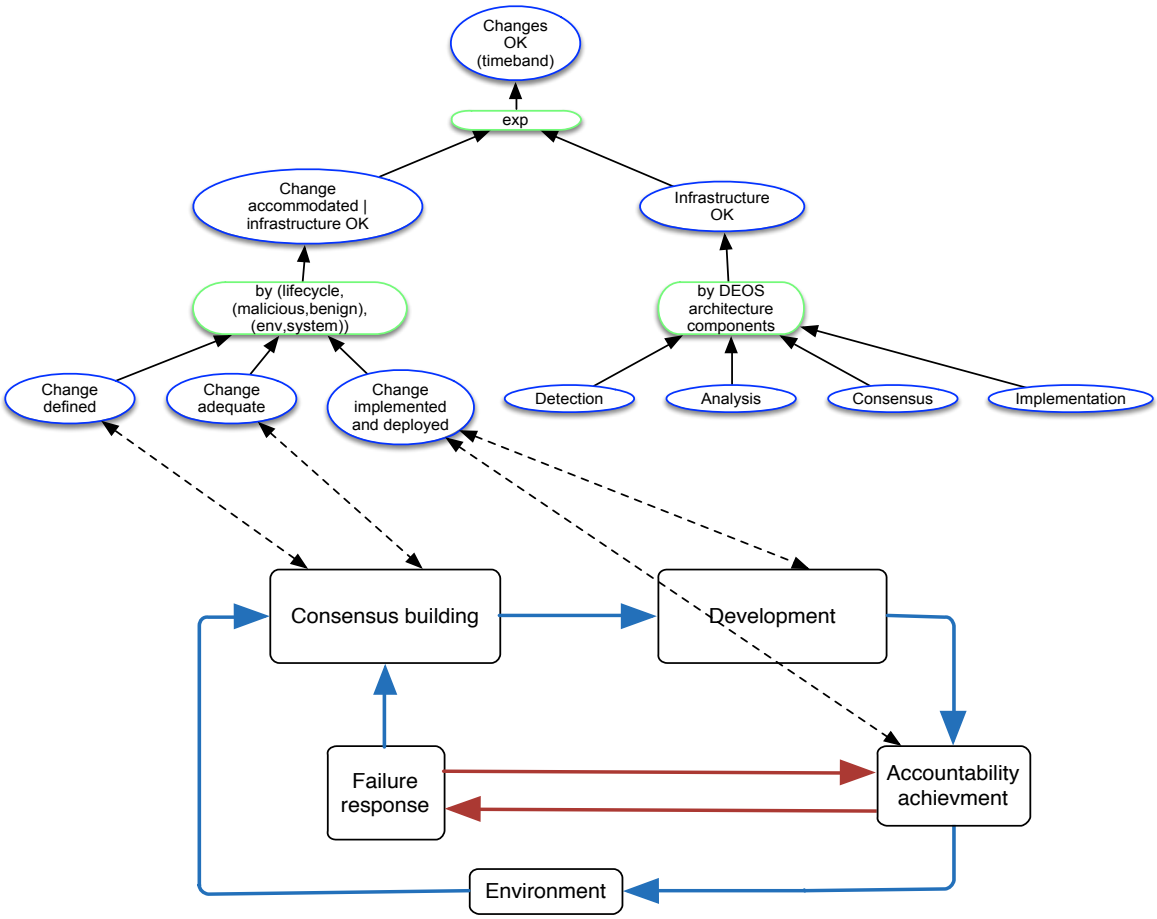


Fig. 2. Example of mapping claims to the DEOS process

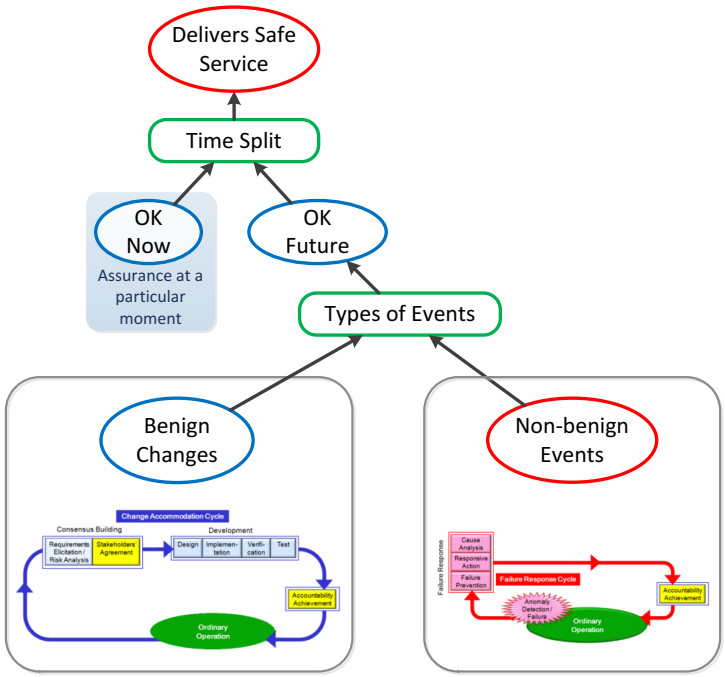


Fig. 3. Process needs to consider non-benign events

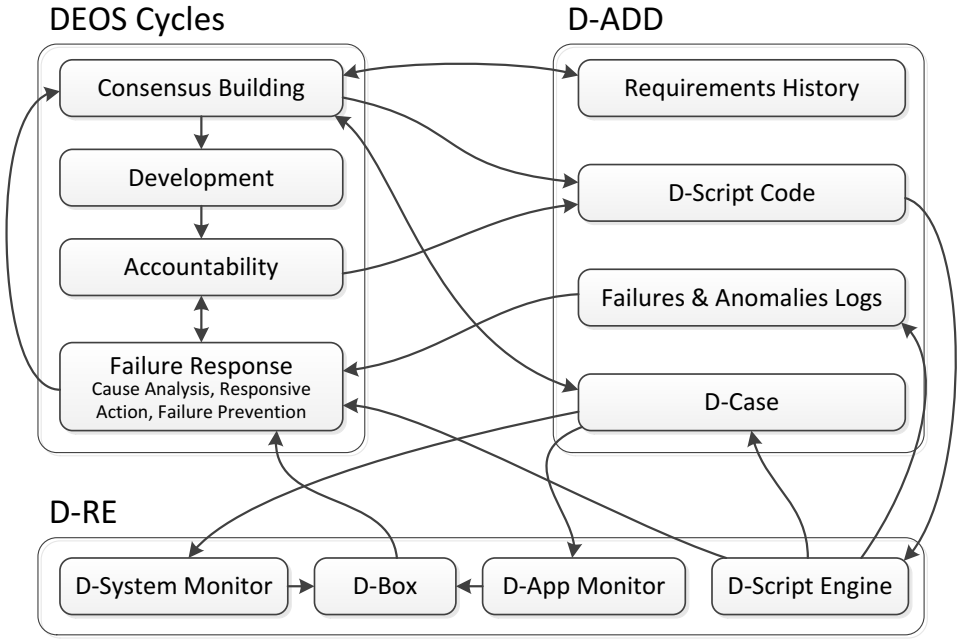


Fig. 4. Detailed data flow diagram in the DEOS framework

To do this we need to create more detailed models of the dataflow within the reference DEOS architecture. This is shown in Fig. 4.

In the traditional DEOS model the relationships on this diagram are trusted, so we can apply the standard security approach to analysing each of them. For example, we can use Microsoft's STRIDE with six main threat categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. An example is shown in Table 1.

