Benjamin Alexander Paulsen*, Sandra Henn, Georg Männel and Philipp Rostalski

Functional Safety Concept EGAS for Medical Devices

Abstract: For patient safety, it is important that a medical device can safely and reliably perform its intended purpose. The challenge in medical technology is that medical devices are heterogeneous systems and thus no widely applicable standard concepts for functional safety exist in medical technology. This is also reflected in the regulatory landscape, with its rather generally applicable standards. Patient safety is currently achieved by performing continuous risk management with an acceptable level of residual risk. Functional safety and its design concepts, as applied in other industries, have so far found little application in the field of medical technology. In this paper, the automotive safety concept "EGAS" is analyzed with regard to its applicability for medical devices. Based on the investigated example of a medical ventilator, important parallels were found between the automotive and the medical device sector, indicating the possibility of successfully applying the EGAS safety concept to medical devices.

Keywords: EGAS, functional safety, standard, risk management.

<https://doi.org/10.1515/cdbme-2021-2189>

1 Introduction

Medical electrical devices are commonly performing safety critical tasks on humans, often in a vulnerable state, thus posing a severe risk of harming the user in case of a device malfunction. A rigorous risk management process needs to be performed during the development process [1] and medical devices have to comply with several standards concerned with

various safety aspects [4]. The resulting system is considered safe if the residual risk is acceptable [4]. This approach places potential failure in the centre of the safety consideration, requiring for the implementation of additional safety measures for identified potential failures that do not meet the acceptance criterion. This commonly results in an increase in system complexity, which might introduce additional risks into the system. Furthermore, general functional safety for the employed hardware architecture is not defined, so that an iterative process is used [2], [4], [5], which potentially requires a significant amount of development time and resources.

For the automotive industry the standard series ISO 26262-(1-12) [6] defines the requirements and processes for the development of functional safety in road vehicles. The goal is thereby to prevent hazardous situations, independent of concrete failures. The standardized process leads to the development of industry spanning safety architectures for certain functions of the car. The EGAS concept for engine control systems developed by the automotive industry is a technical solution to develop a functionally safe hardware architecture [8]. It is well established and proven in the automotive industry [3]. Therefore, we propose the adaption of the EGAS concept for medical devices. Before introducing the EGAS-concept and applying it on the open access pandemic "High Energy particle physics Ventilator" (HEV), we will give a brief comparison between the different risk managements procedures.

2 Medical device standard and automotive standard

In order to ensure an acceptable residual risk, a proper risk management process is required [4] in accordance to EN ISO 14971 [1]. According to the "integrated safety" principle, Medical Device Regulation (appendix I, section 4), the following steps have to be performed: (1) reduction of risk by design, (2) integration of risk mitigation measures and (3) communication of residual risks [5]. The risk acceptance criterion is the combination of the probability and the severity of a potential harm, whereby the benefits must outweigh the risks [1].

*Corresponding author: Benjamin Alexander Paulsen:

Fraunhofer IMTE, Mönkhofer Weg 239a, Lübeck, Germany, email: benjamin.paulsen@imte.fraunhofer.de

Sandra Henn: Institute for Electrical Engineering in Medicine, University of Lübeck, Lübeck, Germany

Georg Männel: Fraunhofer IMTE, Lübeck, Germany

Philipp Rostalski: Fraunhofer IMTE, Lübeck, Germany and Institute for Electrical Engineering in Medicine, University of Lübeck, Lübeck, Germany

Figure 1: Graph which is used to determine the correct ASIL class of a hazard circumstance during risk management of the automotive standard. Figure based on [7].

For the risk evaluation, the sources of possible harm have to be listed and for each single source of failure, a probability for and severity of harm has to be determined. If it is determined that a risk is too high, control measures have to be defined to reduce the risk. After carrying out these measures, all sources of potential failures have to be assessed again and the probability and severity have to be readjusted. This process has to be repeated until the remaining risk is acceptable [1], [4].

In contrast the automotive standard (ISO 26262-(1-12)) aims to define functional safety as the reliable performance of all safety functions for road vehicles [6]. The risk management of the automotive industry uses a graph with a well-defined structure which leads to ASIL (Automotive Safety Integrity Level) classes [6]. An ASIL class is determined for every possible hazard circumstance. More severe risks, where lower probabilities of a damage can be tolerated, require a higher ASIL class and vice versa. If no ASIL class has to be selected, quality management (QM) is sufficient. An ASIL class demands a maximum permissible failure rate. Therefore, this results in defined safety goals, which must be achieved. An ASIL class is chosen according to the graph shown in Figure 1. In contrast to the medical device standards, the approach considers hazard circumstances and not individual sources of harms, thus potentially streamlining the risk management process by focusing on individual hazard circumstance, than on every individual source of harm.

