J. Michael, J. Pfeiffer, A. Wortmann (Hrsg.): Software Engineering 2022 Workshops,
94 Digital Library, Gesellschaft für Informatik 2022

Comparison of Aviation and Automotive Standards and Methods in Terms of Safety and Cybersecurity

Yusuf Akkus[1], Bjoern Annighoefer[2]

Abstract: Safety and security methods from the aviation and automotive are compared. Current safety and security standards and regulations for both product development aspects like systems engineering, hardware/software development and their management are considered. Methods and processes are investigated. The main purpose is to figure out and understand the backgrounds and to characterize the similarities and differences. Moreover, potential opportunities for transferring methods from one industry to another are identified.

Aviation has more systematic development and involves authorities throughout the complete development lifecycle. Huge volumes in automotive leads to quality-driven development. Assessment structure and process activities provide potential transfer. For security both areas face same challenges and standardization activities and development run parallel. Methods are being mainly taken over from safety and assessment is incorporated into the safety assessment lifecycle today. For certification process, authorities must take action in both areas since the security ecosystem includes a bigger scope like infrastructure, communication devices, traffic control.

Keywords: ISO 26262, ARP 4754, DO-178, DO-254, FTA, FMEA, Cybersecurity, ISO 21434, DO-326, DO-356, DO-355, TARA, ASPICE.

1 Introduction

Automotive industry is confronting one of its most radical changes in history. While continuous state of the art development like driver assistance is advancing, disruptive technologies are in focus. Game changers like autonomous driving, e-driving and connectivity control direction of automotive development. Accompanying those technologies, conventional development methods reach their limits in efficiently covering the new scope. Increasing complexity e.g. high numbers of E/E components [1] and SW [2] make it necessary to look for new systematic approaches. Aviation´s experience over decades offers a big chance to learn from. Fly-by-wire systems, automation and systematical development approach is already state of the art. Thus a comparison and potential takeover of methods from aviation can help automotive accelerate defining approaches and establishing processes. Especially safety and security are key domains where automotive potentially benefits most from taking lessons from

[1] Daimler Truck AG, yusuf.akkus@daimlertruck.com

[2] Institute for Aircraft System, University of Stuttgart, bjoern.annighoefer@ils.uni-stuttgart.de

aviation. Aviation exhibits a proven safety depicted in the numbers given in Figure 1.

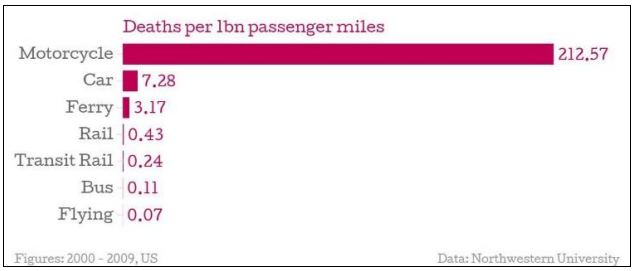

Fig. 1: Death rates in transportation [3].

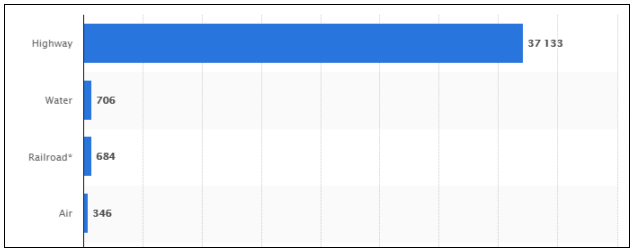

Fig. 2: Number of transportation fatalities in the United States in 2017, by mode [4].

Northwestern University gathered data from 2000-2009 to show death rate in passenger/miles. Fig. 1 shows that there is a factor of around 100 in the death rate between automotive and aviation. Newer numbers like fatalities confirm the same. Figure 2 shows the number of fatalities compared between automotive and aviation. These data are from 2017 and confirm previous factor. Data of Department of Transportation proves aviation´s safety as well [5].

High level of safety in aviation is because of well-established and mandatory incident management, regulations, methods as well as a centrally controlled certification. Automotive on the other hand had been organized federatively and used to empirical safety assurance, but is today at a point where safety obligations reach a level similar to that of aviation, what makes the continuation of established methods, processes and certification procedures at least questionable. This research targets to compare safety and security domain with backgrounds, similarities/differences, benefits, possible synergies to answer each time the question if automotive can take beneficial lessons from aviation. It is important to emphasize that it is not the intention of this research to claim aviation is better than automotive but to look for potential aspects to transfer and share synergies.

1.1 State of the Art

The transfer from aviation to automotive is a common question. Researcher and especially developers seek ways to use techniques and methods that are already developed, validated and established. Gerlach et al. [6] investigated the safety standards

which were ongoing at that time (2011) with the main question if there is a mapping between them. Crots et al. [7] compared the software development artifacts in 2014 and Schwierz et al. [8] did the same for hardware development between the two areas mainly for safety. Ledinot et al. [9] compared several areas like aviation, railroad, automotive etc. in terms of the impact of the assurance levels onto development activities. For cybersecurity, any comparison work between the areas of aviation and automotive was not found during the preparation phase of this research. This could be due to the fact that cybersecurity is a new field where development and standardization are still ongoing or not well established.

The contribution of this work is to compare both areas of safety/security methods by using outcomes of existing works. Similarities and differences are discussed mainly for transfer possibility from aviation to automotive. Main focus for the transfer is new technology, e.g. automated driving. The article structure is as following. Chapter 2.1 starts with a question why aviation is regarded as being safe and then related standards/methods are compared. Chapter 2.2 does the same for the security. Chapter 3 summarizes the results of the comparison with similarities and differences. It includes also the summary of transfer recommendation. Finally in chapter 4 an outlook to the future research is described.