TABLE I. ANALYSIS OF DATA FLOW FROM THE CONSENSUS BUILDING TO THE DEVELOPMENT BLOCK

STRIDE keyword	**Analysis of Data flow from the Consensus Building to the Development block**
Spoofing	Someone acting like a stakeholder (but not actually a stakeholder) sends a set of new requirements to the development.
Tempering	Requirements are modified during while being transferred to the development.
(Non-) repudiation	Developers claim to have not received any requirements for implementation.
Information disclosure	Leakage of requirements to a third party during the transfer process. This can be important as requirements can be confidential (e.g. encrypt all data with this type of key).
Denial of service	Requirements cannot be delivered because of the flooded channel.
Elevation of privilege	Someone gets access to a stakeholder's account and sends requirements to the developers.

This analysis will lead to more detailed recommendation for the implementation of the DEOS process and architecture.

III. DEVELOPING PRINCIPLES

Having used the open systems perspective to frame the problem we can relate these to the principles and guidance for use in standardisation. We can identify principles using a top down approach based on a vision for the industry that we systematically analyses in our CAE framework to derive objectives (see for example the work in [1] applying this to aviation regulation). We can use the DEOS perspective to check our approach for scope. We also undertake a more bottom up analysis by comparing and contrasting the principles from existing guidance on security, risk assessment, assurance and automotive applications.

We have developed claims-evidence-argument approaches to reason and communicate about the trustworthiness of systems. In previous projects we have used them to support the development of policy and to assess the impact of security issues on safety regulation [1] To develop and justify the principles for the Guidance, we are constructing a claims-evidence-argument case showing how the principles support a high-level vision for the industry.

In this Section we provide an overview and some details of the evolving approach.

We start with a proposed high level vision: "We see a world where everyone has confidence in a safe and secure road transport sector". From this, we focus on the cyber-security related issues: "We see a world where there is justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of road transport..."

