Deviational analyses for validating regulations on real systems

Fiona Polack, Thitima Srivatanakul*, Tim Kelly, and John Clark

Department of Computer Science, University of York, YO10 5DD, UK.
*Department of Civil Aviation, Ministry of Transport, Bangkok 10120, Thailand

Abstract. Deviational analysis is a traditional way of exploring the safety of systems. The results of deviational analysis contribute to traditional safety cases and safety arguments. We extend deviational analysis to other aspects of dependability, notably security. We discuss how the evidence of deviational analysis can contribute to the validation of regulations, in the sense of their application of regulations to real systems.

Keyword: deviational analysis, dependability, regulation validation

1 Background

Regulations are intended to control the way that choice operates in critical systems. Validation must include consideration of how well their intent is met by real systems operating within the regulations. We describe the systematic analysis of security, illustrating it with results from a case study of the security of baggage handling in an international airport [11]. The case study was carried out in situ, with the co-operation of the relevant airport staff.

International airline regulations [9] have a goal *to prevent the introduction of explosives or other dangerous devices on to aircraft by way of checked baggage.* This is elaborated [8] to,

1. all baggage is subject to security controls prior to boarding the aircraft;
2. all baggage is protected from interference or the introduction of unauthorised items after acceptance at the check-in counter;
3. baggage for passengers who are not on board the aircraft must not be transported on to the aircraft.

The first two aspects are addressed here. The case study reveals a range of situations where the regulations are in force but their intent was not met.

1.1 Deviational analysis and argumentation

The most mature area of dependability assurance is safety; national and international procedures require operators of aircraft, manufacturing plants and other critical systems to provide evidence of acceptably-safe operation.

In safety, traditional checklist approaches capture experience of development or operation. More powerful approaches use flaw hypothesis to explore the potential for accidents. For example, HAZOP [7] is a systematic, deviational approach applied to models, that encourages imaginative analysis of potential for failure by applying guidewords to concepts and components.

Deviational techniques provide evidence for arguments made to demonstrate to external assessors that a system meets necessary dependability targets. Again, argumentation is most advanced in safety work. In general, we can identify the required dependability attributes for particular types of system, and build policy and regulations based on argumentation of these attributes (see [2]).

Safety cases are typically visualised using the *Goal Structuring Notation (GSN)*. This expresses the structure of an argument in terms of the goals, argument strategies (eg. for decomposing goals), context, assumptions and solutions (where evidence establishes the validity of the stated goal) [5]. The GSN approach has been extended to dependability and policy derivation (see [4]).

1.2 Argumentation and regulations

Our work looks at how well a real system establishes the intention of the regulations under which it operates (we do not directly analyse the regulations). We apply two deviational approaches to models of the baggage handling system. The deviations aim to elicit ways in which baggage security could be compromised, despite the system's established conformance to international regulations.

Our deviational approaches, developed to analyse models for potential security vulnerabilities, apply HAZOP to use cases [13, 14] and security zones [12]. In [11], these approaches provide evidence to a GSN argument that the system is acceptably secure. The goal is to meet the security intent of the regulations. Here, we reflect on security analysis and argument as a means to explore how well the compliant baggage handling system establishes the intent of the regulations.

2 Abuse cases: HAZOP on use cases

Use cases are used to model high-level functional requirements. We propose [11, 13] abuse cases to systematically challenge the meaning of every model element: the use case, its actors and associations. HAZOP is applied to the use case's process steps and their pre- and post-conditions. For actors, HAZOP is applied to their intentions and capabilities, as derived from intended goals.

The technique was devised for use in the early stages of development, to identify and incorporate security-related requirements and development constraints. It is similar to, but more systematic than, other abuse or misuse case techniques used to highlight system vulnerabilities [6, 10], and to work using HAZOP to extract non-functional requirements [1, 3]. In adapting HAZOP for model analysis, each HAZOP guideword must be assigned a clear interpretation for each type of model element. For example, Table 1 gives the HAZOP guideword interpretations for *actor*.