2 Comparison of Aviation and Automotive Standards and Methods

2.1 Safety

Safety methodology have a detailed history in the both areas. Thus the comparison will have a much more structured overview. First the question why aviation is safe will be analyzed and then established standards and methods will be compared.

2.1.1 What makes aviation safe?

Before comparing standards of safety in aviation and automotive, an essential question needs to be answered. What is safe and why does aviation achieve the current level of safety? Safe can be defined as having less incidents with deadly outcome. In the introduction chapter, death/passenger miles was chosen as a parameter and aviation safety is proven. Two main reasons are answering the "why" question. First chronological order of establishing of standards. After civil aviation achieved high volumes in the mid of 20th century, systematical approaches were necessary.

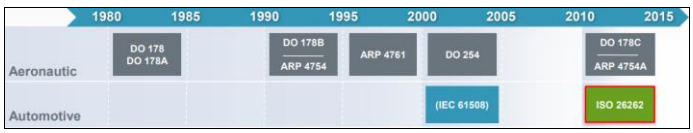

Fig. 3: Chronology of Safety related Standards [10].

Rising concerns about safety pushed the aviation industry to introduce safety related standards earlier than automotive. Figure 3 shows aviation being pioneer in systematic safety approach. E.g. SW standard in aviation DO-178 was initiated by 1980s where the counterpart in automotive ISO 26262-6 was released by 2011. The same is valid for hardware standards (DO-254 earlier than ISO 26262-5). Second reason why aviation is a safer way to travel is the rigorous assessment methods ARP 4761 and involvement and monitoring of the authorities early in the development.

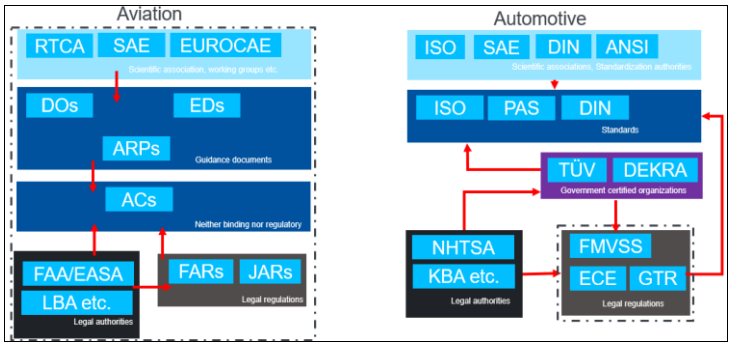

Fig. 4: From Standards to Certification.

Figure 4 shows in the dashed box the main focus during the initial phase of development. Concerns about certification require the aviation industry to not only follow regulation but also strictly follow the recommendation, standards and involve authorities early in the development. This maybe slows down the development, but provides a high level of review in terms of safety compliance. Automotive has a faster process for example because of so-called in-house release were authorized associates arrange the release process. Compliance to standards is the means for release of the development for new technologies.

2.1.2 Standards in Aviation and Automotive

In both automotive and aviation, standards have been established that guide the planning and development lifecycle to make sure safety compliance is considered.

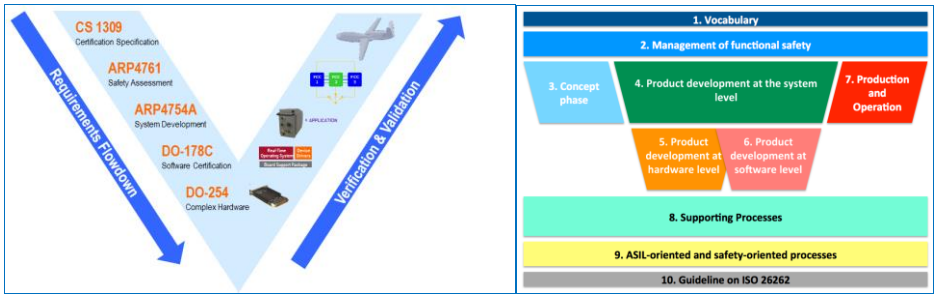

Fig. 5: Development lifecycle Aviation [11] and Automotive [12].

Figure 5 shows standards/documents in development lifecycle. In aviation, safety-related

lifecycle standards are split over several documents ARP (Aerospace Recommended Practices issued by SAE), DO (Documents issued by RTCA), CS (Certification Specification issued by EASA). For automotive all consideration is handled in only one document - ISO 26262. The second version of ISO 26262 even includes more types of road vehicles, e.g. two-wheelers [13]. Thus automotive has a better overview of work products so that all can be found in only one document. The reason for this difference is that aviation has an historical developed document environment and development lifecycle since it has begun earlier introducing standards and learned over the decades. A set of documents as it is established in aviation allows integrating updates easier. Automotive on the other side has raised such concerns later than aviation. It has also learned and gathered aspects/know-how and had a proper base to establish a more structured and compact standard in only one document. Versioning of ISO documents allows automotive to take over updates learned since the last released document.

2.1.3 Requirements Management & Systems Engineering

Requirements and system design are performed according to process defined in the ARP 4754 in aviation in order to initiate and perform certification for safety relevant items.

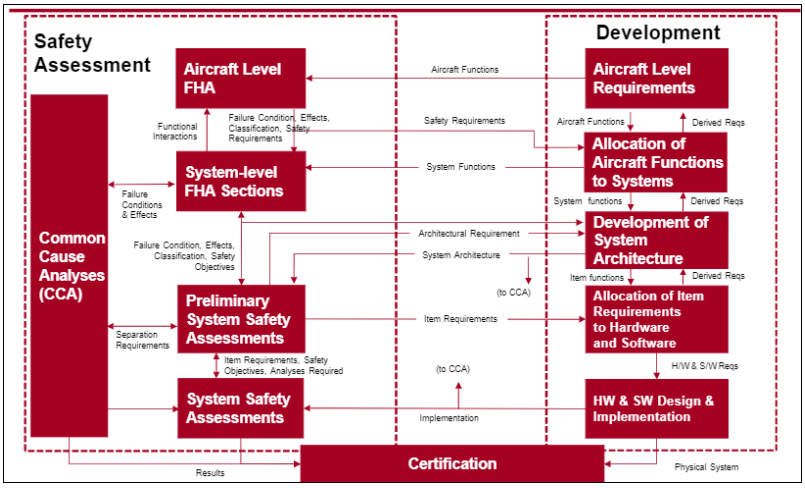

Fig. 6: Development lifecycle in Aviation according to ARP 4754 [14].