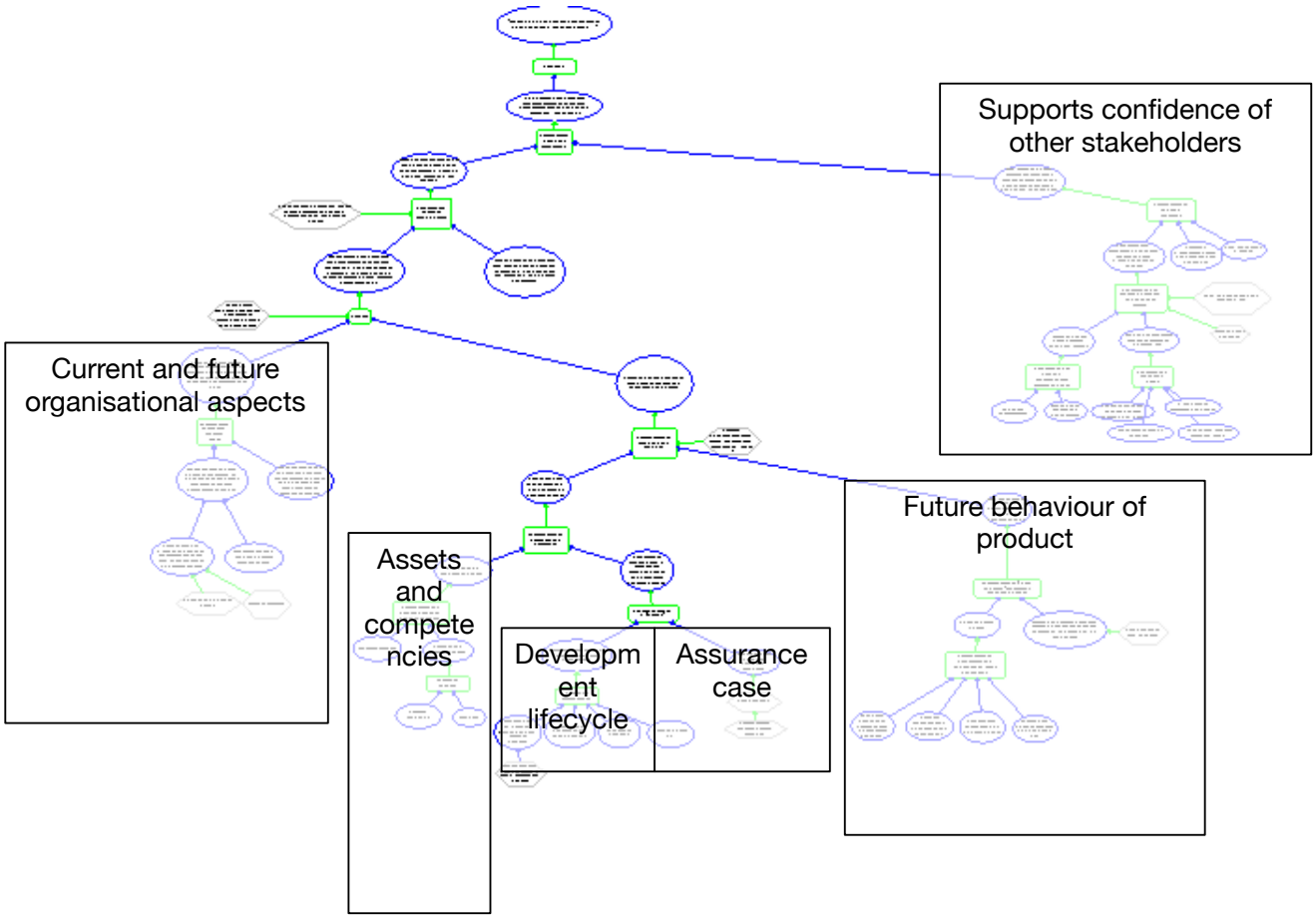


Fig. 5. CAE structure

The complete CAE structure we are developing can be seen in Fig. 5 where we have identified the main areas of the principles. We will expand and develop further on this structure as the project develops.

Review and Mapping of Other Principles

There is considerable work done on developing security principles. We have reviewed the following principles for security:

- DfT/CCAV: The Key Principles of Cyber Security for Connected and Automated Vehicles [2]
- NCSC: NIS Directive Guidance [3]
- ONR: Security Assessment Principles [4]
- NHTSA: Cybersecurity for Modern Vehicles [5]
- Rail Industry Cyber Security Assurance Group: Cyber Security Assurance Principles [6]

We have also documented the ENISA Good practices [7] and the draft IET "Safe and Secure" principles [8] as further useful sources of information.

We have used the ASCE tool to map these principles and to show their interrelationships as shown in Fig. 6. This initial analysis identifies three broad categories of principles that all these documents address to a differing extent:

1. Organisational security
2. Product or project lifecycle
3. Design principles (covering architecture through to component design)

A detailed comparison of the principles is in progress. In addition we use of own experience of assessing the safety and security of systems, as well as consultation with industry and government, to develop a list of cross cutting themes for which we provide more detailed guidance tied into the different principles. We currently envision topics such as the following:

- Lifecycle processes
- Risk assessment and hazard analysis
- Composition of assurance cases