Feature	Guideword	Meaning
Actor Intent	NO	The intent (action) does not take place
	MORE	More than the intent is achieved, eg. sequential or parallel repetition *or* some scalar parameter is too large
	LESS	Actions were incomplete or insufficient
	AS WELL AS	some supplementary or contradictory action occurred as well as that intended
	OTHER THAN	The action achieves incorrect results *or* the actor uses the action for purposes outside the intended
Actor Capability	NO	The actor does not have the ability to perform the action
	MORE, AS WELL AS	More general capability, allowing more than intended action to be performed
	LESS, PART OF	Less capability, or only part of the required abilities, so less is achieved than intended

Table 1. Generic HAZOP guidewords interpreted for use case actor [11]

The baggage handling system has been in operation for many years, so its functional "requirements" are well understood. As expected, abuse cases reveal no new information about functional aspects. However, the analysis reveals various security threats and several implicit security requirements. It also highlights the importance of appropriate inputs and/or information within the system: many of the vulnerabilities relate to incorrect use of baggage tags, or to the possibility of baggage being swapped or tampered with during the check-in process. The HAZOP analysis focuses on areas of vulnerability in the system that might compromise its ability to achieve the intention of the baggage regulations.

In comparison to other security analysis techniques, abuse cases prompt a detailed discussion of how an attack might exploit a vulnerability, and possible effects of exploitation are thoroughly investigated. Airport security managers found the technique beneficial in its ability to identify vulnerabilities in operational tasks and in features of the computer systems related to baggage handling. Importantly, these issues are newly identified, despite the long period of use, under well-managed regulatory procedures.

3 Zonal analysis with HAZOP

Regulations typically assume zoning. For example, transport networks have zones where vehicles can legally travel (roads, rails, air corridors) and park (parts of airports, some road verges). Regulations intend to manage action in and between zones, whilst risk analysis also considers interaction of networks: where roads cross railways, or road vehicles circulate in airports. The importance of zones in security is the ability to identify any means of illicitly crossing the boundary between zones.

In [12], HAZOP challenges the potential channels, and the use of channels, between zones. For the baggage handling system [11], there are three zones: the baggage sorting and make-up area (zone 1), the check-in desk (zone 2) and all

adjacent areas (zone 3). Airport staff identified known channels in relation to these zones. Compliance with the baggage-security regulations implies that these channels are only used in intended ways by authorised agents. Srivatanakul's systematic zonal HAZOP identified over 50 potential vulnerabilities, such as unintended channels to zones 1 an 2, and unintended consequences of intended channels. Thus, zones 1 and 2 were shown to be secure, but checked-in baggage might be compromised by illicit use of a legal entry point in to zone 2.

In most cases, the vulnerabilities are protected by existing controls. However, a few had the potential to cause serious breaches of regulation, prompting re-consideration of how the regulations are interpreted, or application of enhanced access control. Again, the airport security management found the technique an effective audit of security measures.

The HAZOP analyses contribute evidence to a GSN security argument. In [11], sample patterns of analysis are presented to assist the argument of that the security intent of the regulations is met. For example, a security goal formulated as *Access to Zone 1 is restricted to authorised persons* might be decomposed under a strategy, *argument over authorised and unauthorised people*. However, a HAZOP result is that authorised people can legally access a zone and and cause harm. The primary goal must be re-written as, *Access to Zone 1 is restricted to authorised persons for identified purposes*. The analysis proceeds to consider potential violations of security by authorised persons with *unidentified* purposes. At the lowest level, evidence that a security goal is met is by appeal to the fine-grained HAZOP analysis of the zones and channels.

4 Conclusions

In relation to validation of regulations, [11] notes that the vulnerabilities found by the two techniques arise, despite existing security controls and operational tasks that are compliant with the regulations in [8]. It is well-known that security cannot only be considered in general; regulations must be (re)validated in the specific context and domain. Security vulnerabilities arise because it is too easy to comply with the regulations without achieving their intent.

