Abstract—Dealing with Commercial off-the-shelf (COTS) components is a daily business for avionic system manufacturers. They are necessary ingredients for hardware designs, but are not built in accordance with the avionics consensus standard DO-254 for Airborne Electronic Hardware (AEH) design. Especially for complex COTS hardware components used in safety critical AEH, like Microcontroller Units (MCUs), additional assurance activities have to be performed. All of them together shall form a convincing confident, that the hardware is safe in its intended operation environment. The focus of DO-254 is one approach called Design Assurance (DA). Its aim is to reduce design errors by adherence of prescribed process objectives for the entire design life cycle. The effort for certain COTS assurance activities could be reduced if it is possible to demonstrate, that the COTS design process is based on similar effective design process guidelines to minimize design errors. In the last years, semiconductor manufacturers released safety MCUs in compliance to the ISO 26262 standard, dedicated for the development of functional safe automotive systems. These products are COTS components in the sense of avionics, but they are also developed according to a process that focuses on reduction of design errors. In this paper an evaluation is performed to figure out if the ISO 26262 prescribes a similar DA approach as the DO-254, in order to reduce the COTS assurance effort for coming avionic systems.

Index Terms—AEH, ECMP, COTS, Microcontroller, SoC, Avionic, Certification, DO-254, ISO 26262, COTS assurance

I. INTRODUCTION

For development of AEH COTS components are an in-escapable ingredient. From simple electronic hardware such as serial peripheral controller, to complex electronic hardware, like a Microprocessor Unit (MPU), COTS components are widely used in safety critical avionic systems today. The availability of suitable MPUs for safety critical AEH is reducing. MCUs\(^1\) have a bigger market share and should be considered for future developments. Their high degree of functional integration can realize the majority of avionic system design requirements. However, the inherent complexity of a system-on-a-chip is very high and methods for COTS assurance to establish certification conformity are still an open topic of discussion in aerospace [1]. The reason is that, function blocks formerly developed in own responsibility by aviation industry are now part of the MPU. Its whole design life cycle became supplier controlled and is not necessarily aligned to AEH needs coming from certification or targeted operation context. The certification applicant has to demonstrate that the COTS component reached the same level of confidence as it would be achievable by an in-house design using aviation processes, w.r.t. the reasonably reduction of design errors. The concept of this process based evidence is called DA\(^2\). It claims a structured and requirement driven process intended to mitigate design errors, which could not be exposed otherwise due to the potential lack of complete verification [2]. The industry consensus standard DO-254 [3] and further guidance of certification authorities define the DA approach for AEH and how it could be adapted depending on different levels of safety implications induced by the hardware in a given system context. In order to be aligned with certification recommendations, adherence of that approach is an integral part of the argumentation about safe operation of an AEH or its inherent COTS components.

Summarized, MCUs shall be integrated certification compliant into the AEH and it is necessary within an COTS assurance process to demonstrate that the MPU design process produced the level of integrity\(^3\) required for AEH. An evaluation between an appropriate MPU design process and the DO-254 is needed to determine it.

This paper is organized as follows: In section II a short overview is given about current industrial practises for COTS assurance and research projects that contributed in this field. Section III describes in III-A and III-B the challenge and method for the evaluation between the DO-254 and an MPU design process. In section III-C the evaluation is performed and findings for each examined DO-254 hardware design life cycle process are delivered. Section IV contains a conclusion with ideas for future work.

\(^1\)Here also referenced as COTS component.

\(^2\)In context of airborne system and software development also known as development assurance.

\(^3\)Convincing confident about no unexposed design errors reaching the final product.
II. Certification Practice

Although the Federal Aviation Administration (FAA) and the European Aviation Safety Agency (EASA) have different positions about the application scope [4], [5] of the guidance document DO-254 [3], it is still the current recommended industry consensus standard for certification compliant development of AEH. DO-254 deals with a process model that is created around the principle of design assurance and contains additional considerations for the use of COTS components, mainly through an electronic component management process (section 11.2 in [3]) and product service experience (section 11.3 in [3]). In the past, it was unsuccessfully attempted to demonstrate DO-254 design assurance compliance by means of reverse engineering of required process artefacts of an MPU. After years, it was clear that this is not a practical approach [6]. With this lack in mind the certification authorities assigned several research projects to investigate the potential risks and challenges of different COTS technologies and how they can be addressed to satisfy certification requirements. As a result, further guidance materials were derived to enable complex COTS component usage in AEH.

