1.4 – Impact of security on safety

Practical guidance – cross-domain

Authors: Professor Robin Bloomfield, Professor Peter Bishop and Dr Gareth Fletcher (Adelard LLP)

Security and safety have often been treated as separate disciplines, with their own regulation, standards, culture and engineering. Security requirements for vehicles are addressed in standards such as PAS 1885 [1] and ISO 26262 [2], but not in an integrated way with safety, particularly the impact of functional safety requirements on security and the possible hazardous consequences from an attack or intrusion of the system.

This approach is no longer feasible as there is a growing understanding that security and safety are closely interconnected: it is no longer acceptable to assume that a safety system is immune from malware because it is built using bespoke hardware and software, or that it cannot be attacked because it is separated from the outside world by an “air gap”.

Overall, security-informed safety is not generally explicitly addressed in current autonomous vehicles (AVs), and hence, the motivation for PAS 11281 [3]. Overall, we consider the PAS will be challenging for industry.

Security-informed hazard analysis

One of the key topics in PAS 11281 is the impact of security on risk assessment covering the whole life cycle of the vehicle. The PAS states that security concerns could have an impact on:

1. The system boundaries
2. What systems could potentially affect safety
3. The stakeholders involved
4. The validity of design safety assumptions

Therefore, care must be taken during the analysis to account for security concerns as well as safety. Table 1 summarises a 7-step risk assessment process.

Step	Brief description
Step 1 – Establish system context and scope of assessment	Describe the system to be assessed and its relationship with other systems and the environment. Identify the services provided by the system and the system assets. Agree the scope of, and motivation for, the assessment and identify the stakeholders and their communication needs. Identify the type of decisions being supported by the assessment.
Step 2 – Configure risk assessment	Identify any existing analyses (e.g. safety cases, business continuity assessments that provide details of the system), the impact of failure, and the mitigations that are in place. Characterise the maturity of the systems or project and the key uncertainties. Ensure that the risk assessment is focused on the kinds of threats that are of concern. Define possible threat sources and identify potential threat scenarios. Refine generic capability and impact levels for the systems being assessed. Identify risk criteria. Refine and focus system models in light of the threat scenarios and existing analyses to ensure that they are at the right level of detail for an effective security-informed risk analysis.
Step 3 – Analyse policy interactions	Undertake an analysis of policy issues considering interactions between safety requirements and security policies. Resolve any conflicts, show that the trade-offs are satisfactory and document the decisions made.
Step 4 – Preliminary risk analysis	Undertake architecture-based risk analysis, identifying potential hazards and consequences and relevant vulnerabilities and causes, together with any intrinsic mitigations and controls. Consider doubts and uncertainties, data and evidence needs. Identify intrinsic and engineered defence in depth and resilience.
Step 5 – Identify specific attack scenarios	Refine preliminary risk analysis to identify specific attack scenarios. Focus on large consequence events and differences concerning the existing system.
Step 6 – Focused risk analysis	Prioritise attack scenarios according to the capabilities required and the potential consequences of the attack. As with the previous step, the focus is on large consequence events and differences concerning the existing system.
Step 7 – Finalise risk assessment	Finalise risk assessment by reviewing implications and options arising from focused risk analysis. Review defence in depth and undertake sensitivity and uncertainty analysis. Consider whether the design threat assumptions are appropriate. Identify additional mitigations and controls.

Table 1 – 7-step security-informed safety risk assessment

There are a variety of initiatives to integrate security into hazard analyses. We have been using security- (or cyber-) informed Hazard analysis and operability studies (Hazops) [4] to assess architectures of industrial systems [5]. We adapted this well-known approach for systematically performing a safety hazard analysis [6], analysing the deviations of data flows and values between different interconnections in the system. To account for security in a security-informed Hazops, additional security guidewords are added and an enhanced multidisciplinary team (system safety and security experts) is used. Both security and safety perspectives are needed to assess the likelihood of vulnerabilities being exploited and the effectiveness and consequences of their mitigations. An example of a security-informed Hazops analysis is provided below.