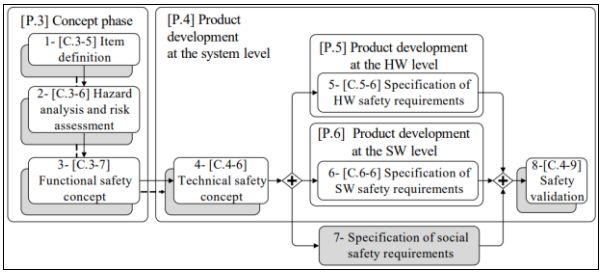

Fig. 7: Development lifecycle in Automotive according to ISO 26262 [15].

Figures 6 and 7 show what artifacts as work products are required in ARP 4754 and ISO 26262. Apart from some domain-specific differences like wording, the artifacts and work flows in both standards are similar. The flow from item/function definition via hazard & risk analysis via safety concept to HW/SW development are given in both industries. Both standards fulfil the needs of their current development. The following differences are important to mention: ARP 4754 requires in many points to involve authorities as early as possible in development process, which is due to the certification concern. It is essential for aviation since a complex system needs involvement of many institutions or persons. This would be an input for automotive to do it the same way especially because automated driving is a complex technology. Another difference is also that ISO 26262 has the main focus to be a standard with the requirement introducing development process for large numbers of vehicles. There is already a second version of ISO 26262 and autonomous driving technologies has not been addressed [16] because it is not the state of the art yet. A new version of the standard will regard the automated driving technology. Beside these differences the similarities between the two standards overweigh.

2.1.4 Safety Assessment

Automotive mainly relies on ASPICE (Automotive Software Performance Improvement and Capability dEtermination derives from ISO 15504). ASPICE mainly monitors processes and evaluates if processes are able to generate work products in a systematic manner with same quality. In aviation assessment is covered by the ARP 4761.

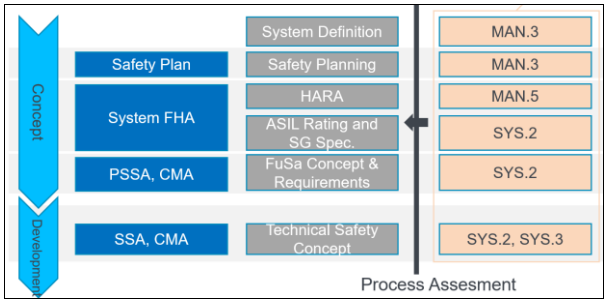

Fig. 8: Artifacts in ARP 4761 (blue), ISO 26262 (grey) and ASPICE.

Figure 8 shows artifacts of ARP 4761 and ISO 26262 that needs to be assessed. Main difference between the two areas is that ARP 4761 is an assessment process itself to evaluate and track safety in compliance with ARP 4754, DO-178, DO-254 etc. including safety assessment methods. ISO 26262 compliance checks are performed by authorities or institutions in-charge. Introducing an assessment ISO standard for safety could ease the job for assessors. On the other hand authorities like TÜV already perform ISO 26262 compliance audits which has a post-assessment character. ASPICE has domains like MAN (management) and SYS (system) that require certain process capability and work products in each case. ASPICE is not a safety assessment, but has an important role especially in the OEM-supplier relations in automotive.

2.1.5 Safety-relevant Software Development

Software development is the first domain where a structured development process need has been raised in aviation. DO-178 of RTCA is the first development guideline for safety-critical software developers and was introduced in the1980s. Although a huge amount has remained the same, there has been an evolution in the DO-178 document. Updates have provided clearer language and terminology with more consistency. More objectives have been added over the years. Current version is the DO-178C. The counterpart of it in automotive is the ISO 26262 part 6.

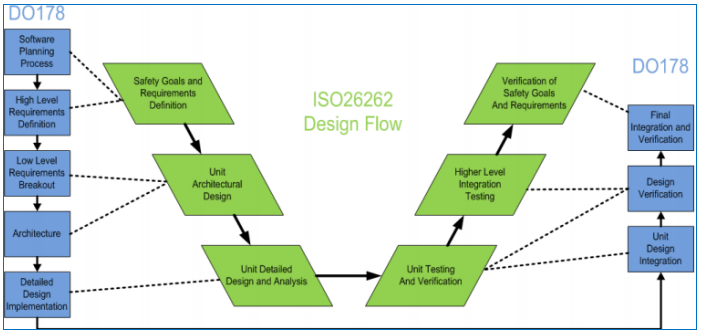

Fig. 9: Development Flow of DO-178 and ISO 26262 part 6 [7].

Figure 9 shows similarities in development flow. Differences are e.g. terminology. Main differences especially in the DAL and ASIL dependency of the two area.

Table 1. Safety Assurance Level Classification

	Aviation	Automotive
No Safety Relevance	DAL E	QM
High Safety Concern	DAL A	ASIL D

Table 1 shows the highest and lowest levels of safety integrity of the two areas. There are processes, activities, methods, tools, means and V&V requirements for each corresponding level [9]. Avionics development has strict verification thus process activities and related actions (objectives) are strongly depending on the DAL [9]. E.g., implementing a piece of code and only the required code and nothing else (avoidance of dead code) is the result that such activities are depending on the DAL. What methods should be used in order to achieve certain work products are not DAL dependent. This gives a certain amount of freedom to the developers since it reduces normative guidance. Automotive on the other hand focuses more on the quality of the work products (artifacts) and focuses more on the development process. So, applied methods/means (like which tools, which quantitative analysis, review etc.) are depending on ASIL and activities of development process also the work products are not strongly depending on ASIL. Automotive is evolving increasingly into high-complex and safety-critical technology. Defining concrete objectives (what exact artefact or work result/outcome)

and activities (defined measure/work to achieve objectives) depending on ASIL would increase confidence onto its products.