Between 2006 and 2011, The Aerospace Vehicle Systems Institute (AVSI) project Authority for Expenditure (AFE) No. 43, released five research reports ([7], [8], [9], [10], [11]) and a handbook [12] addressing the use of MPUs in airborne systems. These reports and the handbook introduced the concept of safety nets, i.e. the employment of mitigations and protections at appropriate levels to protect against unexpected behaviour of an MPU. In the following AVSI AFE-75 project (performed between 2011-2013), the scope was extended to cover all kinds of COTS components including COTS assemblies. AVSI AFE-75 found more than 20 issues on the use of COTS electronics in AEH [1]. Special attention was given to attain a consistent application of safety and reliability guidance for all aerospace companies certifying under FAA [13]. In 2012, EASA released the certification memorandum (CM) CM-SWCEH-001 [14] to address design assurance of airborne electronic hardware. Section 9 in the CM-SWCEH-001 addresses guidelines for COTS digital AEH while section 10 covers the use of COTS graphical processors. Through section 9, EASA extends the application scope of DO-254 to include complex and even highly complex COTS components such as multicore processors as part of the AEH design. This is performed through different activities (from 2 up to 16), depending on device complexity and design assurance level. These activities were partially derived by research findings in [15]. The refined process description is a reasonable guidance coming from experience over many certification projects. In addition, the CM allows using alternative methods for COTS devices, such as reverse engineering of DO-254 life cycle data or other means of compliance. In practice, reverse engineering will be harder to perform the more complex the device is, since typically no detailed design data are provided by the COTS manufacturer. In later years, guidance for use of multicore processors in AEH have been jointly defined by many certification authorities in the Certification Authorities Software Team (CAST) paper No. 32A [16].

In practice, for COTS components different design assurance methods may be used in conjunction with each other, including the additional design assurance methods described in Appendix B in DO-254 [3]. These are:

Architectural mitigation It uses architectural design features to mitigate hardware design and implementation errors. Typically, monitors and dissimilar components may be used for COTS. The safety net approach described by [12] belongs to this approach.

Product service experience It identifies the service experience data and then establishes that the service experience data demonstrates that the reused functionality of the hardware is sufficiently exercised during previous uses of the hardware. EASAS CM [14] extends DO-254's product service experience scope with a COTS based service experience approach. The FAA report FAA [13] also gives guidance for the use of service experience.

Advanced verification methods It includes elemental analysis, safety-specific analysis (SSA), and formal methods. Elemental analysis requires details about the design and is therefore less suitable for COTS devices. SSA may be used as an additional design assurance approach, but may also require some details about the internal design of the device [17]. SSA focuses on exposing design errors that could adversely affect the hardware outputs from a system safety perspective [3]. Formal methods apply mathematics to prove correctness of a design and has according to the authors not been extensively used for airborne COTS design assurance. The determination and validation of the usage domain described in Section 9 in EASAs CM [14], may also be assigned to this category. The validity of the usage domain is ensured by a set of verification activities.

Extended electronic component management It addresses control mechanisms on the COTS manufacturer by means of detailed design data, how errata is maintained and published, how device data is configuration controlled, and how change impact analysis is performed.3

Reverse engineering In this way the life cycle data required by DO-254 are created from available COTS data or created from various reverse engineering techniques such as x-raying the components or detailed tests.

These methods are used complementary as means for COTS assurance or to build up the DA strategy. The assurance process is not a proof, but rather an accumulation of elements that leads to bringing the conviction of industrial partners and certification authorities that the equipment embedding complex COTS hardware is safe [18]. Currently, it is the Certification Review Item (CRI) type of document5 requested by the certification authority that functions as the container.

3Extended by the means of the EASA-CM [14].
4For FAA type certifications, issue papers are the requested type of document.
for the assurance strategy of complex COTS components e.g. MPUs [19].

III. DESIGN ASSURANCE EVALUATION

The previous chapter stated that a COTS assurance process is composed of different methods. The recognition of the COTS design process as a supplementary argument for the design integrity and is not often considered in industrial practice. It is required to collect as much assurance as possible, and process based evidence is one type of that.

If it could be demonstrated that the resulting integrity level of the MCU design process is comparable to the one of DO-254; this could establish a base of trustworthiness for all other assurance activities.