Summary of approach

The deployment of autonomous technologies may follow an innovation cycle that first focuses on functionality and seeks to progressively add additional assurance and security. This will make the development of the assurance and safety cases and associated security and safety risk assessments particularly challenging. From our experience we currently recommend:

1. Explicitly define the innovation cycle and assess the impact and feasibility of adding assurance and security. Adapt the 7-step risk assessment process to the specific lifecycle being used.
2. Address the approach to security-informed safety at all stages of the innovation cycle, including undertaking a security-informed hazard analysis during development. The hazard analysis should be reviewed periodically during operation or when a safety-related component has been updated or additional threat or vulnerability information becomes available.
3. If safety, security and resilience requirements are largely undefined at the start of the innovation cycle, the feasibility of progressively identifying them during the innovation cycle should be assessed, together with the issues involved in evolving the architecture and increasing the assurance evidence.
4. Apply PAS 11281 to systematically identify the issues. If this is not possible because of the lack of defined processes or availability of information, consider a partial and project-specific implementation of the PAS to meet the innovation cycle.
5. Collect experience in developing a security-informed safety case and in integrating security issues into the safety analyses needed to implement the PAS.

Further details on this guidance can be found in [7].

Example of application of guidance

Step 4 of the 7-step risk assessment process was applied to the TIGARS Evaluation Vehicle (TEV). We performed a security-informed Hazops on the TEV architecture. This process is similar to the Hazops safety analysis with the addition of malicious security acts included in the possible causes of a hazard. We used a standard set of data flow and data value guidewords and reviewed key components of the architecture to understand the potential hazards in the system. The credibility and likelihood of a successful attack on the system depend on the capability level of the threat actor. We decided to consider threat actors with sophisticated capability and expert knowledge of the system. After all, once the vehicle is available for purchase there is nothing stopping a would-be adversary from purchasing a target vehicle to acquire detailed knowledge and have a testbed for their attacks.

Figure 1 shows the simplified architecture that was used for the security-informed safety Hazops of the TEV. We focused on the interfaces which involved Machine Learning (ML) components, such as object detection and fusion (denoted as 1, 2 and 3 in Figure 1). These components have additional complexity and differ from traditional components in road vehicles. It should be noted that the TEV is a research and development vehicle and not developed to any automotive standards. The results from applying the PAS in our case study may have been different if the TEV was not partly a research vehicle and a more mature system was being developed.