2.1.6 Safety-relevant Hardware Development

Hardware development guidelines in aviation are issued by RTCA with DO-254. It is the main input for AEH (Airborne Electronic Hardware) developers. The Automotive counterpart is the ISO 26262 part 5. In both documents/standards requirements on development process are mentioned. Both aviation and automotive have raised their HW concerns later (around two decades) than SW concerns. The following table compares development flow of both standards.

Table 2. HW Design lifecycle in both fields [8]

DO-254		ISO 26262	
Ref	**Name**	**Ref**	**Name**
4	Planning Process	5-5	Initiation of Product Development at the Hardware Level
5.1	Requirements Capture Process	5-6 8-6	Specification of Hardware Safety Requirements
5.2	Conceptual Design Process	5-7.4.1	Hardware Architectural Design
5.3 5.4	Detailed Design and Implementation Process	5-7.4.2	Hardware Detailed Design
5.5	Product Transition Process	5-7.4.5	Product, Operation and Decommissioning
6	Validation and Verification Process	8-9 8-6 5-6 5-7.4.4 5-10	Verification
7	Configuration Management Process	8-7 8-8	Configuration and Change Management
8	Process Assurance	2-6	Safety Management during the Concept and the Product Development

Table 2 shows that HW development lifecycle and related activities. Both areas are similar to each other. Aviation and automotive HW development have following differences: Aviation has the main architectural requirement of redundancy on system level which is due to the strict safety requirements that makes redundancy necessary. This has led over the years to use high number of components with available DALs. Automotive on the other hand needs cost reduction and works mainly on reducing the number of components by using high ASILs. Moreover, since automotive has an enormous impact on the market with its huge size, suppliers of HW mainly have focused developing according to the needs of automotive [17]. Compared to automotive, aviation industry was not able to make pressure on the E/E manufacturers due its smaller market size. For both areas, a common interest approach was the idea using COTS hardware to use synergy in cost reduction. FAA released in 2011 a report what safety requirements are valid in using COTS [18]. According to that common risk areas for usage of COTS

are identified and requirements on testability, monitoring and architecture for aviation are described [18].

2.1.7 Tools, Methods & Quantitative Approachs

Hazard analysis and risk assessment are being used in both area as a starting point. In aviation it is called FHA (Functional Hazard Analysis). HARA (Hazard analysis and risk assessment) is being applied in automotive. Both are similar to each other. Since both set up on functional level and investigate depending on the functional context the severities and exposures of hazards. But main difference is that aviation uses hazard categories as a result of severity and probability. HARA includes a third additional parameter the so-called controllability. The three parameters of HARA are severity which is what extent the hazard would have, probability/exposure what possibility an event/hazard may have and controllability if/in what amount is the hazardous situation is able to be avoided. DAL is depending on two parameters exposure and severity (controllability is in indirect way contained within severity) and ASIL on three. However, new technologies like automated driving raise the question if the controllability by driver is still a valid concern in future. To answer that question the performance of the automated driving function in automotive must be quantified to able to set the controllability value.

Aviation and automotive use several tools in order to investigate hazards. There is FTA (Fault Three Analysis) which is a top-down concept to find out root causes by going from failure case down to fault event. And there is also FMEA (Failure Mode and Effects Analysis) which is bottom-up concept to figure out what functional failure modes certain fault events may have. FTA and FMEA mark an interesting point in the comparison of aviation and automotive. FTA and FMEA are methods that were developed for aviation in the 1960s [19]. Increasing complexity made aviation develop qualified tools for safety. After successful application in aviation, these methods have begun to be used in automotive as well. Due to the need of quantification of safety metrics because increasing complexity also automotive (huge amount of E/E systems) a transfer of FTA and FMEA from aviation is already successfully done.

2.2 Cybersecurity

In the same way as safety, cybersecurity standards will be compared. Since cybersecurity is a new field, recent developments will be also regarded.

2.2.1 Differences to Safety

Compared to safety, cybersecurity domain is a rather new area. Both incidents and concerns have arisen in recent years thus the activities related to cybersecurity lifecycle have started. Especially connectivity has become an essential part of the cybersecurity ecosystem. Attacks have started and measures are being developed to counter them.

2.2.2 Is Aviation more secure?

Unlike safety, security is an area which is very new and there are not yet enough data to provide statistical evidence about incidents. There are not yet enough incidents to

provide a chart where “Deaths per passenger miles” is compared. Therefore instead of looking for such a chart, incidents can be listed which have occurred in the recent years in order to have an estimation about the extent and scope of cyber-attacks.

2.2.2.1 Aviation Cybersecurity incidents

The threats to commercial aviation started very early. Table 3 shows a summary of the threats. Jenkins [20] lists the security attacks to the commercial aviation.

Table 3. Pre-cybersecurity era (number of terror attacks) [20]

Time Period	Attacks
1968-1970	43
1971-1973	49
1974-1976	62
1977-1979	67
1980-1982	105
1983-1985	80
1986-1988	44

In cybersecurity era (2010s), the following incidents are listed amongst others:

2016/17: Some specific cyber-attacks targeted aviation. Typically airports and airlines. Main target in this case was to give to financial damage and image degradation. Safety was not endangered. The main victims of these attacks were Vietnam and Ukraine [21].