The concept of DA in DO-254 is defined as planned and systematic actions used to substantiate [...], that design errors have been identified and corrected [...] [3]. The extent of DA guidance, according to the title of DO-254, goes with error mitigation strategies beyond error avoidance. Thus, it is necessary to design the hardware such that it safely performs its function as intended also under abnormal behaviour. However, the evaluation precludes these fault tolerance or fail-safe aspects in order to concentrate on the overall design approach. So activities for fault avoidance to minimize design errors are separated from fault mitigation techniques that reduce consequences triggered by these errors.

A. Challenge

Aviation industry has another perspective on hardware design compared to most semiconductor manufacturer. This is logical since COTS components are targeted to domains with different claims according to design and safety goals; and the avionics industry is not among the biggest players in embedded systems. Nevertheless, avoidance of design errors is also a business case for COTS or semiconductor manufacturers in order to mitigate the risk of an economic loss by product recalls. The used approach is sufficient for this trade-off but not necessarily from a safety perspective which would cause an increased workload to reach a higher confidence.

The possible DA misalignment is a widespread opinion in aerospace, but it could not be carefully substantiated during a literature search. Origin of this attitude can be that only the DO-254 approach and its naming is in mind when this topic is discussed. Indeed, there are also references that if the COTS design process is requirements driven it could be based on similar approach as the one described in DO-254 [15]. Findings in [20] demonstrates that the verification phase of COTS components could be more comprehensive as it is required in DO-254, but because it is not compliant to DO-254 no certification credit can be claimed. Every single domain, especially safety-related one, is aware about the consequences of systematic faults and intend to reduce their likelihood of occurrence. It is generally accepted that no quantitative methods are available to measure how many possible design errors are present after a certain approach [21]. Because we cannot demonstrate how well we have done, we will show how hard we have tried [22]. So specific expert judgement and best practices are promoted for each domain as sufficient mean. These circumstance makes a comparison or evaluation quite difficult.

B. Method

1) Evaluation Goal: For the evaluation a terminology is needed as comparison scale between both processes. The known concept of Hardware Design Assurance Level (HWDAL) from DO-254 is not used. This concept is not independent since it is interwoven with the avionic domain and it proportionally depends on the severity of the failure condition caused by the malfunction of the hardware. For the evaluation the naming of integrity level is proposed, since it is independent of a domain or corresponding standard. In [21] it is stated that DA [...] establishes a level of confidence that the [...] [design] has been accomplished in a sufficiently disciplined, rigorous manner to limit the likelihood of [design] errors [...]. The integrity level represents this confidence about the limitation of design errors as property of the DA process.

Like a gap-analysis are the differences between the design approach of an MCU and the DO-254 identified. The evaluation goal is to qualitatively assess these differences of the COTS design approach w.r.t. their impact of the integrity level. The evaluation focus is on avoidance of design errors compared against the DO-254 guidance. Therefore, a determined integrity level is qualitatively given in relation to the DO-254. This ensures the applicability of evaluation results for the COTS assurance case.

2) Definition of Avionics Evaluation Base: The DO-254 is one single document, but also has interdependencies with the ARP4754A [23] and DO-178C [24] standards on system and software level. This structure is derived by a top down development concept, starting at the aircraft system level. Safety and functional requirements are broken down to the hardware levels. This ensures the satisfaction of important safety aspects that are an overall system property. The system safety assessment is conducted in conjunction with the hardware design team, but it is not in responsibility or scope of DO-254 hardware design life cycle that started at document section 3. At this point all implications on hardware regarding safety have to be formulated as safety requirements. During the whole design life cycle the assurance of safety is still in mind, but it is formalized as requirements that have to be correctly implemented.

The evaluation results shall be used within a DA strategy for a highly safety critical COTS component. The DO-254 introduces an assurance level approach to determine the process guidance by means of different severity stages in case of a malfunction. HWDAL A or B have to be considered for highly safety critical systems with catastrophic or hazardous failure conditions. For both, the same guidance set is applicable and thus they are considered for the evaluation. If the examination findings shall be reused for lower HWDAL, it can be adjusted afterwards.

6On system level it is called item development assurance level.
The relevant DO-254 process guidance, considered for the evaluation, is located form chapter 3 to appendix B. For reasons of clarity and comprehensibility, further certification guidance materials for the DO-254 are skipped for the present. Despite, it is necessary to bear in mind these additional documents if a later certification is intended. For a further evaluation iteration they will be considered.