In terms of the validation of regulations, our HAZOP analyses do not look at the regulations themselves, but at the ability of a system to uphold the intent of the regulation. HAZOP analysis is a widely-accepted systematic approach, applied to models of systems to detect and evaluate potential failures or vulnerabilities. Here, HAZOP generates significant insight in to potential security threats that would cause the system to violate the security intentions of the international baggage regulations.

Abuse cases identify vulnerabilities in the interactions of people and processes, whilst zonal HAZOP seeks side channels by which secure zones can be attacked. Both are used here to explore how the intent of the regulations is borne out in the actual system.

Although the zonal HAZOP case study concentrates on physical zones, HAZOP can also be applied to logical zones [12]. An important sort of logical zone,

in relation to regulation, is areas of responsibility; the analogy of illicitly crossing a boundary between zones is gaps or overlaps in the responsibilities of people or systems that contribute to compliance with the regulations.

The deviational analyses provide a valuable security audit of the existing system, and prompt consideration of the need for specific guidance on how to achieve the intent of the regulations in specific situations. If similar analyses were to be applied to systems for which new regulations were being prepared, possible omissions or errors could be detected and corrected in the draft regulations.

References

1. K. Allenby and T. P. Kelly. Deriving safety requirements using scenarios. In *5th IEEE International Symposium on Requirements Engineering (RE'01)*. IEEE Computer Society Press, 2001.
2. G. Despotou and T. Kelly. Extending the safety case concept to address dependability. In *22nd International System Safety Conference*. System Safety Society, August 2004.
3. B. P. Douglass. *Real-time UML (2nd ed.): Developing efficient objects for embedded systems*. Addison-Wesley Longman Ltd., 2000.
4. M. Hall-May and T. Kelly. Planes, trains and automobiles - an investigation into safety policy for systems of systems. In *23rd International System Safety Conference*. System Safety Society, August 2005.
5. T. P. Kelly. *Arguing Safety - A Systematic Approach to Safety Case Management*. PhD thesis, Department of Computer Science, University of York, 1999. http://www.cs.york.ac.uk/ftpdir/reports/YCST-99-05.pdf.
6. J. McDermott. Abuse-case-based assurance arguments. In *17th Annual Computer Security Applications Conference.*, pages 366–376. IEEE Computer Society, 2001.
7. MoD. Defence standard 00-58: HAZOP studies on systems containing programmable electronics. Technical report, UK Ministry of Defence, 1996.
8. International Civil Aviation Organisation. Annex 17, safeguarding civil aviation against acts of unlawful interference. ICAO, 2002.
9. International Civil Aviation Organisation. Doc 8973, security manual for safeguarding civil aviation against acts of unlawful interference. ICAO, 2002.
10. G. Sindre and A. L. Opdahl. Eliciting security requirements by misuse cases. In *Proc. of TOOLS Pacific 2000*, pages 120–131. IEEE Computer Society, 2000.
11. T. Srivatanakul. *Security Analysis with Deviational Techniques*. PhD thesis, Department of Computer Science, University of York, UK, 2005. http://www.cs.york.ac.uk/ftpdir/reports/YCST-2005-12.pdf.
12. T. Srivatanakul, J. Clark, and F. Polack. Security zonal analysis. Technical Report YCS-2004-374, Department of Computer Science, University of York, UK, 2004. http://www.cs.york.ac.uk/ftpdir/reports/YCS-2004-374.pdf.
13. T. Srivatanakul, J. A. Clark, and F. Polack. Effective security requirements analysis: HAZOP and use cases. In *Information Security: 7th International Conference*, volume 3225 of *LNCS*, pages 416 – 427. Springer, September 2004.
14. T. Srivatanakul, J. A. Clark, and F. Polack. Writing effective security abuse cases. Technical Report YCS-2004-375, Department of Computer Science, University of York, UK, 2004. http://www.cs.york.ac.uk/ftpdir/reports/YCS-2004-375.pdf.