2017: A ransomware “WannaCry” attacked infrastructure and main civil aviation actors like Boeing and LATAM Airline Group etc. Target was financial damage. It was world-wide synchronized attack and estimated damage of appx. $4B was put on victims [21].

2015: One of the historical moments in aviation cybersecurity was a White Hat attack. Chris Roberts who is a white hat hacker, which means that he works for companies in order to improve their cybersecurity infrastructure, arranged to intrude into the computer system during a flight of a Boeing 737/800. He arranged to hack into the system via IFE.

Fig. 10: Chris Roberts message after hacking B737 [21].

2.2.2.2 Automotive security incidents

2015: A Jeep was remotely hacked during highway drive. Again, it was a white hat attack in order to see the cybersecurity robustness of the vehicle. It was able to take over control of vital systems of the vehicle.

Fig. 11: A Jeep was remotely hacked [22].

2020: An article showed that there has been a huge increase over the last three years in automotive cyber-attacks [23]. There are several reasons: Financial damage, hijacking etc. and white hat attacks which aim to detect cybersecurity weaknesses.

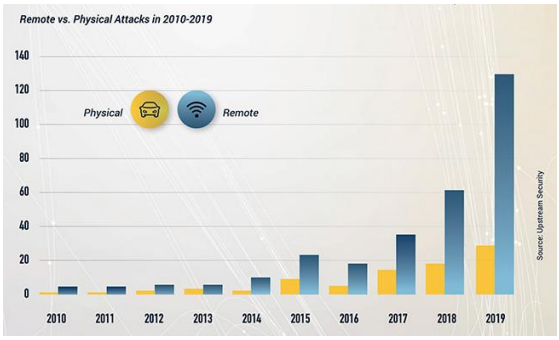

Fig. 12: Increase of Automotive Cyber-attacks [23].

2.2.2.3 Comparing Aviation and Automotive incidents

One of the main conclusions from the list of incidents is after the second half of the last decade there have been a huge increase of the cyber-attacks in both areas. Hackers used many different techniques to hack aviation and automotive components and infrastructure. In both areas the security ecosystem has become increasingly more complex and this gives attackers new access points like hardware, web, traffic control etc. This is why concerns and activities about cybersecurity have accelerated over the recent years.

2.2.3 Standards and Document Landscape

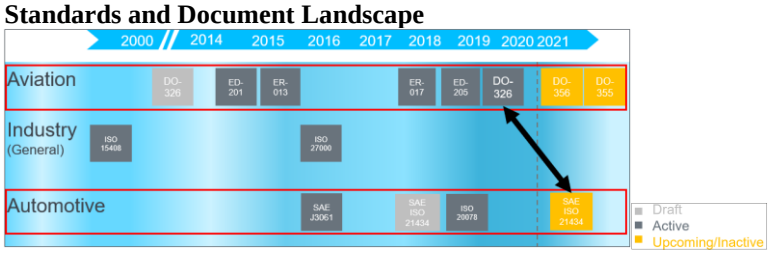

Fig. 13: Chronology of security-related standards.

DO-326 is the aviation counterpart of the automotive ISO/SAE 21434 standard. DO-326 includes description of necessary objectives/activities for the certification of security related development. Figure 14 confirms that standardization activities have accelerated in both areas after the 2nd half of the 2010s. First drafts are there as means of applicable methods and then they became official or awaiting to be official/active. Development activities are ongoing, so an interaction of security activities may bring synergies in both areas. Both can benefit from such cooperation since most attacks use similar techniques.

Fig. 14: Aviation (left) and Automotive (right) Security-related Standards.

Figure 14 compares both areas´ document landscapes and following statement can be made: Like for safety, aviation has a distributed document landscape. RTCA/EUROCAE define their activities methods etc. in several documents. Automotive manufacturers and suppliers can use ISO/SAE 21434 as a compact document and all necessary inputs from other documents are addressed within the ISO/SAE 21434. ISO/SAE 21434 was issued with a joint working group of ISO and SAE thus has a recognition in all automotive authorities. Table 4 gives a mapping from comparable documents of both areas.

Table 4. Aviation and Automotive Counterparts of Cybersecurity documents

Domain	Aviation	Automotive
Req.Management & System Eng.	DO-326/ED-202	ISO 21434-7,8
Methods	DO-356/ED-203	ISO 21434-6
Post-Development	DO-355/ED-204	ISO 21434-9

2.2.4 Product Security Development Lifecycles

Similar to the safety section, product development lifecycles are compared in order to give an overview of differences/similarities.

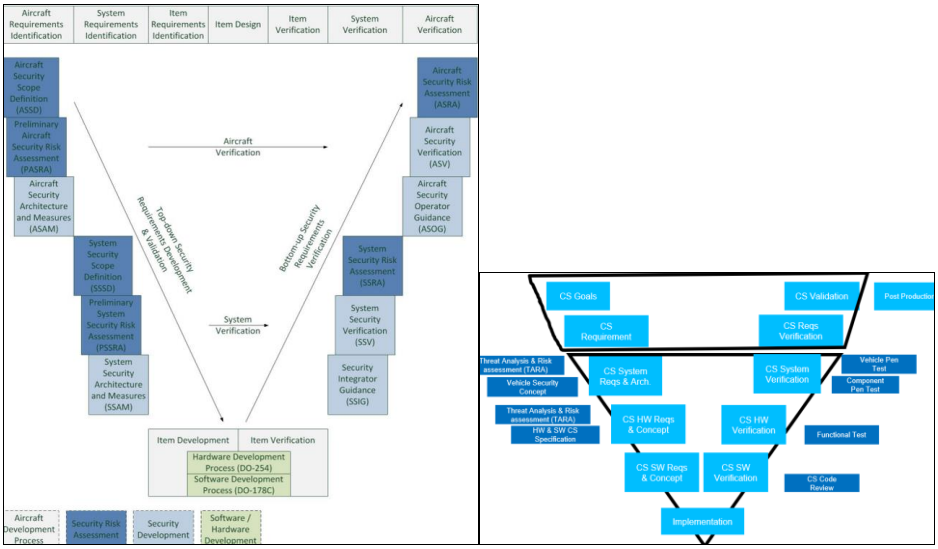

Fig. 15: Development Lifecycle according to DO-326 [24] and ISO/SAE 21434.