3) Determination of a suitable COTS Evaluation Base: As counterpart for the evaluation an MCU should be selected that is potentially appropriate also in technical aspects. Its design approach should have similarities to the DO-254 in following properties:

**Standard Based** The MCU manufacturer derived its design process from a widespread standard. This enables the evaluation on a higher abstraction level when comparing the DO-254 with another standard. Additionally, assessment results can be reused for other products realized in accordance to the same standard.

**Process or product centred** A design process can consist of requirements on the product to define its nominal performance that shall be designed or on the process. The DO-254 does not claim requirements on the product performance. Only for DA some aspects are prescribed like architectural mitigation that have an impact on the product design.

**Avoidance of systematic errors** This should be explicitly stated or be a recognizable goal of the process. An assurance level approach that defines the process rigour is a good indication for that.

By searching for MCU candidates on the market, automotive products developed in compliance to the ISO 26262 [25] were identified. The design process is derived in compliance to the ISO 26262 which satisfies the above mentioned criteria. This process is based on a widespread standard that also focuses on hardware design. The ISO 26262 was specified for the development of functional safe electrical and/or electronic systems in a passenger car and highlighted the avoidance of design errors as one goal. This is achieved by an assurance level based design approach. Like DO-254, ISO 26262 defines process requirements to ensure the integrity of the design. The specification of nominal product performance is not considered by ISO 26262.

Especially this third party assessed and safety aware standard compliant design process is an advantage for AEH manufacturer. The process is still controlled by the COTS supplier but the framework is public. For a safety-aware process the reachable level of integrity is likely rather higher than for an MCU designed for the consumer market. For several years semiconductor manufacturers provided such kind of safety MCUs. They reach a high diagnostic coverage by the integration of safety mechanisms to reduce chip external provisions. These complex MCUs are equipped with a mixture of enough computing performance and interfaces, so they are appropriate for e.g. unmanned air vehicle applications.

The ISO 26262 consists of ten parts which together specify how a functional safe system, composed of software and hardware, shall be developed on vehicle level. Basically, the standard defines a top down development approach like in the aviation domain. However, a tailored life cycle is proposed, called Safety Element out of Context (SEooC), to enable the development of generic components, like an MCU, independent of a specific system development. The ISO 26262 part 5 with the title: Product development at the hardware level and all referenced parts have to be considered for the SEooC approach and as consequence also for the evaluation.

4) **Evaluation Procedure:** DO-254 section 1.7 states that if alternative processes are used as the one described in DO-254, it has to be evaluated if objectives are fulfilled with the same level of DA. This is also the target of this evaluation, to examine if the described ISO 26262 processes enable a similar integrity level of the designed hardware. This is done for each DO-254 process expecting the certification liaison, since this is not a comparable process for the ISO 26262 as for its adherence no governmental authorities are responsible nor claim it. An accredited organization like the TÜV SÜD is able to verify that a semiconductor manufacturer developed an MCU compliant to the ISO 26262. The standard do not describe the interdependencies between certification organisation and the company applying it.

Every specified DO-254 process defines objectives and activities that formulates the guidance on how to accomplish the objectives. Associations between objectives and activities are not explicitly described. However, for the evaluation it is helpful to understand the linkage between them, because the activities are more descriptive as the objectives, so they are more suitable for the evaluation. The ISO 26262 specifies for each process requirements which are formulated on a similar abstraction level as the DO-254 activities.

The evaluation procedure starts with DO-254 activities and map them with suitable ISO 26262 requirements. In order to facilitate the mapping, the DO-254 activities are excerpted and reduced to the essentials. After this, all associations are established between DO-254 objectives, DO-254 activities and ISO 26262 requirements. In order to make a statement about the ISO 26262 compliance of each DO-254 objective, all associations form ISO 26262 requirements via DO-254 activities to DO-254 objectives are considered. From table II to X these associations are shown. To build these relations, it is necessary to interpret the equivalence between the DO-254 activities and the ISO 26262 requirements, because each standard uses its own vocabulary. For readability reasons, associated ISO 26262 requirements and DO-254 activities are only presented as item numbers. At the end of each process evaluation a qualitative statement is presented if the process

---

7 The technical suitability and associated certification effort are not considered here.

8 Objectives and activities related to certification liaison process are omitted.

9 As described in III-B1, the evaluation or mapping is only preformed against the DO-254 processes.
Table I: Hardware Design Life Cycle Process Mapping