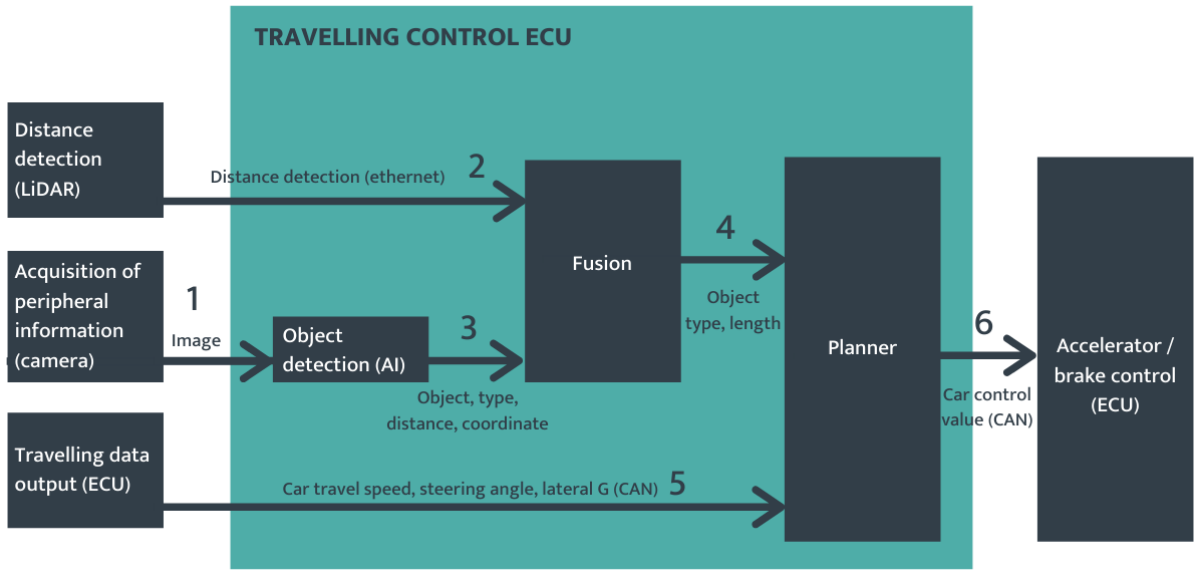

Figure 1 – Overall architecture of the TEV

We found that security issues could pose credible threats to ML components if the inputs or outputs were able to be modified by the threat actor. We would expect real-world autonomous vehicles (AVs) to be more mature systems with additional security hardening than the TEV in our case study; however, security should still be considered during the risk assessment and design of the AV. Our hazard analysis highlighted some additional alarms and monitoring that could be added to the TEV to help annunciate potential failures and problems of the ML components.

An example extract from the hazard analysis summary for component 1 is shown in Table 2.

Guideword	Interruption	Causes	Hazard	Mitigations
• Data flow: no action	• No image from camera	• C1: Hardware failure • C2: Lens tampering	• H3: Spurious safety stopping	• M1: LIDAR cross-check • M2: Pre-test checks • R1: Diagnostic for camera feed failure • R2: Diagnostic check for image quality

Table 2 – Extract from hazard log summary of TEV for data flow 1

Table 2 shows a traditional hardware reliability cause with a more security-focused cause both having possible contributing factors to a hazard. From this record in the Hazops, we recommended that diagnostic checks should be added to check that the camera feed is alive and assess the quality of the image from the camera.

The hazard is because upon failure of the advanced cruise control the TEV will enter into an emergency stop procedure. Having this function activated too often represents a hazard for the system.

The components in the system without ML are still susceptible to security compromise; for example, if falsified/altered data was sent to the planner setting target speed it would be possible to crash the TEV into obstacles that the LIDAR sensors had detected, or even spuriously apply the emergency brake at opportune moments; the centre of a traffic junction could be a hazardous place to stop.

References

- [1] BSI PAS 1885:2018 – The fundamental principles of automotive cyber security. Specification, 2018.
- [2] ISO 26262:2018 Road vehicles – Functional safety.
- [3] BSI PAS 11281:2018 – Connected automotive ecosystems. Impact of security on safety. Code of practice, 2018.
- [4] Security-Informed Safety: If it's not secure, it's not safe, Bloomfield (2013), R. E., Netkachova, K. & Stroud, R. Software Eng. for Resilient Systems, A. Gorbenko, A. Romanovsky, and V. Kharchenko, eds., LNCS 8166, Springer, 2013, pp. 17–32.
- [5] The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned, Bloomfield, R. E., Bendele, M., Bishop, P. G., Stroud, R. & Tonks, S. (2016). Paper presented at the First International Conference, RSSRail 2016, 28-30 Jun 2016, Paris, France.
- [6] IEC 61882:2016 Hazard and operability studies (HAZOP studies) – Application guide.
- [7] Bloomfield, R., Fletcher, G., Khlaaf, H., Ryan, P., Kinoshita, S., Kinoshit, Y., Takeyama, M., Matsubara, Y., Popov, P., Imai, K. and Tsutake, Y., 2020. Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS - A collection of Technical Notes Part 2. arXiv preprint arXiv:2003.00790.