Figure 15 shows the development lifecycles in aviation and automotive. In aviation DO-326 activities are embedded into development lifecycle similar to ARP 4754. DO-326 can be considered as security counterpart of the ARP 4754 document. Both lifecycles get developed/reviewed by the same iteration. In automotive there is a security development lifecycle defined for its own. ISO 21434 is considered separately from safety lifecycle. In the initial phases, possibly due to lack of experts or structure of companies security was mainly handled by safety experts. But security structure has been established quickly and automotive feature two separate lifecycles for ISO 26262 and 21434 now. The structure is similar to ISO 26262. A small detail is that software and hardware are on the same level in the v-cycle. Since hardware related attacks are considered first hardware comes before software in the v-cycle now.

In general, both areas have established a well-structured document landscape. This is due to the urgency driven by the concerns raised in recent years, but because of the lessons learned from safety domain over the last decades. Since the requirements management and system engineering parts are already established and also adapted for each area correspondingly a possibility to transfer methods remains low. For future revisions, separate v-cycles are proposed since the safety and cybersecurity domain will get bigger and the scope is different. Separate life-cycles will help developers to focus on their own domain and also avoid road-blockers from other domain to go ahead.

2.2.5 Comparison of Cybersecurity methods

Like safety, in security both aviation and automotive try to benefit as much as possible from the lessons learned. Methods that are being used in safety are applied in an adapted way in security. DO-356 introduces a threat tree analysis which combines the classic FMEA and FTA for the security investigations similar to the Figure 20. Automotive has

several methods for TARA (Threat Analysis and Risk Assessment).

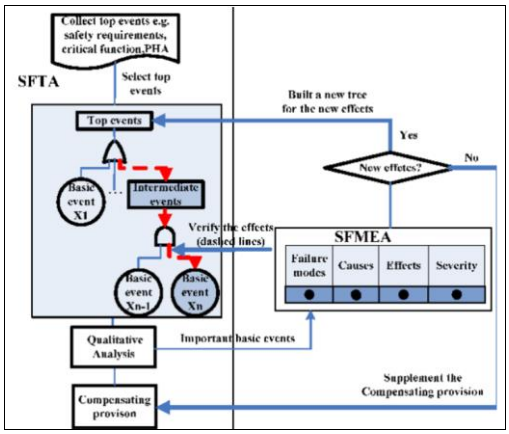

Fig. 16: Security FMEA and FTA combined [25].

In [26] a list of possible TARA methods is shown.

- ISO 21434-6 introduces some general methods
- EVITA: considers cybersecurity objectives (operational, safety, privacy, financial) with considerations for threat identification and threat classification
- HEAVENS: HEAling Vulnerabilities to Enhance Software Security and Safety
- SAHARA: Security-Aware Hazard Analysis and Risk Assessment …

Methods being used originate from safety. For bottom-up consideration a security adapted FMEA (SFMEA) and for top-down consideration a security adapted FTA are being used. Both areas tend to use combined methods of bottom-up (SFMEA) and top-down (SFTA). The main question about automated driving is if an additional consideration is needed. The automotive industry commonly agrees on ISO/SAE 21434 as a means of compliance even for automated driving [27].

2.2.6 Post-Development Lifecycle

Aviation uses DO-355 document in order to perform all post-development activities. It is the Information Security Guidance for Continuing Airworthiness. Combined with Airworthiness Security Process there is an overall guidance for aspects like Airborne SW handling, Aircraft components handling, Aircraft network access points, digital certificates, incident management and operator risk assessment. Authorities, airlines and airport operators uses this document as main guidance in order to comply with regulations. Additional stakeholders are software developers, component developers, ground support and related fields mentioned above. Automotive industry exhibits a higher granularity in order to distinguish between the post-development phases. ISO-21434 part 9 defines post-development sections: ISO-21434-9.1 provides security specification for production phase; Part 9.2 describes guidelines in order to perform cybersecurity monitoring e.g. to collect data or info about incidents; Vulnerability

handling & incident response in part 9.3; and updates in order to implement cybersecurity requirements and capabilities are regulated via part 9.4.

In general, the post-development phase and further steps are sector-related. There could be the possibility to use synergy from the countermeasures that are developed since most of the attacks are performed remotely and a common defense versus such attacks can be developed, which can be used in both areas. An additional field which comes into mind when addressing the post-development it is the traffic control (both aviation and automotive) since it is one of the main components of the cybersecurity ecosystem. This topic shall be investigated in detail.

2.2.7 Assessment Structure

Similar structures to safety are there. Aviation uses ARP 4761 assessment lifecycle in order to cover DO-326 activities. Automotive right now has no common practice to assess security lifecycle. Any mandatory method to assess the security is not mentioned/issued by the authorities. Companies handle that within their supplier-manufacturer relationship based on the activity requirements by ISO 21434. In [28] an integrated assessment of ASPICE, ISO 26262 and ISO/SAE 21434 is introduced. This is the main tendency and it shall be performed in the way that ASPICE covers to assess in the initial development phase all relevant activities.

2.2.8 Validation & Certification

For certification DO-326 defines 12 objectives and 62 activities for security specific assurance and 24 objectives with 56 for security development assurance including certification related ones. These steps shall always to include authorities where a validation plan is attached to the certification plan. Automotive follows the classic method of in-house release where a security validation plan and release process are defined together with safety. Each OEM follows its own release plan and authorities are included mainly in release phase unlike aviation. For automated driving, including authorities intensely into development shall be done, since security has even a bigger ecosystem with several attack sources.