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

Table II: Planning Process Mapping

| DO-254 Objectives
| ISO 26262 |
|------------|----------|
| 1) The hardware design life cycle processes are defined. |
| 2) Standards are selected and defined. |
| 3) The hardware development and verification environments are selected or defined. |

| DO-254 Nr | ISO 26262 Nr |
|-----------|-------------|
| 1.        | 1.          |
| 2.        | 2-6.4.3.5f  |
| 3.        | 5-7.4.2.4   |
| 4.        | 2-6.4.4.1   |
| 5.        | 2-6.4.3.5h  |
| 6.        | 5-5.4.1     |
| 7.        | 2-6.4.3.5j  |
| 8.        | 2-6.4.4.2   |
| 9.        | 2-6.4.4.1   |
| 10.       | 2-6.4.8.1   |
| 11.       | 2-6.4.7.1   |

According to ISO 26262 reach a comparable integrity level as the corresponding DO-254 process.

The ISO 26262 defines an assurance level approach called Automotive Safety Integrity Level (ASIL), where D is the level that claims the highest amount of risk reduction. All requirements and methods of the ISO 26262 applicable for ASIL D are considered.

C. Realisation

Before the evaluation is done according to the procedure described in III-B4, hardware design life cycles of both standards should be compared in order to give an overview about the applied process mapping. Table I shows all DO-254 hardware life cycle processes relevant for the evaluation with the best associative ISO 26262 processes. Even though, the configuration management is mappable and an important process in a design life cycle, it is not considered in this evaluation since the ISO 26262 referencing another standard at this place. The reference numbering syntax of ISO 26262 part number, a hyphen as separator and then the chapter numbering. In section III-C it is outlined how suitable this mapping is w.r.t. the DO-254 intention of the processes.

Neither ISO 26262 nor DO-254 prescribe a life cycle model, since this is not a part of the evaluation. Both standards define a reference process model that indicates the idealized process sequencing and remarks that they may be iterative entered and re-entered with feedback flows. This depends on many factors and has to be defined by the applicant.

10 The mentioned V-model in ISO 26262 is just for reference.

Table I: Hardware Design Life Cycle Process Mapping

12 Tool assessment approach is not considered.
mapping in table III shows that six DO-254 activities are associated to objective one. They describe that requirements from different sources shall be reasonably identified, documented and linked to each other. Safety and derived requirements are emphasized. The source of a requirement could be the system level process or design constraints. A derived requirement is a requirement that is an interpretation of an allocated system requirement or a consequence of a design constraint and is defined to be implementable on the hardware level. The ISO 26262 also knows concepts of derived requirements but concentrates on safety related requirements. Requirements without safety relationships can be managed outside of the ISO 26262 life cycle. This is not the case for the DO-254. Bidirectional traceability between hierarchical requirements levels are requested by both standards. According to DO-254 objective two and three, the ISO 26262 specifies that all hardware requirements have to be verified with higher level specifications.

**Evaluation findings** The concentration on safety-related requirements, in the requirements capture phase of the ISO 26262, could cause misunderstandings by managing non-safety-related requirements in another way. However, according to ISO 26262 design process all requirements, even non-safety requirements, have to be handled within one development process. The DO-254 clearly states that all allocated requirements have to be considered. It is a debatable point whether it is practical in a real development to separate the managing of some requirements, but it is possible. Such a situation could increase the potential of design errors. This cause an integrity level deprecation of the ISO 26262.

3) **Conceptual Design Process:** Within the conceptual design phase, the hardware architecture shall be defined. All components are described with their interactions with one another on a higher level description, like the detailed design afterwards.

The ISO 26262 is also aligned with the objective number one, refer table IV. The requirements implemented in the hardware architecture shall be traceable to the lowest level of hardware component. If safety specific architectural constraints are formulated as hardware safety requirements, they are considered in the architecture. Unused functions are addressed in ISO 26262 if they have a safety impact. In this case, their independence has to be demonstrated. The feedback of derived requirements according DO-254 objective two is not explicitly described in ISO 26262. Problems with requirements are communicated in the verification phase as specified in ISO 26262.

**Evaluation findings** The ISO 26262 fulfils the objectives, see table IV. The DO-254 emphasizes safety-related aspects of the hardware architecture, that should usually be introduced by requirements coming from the safety assessment. ISO 26262 does not explicitly mention that also in this phase requirements could be derived, but the incremental re-entering of the requirement specification phase could be performed. The ISO 26262 process is considered on an equal level of integrity.