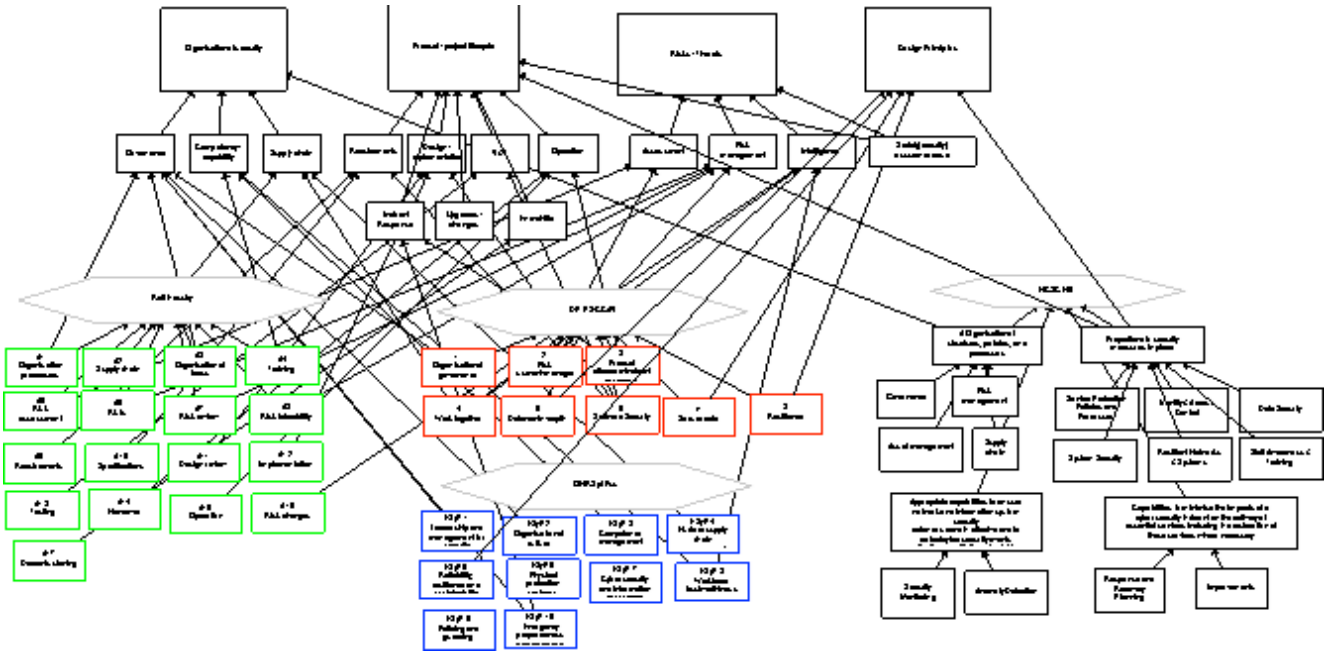


Fig. 6. Overview of mapping of principles

CONCLUSIONS AND NEXT STEPS

We have described how a security informed analysis of the open systems dependability model of DEOS can be used to frame the problem of open systems and security. Together with an approach for analysing objectives based on claims, arguments and evidence, we are developing a set of principles and rationale for the security and safety of road transport systems. The associated CAE will provide a generic template for a security informed safety case. This is currently work in progress but the intention is to publish in late 2018 the output of this work to support a new standard for the industry.

REFERENCES

[1] Bloomfield, Robin and Bishop, Peter and Butler, Eoin and Netkachova, Kate, Using an Assurance Case Framework to Develop Security Strategy and Policies, Publisher, in Computer Safety, Reliability, and Security, SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, Springer International Publishing, 2017, 10.1007/978-3-319-66284-8-3

[2] HM Government, The Key Principles of Cyber Security for Connected and Automated Vehicles, August 2017.

[3] National Cyber Security Centre, Networks and Information Systems (NIS) Directive: Security objectives and principles. Retrieved 28 September 2017 from https://www.ncsc.gov.uk/information/networks-and-information-systems-nis-directive-security-objectives-and-principles.

[4] Office for Nuclear Regulation, Security Assessment Principles for the Civil Nuclear Industry, v1.0, 2017.

[5] National Highway Traffic Safety Administration, Cybersecurity best practices for modern vehicles. Report No. DOT HS 812 333, October 2016.

[6] Rail Industry Cyber Security Assurance Group, Cyber Security Assurance Principles, Issue 7, November 2016.

[7] ENISA, Cyber security and resilience of smart cars - good practices and recommendations, December 2016.

[8] IET Safe and Secure Code of Practice Principles, version 0.6 (draft).

[9] Mario Tokoro, Open Systems Dependability, ISBN 978-1-4665-7751-0, CRC press 2013