2.2.9 Traffic Control and Monitoring

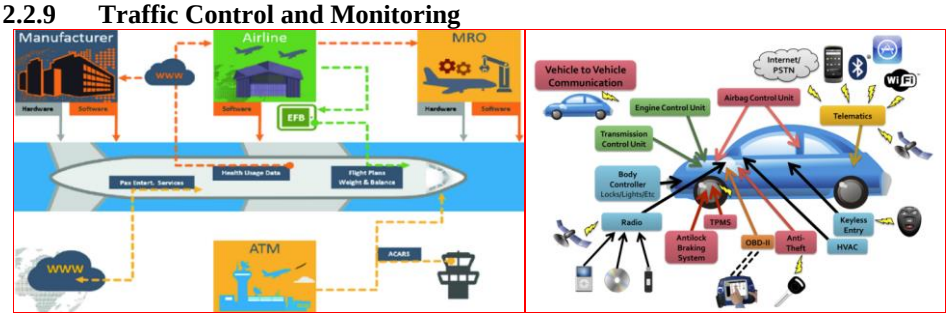

Fig. 17: Aviation Cybersecurity Ecosystem left [29] Automotive right [30].

The security ecosystem in both areas show that the air/road traffic control together with its monitoring mechanism is/shall be an important part of cybersecurity consideration.

ED-205 mentions already some aspects and automotive slightly touches this topic. However, for both today's systems and upcoming automated systems in both areas (flying and driving) a concept of traffic control and monitoring is needed. Thoughts and rough concept shall be worked out.

3 Summary

Comparison of both areas shows that there is a potential to carry over methods. Depending on the domain there is either high or low possibility to learn from aviation.

3.1 Findings

3.1.1 Safety

First question was why aviation is safer than automotive. This was answered by showing that aviation had an earlier start in systematic development and also broader involvement of the authorities. Also, well-established incident management has led to a better understanding of failure modes. That´s why learning effect was earlier in the aviation industry. Document/standard/guideline environment is more structured and with a better overview in automotive since complete development lifecycle is supported by just one standard ISO 26262. Aviation has a split document structure. The activities mentioned in aviation lifecycle have obligation as means of certification. In automotive the obligation is rather a standard which must be regarded as guidance.

Product developments artifacts and activities are similar in both areas. The main difference is the enhanced involvement of the authorities due to the certification regulations in aviation. ARP 4761 rules prescribe a complete safety assessment lifecycle. Automotive relies on ASPICE first and an ISO 26262 audit follows by involvement of TÜV or similar. Assessment structure have been established in both areas.

SW development lifecycles are also similar in both areas. The main difference is that related process activities are DAL dependent in aviation but not ASIL dependent in automotive. DAL dependency is important to make sure development provides specified products which is important for safety-critical systems. HW development is mainly impacted by the size of the manufacturers. So, automotive controls the market more than aviation. HARA in automotive needs an update of the third input parameter controllability in automated driving. There has been already a very successful transfer. FTA and FMEA are being applied in both areas.

3.1.2 Cybersecurity

Cybersecurity is a new field with new challenges and technical aspects. A quantitative comparison is not feasible today since there are no sufficient statistics on incidents. For early statistic investigations each particular incident shall be analyzed for its own. A quantitative analysis based on larger numbers will be most probably available in the

upcoming years after a period of time enough to cover/occur sufficient incidents. There is huge increase of cyber-attacks in both areas after 2nd half of the last decade. Standardization chronology shows an almost simultaneous development in both areas.

Again in security there is split of documents in aviation and automotive has a compact ISO 21434. With counterparts as chapters from ISO 21434 versus documents of RTCA correspondingly. System Engineering and Requirements management process are well established in both areas via DO-326 and ISO/SAE 21434. This is because both have ARP 4754/ISO 26262 as a base procedure.

Methods are mainly referred to DO-356/ISO 21434-6. The threat analysis and assessment methods are transferred from the well applied FTA and FMEA in both areas correspondingly. Both areas apply a security adapted way of these techniques. In terms of Automated Driving the automotive industry commonly agrees on ISO/SAE 21434 as a means of compliance. Security certification process including the validation activities is described step by step in aviation via DO-326 since it follows similar structure like in ARP 4754/4761. Automotive as well follows same procedure like in safety. The security ecosystem in both areas show that the air/road traffic control together with its monitoring mechanism is/shall be an important part of cybersecurity consideration. ED-205 mentions already some aspects and automotive slightly touches this topic.

3.2 Conclusion

Car manufacturers shall include authorities right in the beginning of their development especially for automated driving projects. An incident management concept similar to aviation shall be established.

ISO 26262 does not cover automated driving technology as of today which should be updated. For SW development automotive can benefit from making process activities (defining objectives concretely) dependent from ASIL. Using COTS HW would help aviation to reduce cost. FAAs report on restrictions and constraints can help avionic developers/manufacturers.

For cybersecurity a close interaction between the two areas of aviation and automotive may bring synergies into both since there are still activities and development ongoing. In addition, similar attack technologies make it possible to benefit from each other. Security assessment structure in both areas is based on a safety assessment structure. Aviation to integrate DO-326 assessment together with ARP 4754, 4761. Automotive right now has no common practice, but shall consider cybersecurity together with safety maybe in an already existing assessment structure (ASPICE). But safety and cybersecurity assessments shall not be always combined in order to avoid road-blockers.

For automated driving authorities shall be included development/release process.

4 Outlook

Both areas work with specific but similar methods. Where transfer possibilities are listed above security offers synergies in some areas. Incident management for automotive shall be detailed which will be worked out in the further phases of this work.

Automotive gets the pressure that documents are not ready for automated driving. ISO has already issued a new task with the target defining rules and acceptable means of release for automated driving which will be covered in the document ISO 5083.