4) **Detailed Design and Implementation Process:** Detailed design and implementation are separate processes in DO-254. ISO 26262 does not describe a dedicated phase for implementation of the design. It is assumed as a part of the overall hardware design phase, that is ending with a component ready for test activities. Both tables V and VI show that most of the mapped ISO 26262 requirements do not originating from the dedicated ISO 26262 processes used as evaluation counterpart. So the concrete activities mentioned by the DO-254 processes have to be associated, on the ISO 26262 side, with requirements from other phases.

The first objective of the detailed design process is respected by the ISO 26262. However, the highlighting of safety aware-

---

**Table III: Requirement Capture Process Mapping**

| DO-254 | ISO 26262 |
|--------|-----------|
| Obj Nr | Act Nr |
| 1. 1. | 8-6.4.2.3; 5-6.4.2 |
| 1. 2. | 8-6.4.2.5a,c |
| 1. 3. | 5-6.4.1 |
| 1. 4. | 5-6.4.1; 5-6.4.2 |
| 1. 6. | 8-6.4.2.4e |
| 1. 8. | 8-6.4.1; 8-6.4.3.2a,b |
| 2. 5. | 5-6.4.9 |
| 3. 7. | 5-6.4.9 |

**Table IV: Conceptual Design Process Mapping**

| DO-254 | ISO 26262 |
|--------|-----------|
| Obj Nr | Act Nr |
| 1. 1. | 5-7.4.1.1 |
| 1. 2. | 5-7.4.1.1; 5-7.4.1.5; 5-7.4.3.5* |
| 1. 5. | 5-7.4.1.1; 5-7.4.1.6 |
| 2. 3. | 5-7.4.4.2* |

*Origin outside the mapped process.
Table V: Detailed Design Process Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) The detailed design is developed from the hardware item requirements and conceptual design data. | 5-7.4.4.1* |
| 2) Derived requirements are fed back to the conceptual design process or other appropriate processes. | 5-7.4.1.1* |
| 3) Requirements omissions and errors are provided to the appropriate process for resolution. | 5-7.4.1.6* |
| 4) | 5-7.4.3.5* |
| 5) | 5-7.4.2.2 |

Table VI: Implementation Process Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) A hardware item is produced which implements the hardware detailed design using representative manufacturing processes. | 4-11.4.2.2* |
| 2) The hardware item implementation, assembly and installation data is complete. | 4-11.4.1.1* |
| 3) Derived requirements are fed back to the detailed design process or other appropriate processes. | 4-11.4.1.1* |
| 4) Requirements omissions and errors are provided to the appropriate process for resolution. | 5-7.4.5.1; 5-7.4.5.2 |

Table VII: Product Transition Process Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item. | 4-11.4.2.2* |
| 2) Manufacturing requirements related to safety are identified and documented and manufacturing controls are established. | 4-11.4.1.1* |
| 3) Derived requirements are fed back to the implementation process or other appropriate processes. | 4-11.4.1.1* |
| 4) Errors and omissions are provided to the appropriate processes for resolution. | 4-11.4.2.3* |

Evaluation findings: The ISO 26262 plans in a very similar manner the product transition like DO-254. Derived requirements feedback and the concrete manufacturer control are not mentioned by ISO 26262, but this does not lead to a deprecation for the evaluation. The resulted integrity level of this process is comparable →.

6) Validation and Verification Process: In DO-254 and ISO 26262, validation and verification are supporting processes. This means, that they are concurrently performed with the former evaluated design processes. Between validation and verification no differentiation is stated in ISO 26262 in the way like in the DO-254. The supporting process verification in ISO 26262 part 8 is the conceptual root where the process is described in general. At hardware level, validation

---

14 See table V and VI. 

*Origin outside the mapped process.
Table VIII: Validation Process Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) Derived hardware requirements against which the hardware item is to be verified are correct and complete. | 5-6.4.2; 8-6.4.3.4 |
| 2) Derived requirements are evaluated for impact on safety. | 8-6.4.3.1e; 8-6.4.3.3; 8-9.4.1.1c |
| 3) Omissions and errors are fed back to the appropriate processes for resolution. | 5-6.4.9b |
| 4) | 5-6.4.9d |
| 5) | 8-9.4.3.2a |
| 6) | 8-9.4.4.2 |

Table IX: Verification Process Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) Derived hardware requirements against which the hardware item is to be verified are correct and complete. | 5-10.4.5 |
| 2) Derived requirements are evaluated for impact on safety. | 8-9.4.2.3; 8-9.4.2.1; 8-9.4.1.1b |
| 3) Omissions and errors are fed back to the appropriate processes for resolution. | 8-9.4.3.2 |
| 4) | 8-9.4.1.1 |
| 5) | 8-9.4.1.2 |

Table X: Process Assurance Mapping

| DO-254 Objectives | ISO 26262 |
|-------------------|-----------|
| 1) Life cycle processes comply with the approved plans. | 2-6.4.3.2; 2-6.4.7.1 |
| 2) Hardware design life cycle data produced complies with the approved plans. | 2-6.4.8.1 |
| 3) The hardware item used for conformance assessment is built to comply with the associated life cycle data. | 2-6.4.7.1 |

Evaluation findings

Both standards have different meanings of the term validation and verification. This is not a show stopper for reaching the same level of integrity. However, the different depth of traceability, the omission of independence and the less rigour for verification means in ISO 26262 results in a lower integrity level as requested by DO-254.

7) Process Assurance: In contrast to the DO-254, the ISO 26262 prescribes the organizational structure for the process assurance activities in a different context and role. The requested independence by DO-254 is satisfied by ISO 26262. Confirmation measures are performed by persons from a different department or organization. The DO-254 objectives are fulfilled by a small set of ISO 26262 requirements. The reason is, that two kind of confirmation measures are responsible to verify work products, output of processes, and the adherence of the plans. Table X shows that all DO-254 activities could be mapped to ISO 26262 requirements with a similar intention. The required degree of independence during process assurance is satisfied by ISO 26262.
DO-254 objectives are addressed with an approach that focused on the same kind of activities. Hence, for this process the ISO 26262 contributes to the product integrity on the same level as the DO-254 →.

IV. Conclusion

The performed evaluation could be considered as a first step to get an impression about the differences between the both standards in avoidance of hardware design errors. The applied qualitative measure of integrity level, in relation to the DO-254, results in a tendency that the ISO 26262 will not reach the necessary design assurance requested by the DO-254. This is derived from the evaluation findings in section III-C, where discrepancies for following processes were determined: requirements capture, detailed design, implementation, validation and verification process.

An evaluation on the abstract level of standard documents is not sufficient to come to a final result, if an automotive microcontroller unit developed with an ISO 26262 compliant process has a lower integrity level as requested by DO-254. The provided evaluation findings can be reused for a deeper analysis on the interpreted level of the standard. This means, to evaluate an ISO 26262 compliant development process of an MCU manufacturer with the additional certification authority guidance for DO-254, that give a better clarity on interpretation of the DO-254 document. For this purpose, a contact is established to a COTS manufacturer.

As a further part of this deeper evaluation, the ISO 26262 certification, authorised by an independent accredited organisation like TÜV SÜD, is considered. It is necessary to understand how such a certificate is issued. What are the inspection methods and the focused areas? These have to be compared against the certification authority approach. Findings of that evaluation are especially valuable, because it is supposed that MCU manufacturers are willing to disclose same documents with a certification authority.

In view of ever growing market share of hardware components for safety-related embedded systems [26], such evaluation findings will become of more relevance. It is a benefit for certification authorities to understand the meaning of such COTS component standards w.r.t. to their own regulations and accepted means of compliance. Avionic and semiconductor industries could both profit from products that consider aviation concerns.

ACKNOWLEDGMENT

This paper is sponsored by the Airbus Defense and Space endowed professorship “System Technology for safety-related Applications” supported by “Stifterverband für die Deutsche Wissenschaft e.V.”

MDHs work in this paper is supported by the Swedish Knowledge Foundation within the project DPAC.  

REFERENCES

[1] L. Condra, G. Horan, H. Forsberg, D. Matthews, J. Peterson, A. Martin, S. Barbagelata, K. Lillestolen, D. Redman, B. Petre, C. Kilgore, J. Strasburger, and R. Manners, “AFE 75 COTS AEH Issues and Emerging Solutions,” FAA, Tech. Rep., 2014.

[2] R. K. Thornton, “Review of Pending Guidance and Industry Findings on Commercial Off-The-Shelf (COTS) Electronics in Airborne Systems,” FAA, Tech. Rep. DOT/FAA/AR-01/41, 2001.

[3] RTCA, “DO-254 Design Assurance Guidance for Airborne Electronic Hardware,” 2000.