But for both today´s systems and upcoming automated systems in both areas (flying and driving) a concept of traffic control and monitoring is needed. Thoughts and rough concept shall be worked out which will be a next step of this work.

5 References

[1] https://www.embitel.com/blog/embedded-blog/automotive-control-units-development-innovations-mechanical-to-electronics. 5/12/2020

[2] https://www.visualcapitalist.com/millions-lines-of-code/.5/12/2020

[3] https://www.cityam.com/one-chart-showing-safest-ways-travel/. 5/13/2020

[4] Statista, Number of transportation fatalities in the United States in 2017, by mode,https://www.statista.com/statistics/860124/us-transportation-fatalities-by-mode/, 01.03.2021

[5] https://www.bts.gov/content/transportation-fatalities-mode, 205/13/2020

[6] M. Gerlach, S. Weißleder, and R. Hilbrich, “Can Cars Fly? From Avionics to Automotive: Comparability of Domain Specific Safety Standards,” 2011, urn_nbn_de_0011-n-2485950.pdf (fraunhofer.de), 27.05.2021

[7] Kevin Crots, Paul Skentos, et al., “A Comparative Analysis of Aviation and Ground Vehicle Software Development Standards”, https://dornerworks.com/wp-content/uploads/2015/01/64_Crots_Kevin.pdf, 5/14/2020

[8] Andreas Schwierz, Hakan Forsberg, “Design Assurance Evaluation of Microcontrollers for safety critical Avionics”, https://arxiv.org/pdf/1803.09427.pdf, 5/15/2020

[9] Emmanuel Ledinot, Jean-Marc Astruc, et al., “A cross-domain comparison of software development assurance standards”, https://pdfs.semanticscholar.org/4c15/1cc5b24342dd1f5950561f3a27c9c585c909.pdf, 5/15/2020

[10] John Cotner, “Functional Safety and ISO26262 Compliance”, APF-AUT-T0503”, September 2013, Link: https://www.nxp.com/docs/en/supporting-information/DWF13_AMF_AUT_T0503.pdf, 5/14/2020

[11] https://www.curtisswrightds.com/news/blog/system-safety-certification-using-safety-certifiable-cots.html, 5/14/2020 .

[12] ISO26262, flow of workproducts visualized – system.network (icomod.com), 12/10/2021

[13] https://www.embitel.com/blog/embedded-blog/asil-vs-msil-iso-26262-12-2018-standard-introduced-for-two-wheelers/, 5/14/2020

[14] Chris Harper, Identification of Needs for Tool Support in Meeting Aircraft Avionics Systems, Hardware & Software Certification Standards, http://docplayer.net/13472550-Asuresign-aero-natep-grant-ma005.html, 5/14/2020

[15] Mohamad Gharib, Paolo Lollini, et al. “Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach”,

https://www.researchgate.net/publication/319464174_Dealing_with_Functional_Safety_Requirements_for_Automotive_Systems_A_Cyber-Physical-Social_Approach, 5/14/2020

[16] https://www.automotive-iq.com/electrics-electronics/articles/what-challenges-does-autonomous-driving-pose-iso-26262-part-ii, 5/14/2020

[17] Andreas Schwierz, Georg Seifert, Sebastian Hiergeist, “Funktionale Sicherheit in Automotive und Avionik: Ein Staffellauf”, https://dl.gi.de/bitstream/handle/20.500.12116/141/paper01.pdf?sequence=1&isAllowed=y, 5/15/2020

[18] FAA, “Handbook for the Selection and Evaluation of Microprocessors for Airborne Systems”. https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/AR_11_2.pdf, 5/15/2020

[19] Clifton Ericson, “Fault Tree Analysis – A Histrory”, https://web.archive.org/web/20110723124816/http:/www.fault-tree.net/papers/ericson-fta-history.pdf, 5/15/2020

[20] Brian Michael Jenkins, “The terrorist threat to commerical Aviation”, March 1989, The Terrorist Threat to Commercial Aviation (rand.org), 04.06.2021

[21] Aharon David, “DO-326A/ED-202A Aviation Cyber-Security - Afuzion”, Afuzion Training 2019, https://afuzion.com/do-326a-ed-202a-aviation-cyber-security/, 1/10/2021

[22] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, 1/1/2021

[23] https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/, 1/1/2021

[24] Christoph Torens, “Safety versus Security in Aviation, Comparing DO-178C with Securiry Standards”, 2020, Link: https://elib.dlr.de/133710/1/SafetyVersusSecurityStandards.pdf, 1/10/2021

[25] Ministero Della Difesa, “Cyber Security for Air Systems”, July 2020, Link: http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/7Categoria/Documents/AER_EP_DT_2020_026_Ed_02072020.pdf, 1/10/2021

[26] Hasan Ibne Akram, “Bridging the Cybersecurity Gap in Automotive”, Whitepaper 2020, https://matrickz.clickfunnels.com/matrickz_iso21434_whitepaper, 1/10/2021

[27] Joint Working Group from Automotive Industry, “Safety First for Automated Driving”, 2019, Link: https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf, 1/10/2021

[28] Macher, G., Schmittner, C., Dobaj, J., Armengaud, E. et al., "An Integrated View on Automotive SPICE, Functional Safety and Cyber-Security," SAE Technical Paper 2020-01-0145, 2020, Link: https://www.researchgate.net/publication/319453667_Automotive_SPICE_Safety_and_Cybersecurity_Integration, 1/10/2021

[29] Marrti Lehto, “Cyber Security in Aviation, Maritime and Automotive”, 2020, Link: https://link.springer.com/chapter/10.1007/978-3-030-37752-6_2, 1/10/2021

[30] David Silver, “Autonomous Security”, 2017, 08.01.2020, Link: https://medium.com/self-driving-cars/autonomous-security-564571bf6373, 1/10/2021