[4] “Subject: RTCA, INC., DOCUMENT RTCA/DO-254, DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE,” FAA, Tech. Rep. AC 20-152, 2005.

[5] EASA, “Certification Specifications and Acceptable Means of Compliance for Large Airplanes CS-25,” 22.06.2016.

[6] V. Hilderman and T. Baghi, Avionics certification: A complete guide to DO-178 (software), DO-254 (hardware). Leesburg, VA: Avionics Communications, 2007.

[7] R. N. Mahapatra and S. Ahmad, “Microprocessor Evaluations for Safety-Critical, Real-Time Applications: Authority for Expenditure No. 43 Phase 1 Report,” FAA, Tech. Rep., 12.2006.

[8] R. N. Mahapatra, P. Bhojwani, Lee Jason, and Y. Kim, “Microprocessor Evaluations for Safety-Critical, Real-Time Applications: Authority for Expenditure No. 43 Phase 3 Report,” FAA, Tech. Rep., 02.2009.

[9] R. N. Mahapatra, P. Bhojwani, and Lee Jason, “Microprocessor Evaluations for Safety-Critical, Real-Time Applications: Authority for Expenditure No. 43 Phase 5 Report,” FAA, Tech. Rep., 05.2011.

[10] R. N. Mahapatra, J. Lee, N. Gupta, and B. Manners, “Microprocessor Evaluations for Safety-Critical, Real-Time Applications: Authority for Expenditure No. 43 Phase 4 Report,” FAA, Tech. Rep., 09.2010.

[11] B. Geen, J. Marotta, B. Petre, K. Lillestolen, R. Spencer, N. Gupta, D. O’Leary, J. D. Lee, J. Strasburger, A. Nordsieck, B. Manners, and R. N. Mahapatra, “Handbook for the Selection and Evaluation of Microprocessors for Airborne Systems,” FAA, Tech. Rep., 2011.

[12] L. Mutuel, B. Franck, and A. Franck, “Final Report for Software Service History and Airborne Electronic Hardware Service Experience in Airborne Systems,” FAA, Tech. Rep., 2016.

[13] “Development Assurance of Airborne Electronic Hardware,” EASA, Tech. Rep. EASA CM - SWCEH - 001 Rev. 1, 2012.

[14] F. FAUBLADIER and D. RAMBAUD, “Safety Implications of the use of system-on-chip (SoC) on commercial-of-the-shelf (COTS) devices in airborne critical applications: Safety Implications of the use of system-on-chip,” EASA, Tech. Rep. EASA.2008/1, 2008.

[15] Certification Authorities Software Team, “Position Paper CAST-32: Multi-core Processors,” 2014.

[16] H. Forsberg, “Safety-specific analysis as additional design assurance for microprocessors,” in IEEE/AIAA 27th Digital Avionics Systems Conference, 2008, IEEE, Ed. IEEE, 2008, pp. 5.D.2–1–5.D.2–12.

[17] X. Jean, L. Mutuel, and V. Brindjejonc, “Assurance methods for COTS multi-cores in avionics,” in 35th DASC - Digital Avionics Systems Conference, IEEE, Ed. IEEE, 2016.

[18] H. Forsberg and K. Karlsson, “COTS CPU Selection Guidelines for Safety-Critical Applications,” in 2006 ieee/aiaa 25TH Digital Avionics Systems Conference, pp. 1–12.

[19] B. Butka, “Advanced Verification Methods for Safety-Critical Airborne Electronic Hardware,” FAA, Tech. Rep., 2015.

[20] CAST. “CAST-24: RELIANCE ON DEVELOPMENT ASSURANCE ALONE WHEN PERFORMING A COMPLEX AND FULL-TIME CRITICAL FUNCTION,” Tech. Rep., 2006.

[21] J. Rushby, Scientific Certification. [Online]. Available: http://www.csl.sri.com/users/rushby/slides/hcss-as06.pdf

[22] SAE Aerospace, “ARP4754A Guidelines for Development of Civil Aircraft and Systems,” Tech. Rep. ARP4754A, 2010.

[23] RTCA, “DO-178C Software Considerations in Airborne Systems and Equipment Certification,” Tech. Rep., 2011.

[24] ISO, “ISO 26262 Road vehicles – Functional safety,” Tech. Rep., 2011.

[25] Andrew Hopkins, “The Functional Safety Imperative in Automotive Design,” ARM, Tech. Rep., 09.2016.