3 Architecture of the EGAS concept

The following account of the architecture of the EGAS concept is based on the work of Nägler et al. [8]. The monitoring concept relates to a system which consists of three main components – sensors, actors and a functional computer.

Figure 2: 3-level monitoring concept of the EGAS architecture. Figure based on [8].

The sensors are designed redundantly and used to monitor all relevant physical units. The functional computer is used to compare the redundant sensors for consistency, to safely control the actuators and to recognize any errors during operation of the sensors and actuators. This computer is monitored by a smart watchdog to ensure the correct functionality. The necessary process steps to develop the monitoring system are:

1. System definition
2. Definition of the system to be secured
3. Hazard and risk analysis
4. Definition of safety goals
5. Monitoring concept to meet the safety goals

The first step contains the listing of all components and functionalities of the system. After the listing process the components and functionalities are linked to each other related to their interaction. In the second step, this list is reduced to the components and functionalities which are safety critical and relevant for the EGAS monitoring concept. The third step contains hazard and risk analysis, which determines the possible hazard circumstances. For this purpose, the ASIL classes are determined analogously to the ISO 26262-(1-12). In the fourth step, for every hazard circumstance a safety goal is defined, which is connected to their ASIL class. In the last step, the monitoring (see Figure 2) concept is developed which will be presented in the following.

In total the concept comprises of three levels – a function level (level 1), a function monitoring level (layer 2) and a

computer monitoring level (level 3). If an error occurs, every level can trigger an error reaction and the system is controlled into a safe state. In level 1 the values of the redundant sensors are compared and the actual signal is calculated. An error reaction is triggered, if the sensor signals deviate. In level 2 the correct functionality of level 1 is evaluated by comparing the actual value with the pre-set signal. If the actual signal is not valid, an error reaction is triggered. Level 3 is divided in the monitoring software of the functional computer and the physically independent smart watchdog. The smart watchdog uses a pool of defined questions to ask the monitoring software in fix time periods, if the program flow control and the instruction set of the calculation core work correctly. Both answers are linked and send to the watchdog which checks the correct content of the answer and the arriving time. If the answer is incorrect, the watchdog asks the identical question again. If the incorrect answer is repeated, an error reaction will be triggered. Level 2 memory is also tested by level 3 monitoring software but independently from the watchdog. Moreover, the monitoring software monitors the smart watchdog by checking the time window of arriving questions and deliberately returning wrong answers.

4 Adaption of the EGAS concept

In order to investigate the adaptation of the concept to a medical device, the HEV [9] is used as a demonstrator. The HEV ventilator described in full detail in Buytaert et. al. [9] was developed during the COVID-19 pandemic to address the shortage of low and mid-priced ventilators. Due to its open design, the system is an ideal basis for scientific research and will be used for assessing the applicability of the EGAS concept in the medical device industry. Since the safety-critical part of the HEV is relevant for the application of the EGAS concept, the following refers to the pneumatic unit (see Figure 3), where automatically regulated parts are marked in green and manually controlled parts in orange.

The buffer is the central component of the pneumatic unit. Via two supply lines, O₂ and air are fed into the buffer with the aid of valves and pressure regulators. The pressure sensors (denoted with “P”) monitors the pressure of the supply and regulated lines. The buffer is filled with the gases until a desired pressure is reached. Thus, the gases are mixed and a desired oxygen concentration can be achieved. The mixed gas is supplied to the oxygen sensor and the patient via the inhale valve. The used gases are discharged via the exhale valve and passed through the PEEP (Positive End Expiratory Pressure) valve. In addition, the CO₂ content in the expired air is measured. With the help of the pressure sensors for the inhale and exhale gases, both the parameters for regulated ventilation are calculated and the safety-relevant pressure in the inhale

Figure 3: Simplified architecture of the pneumatic unit of the HEV. Figure based on [9].

and exhale lines to the patient is measured. To protect the patient from overpressure, a mechanical buffer relief valve and an inhale relief valve protects the patient. An electronically controlled purge valve also opens, if the pressure sensor of the buffer measures an overpressure. The built-in non-return valves ensure – with one exception – that an unintentional backflow of gases cannot occur. The inhale guarantee valve, however, ensures the supply of air in the event that the inhale valve should fail. After all components and functionalities of the system are listed and linked to each other (first step), the list is reduced to the safety critical part of the HEV (second step). In relation to the pneumatic unit, the EGAS system contains three main components: input for the pre-set signal (set by the clinician), functional computer for the safety critical ventilation control and actuators for the safety critical ventilation. For the HEV the actuators for the safety critical ventilation are the inhale valve, exhale valve, purge valve and PEEP valve. Examples of possible hazard circumstances and the related classifications are given in Table 1 (third step). The main difference in this classification for a medical device in contrast to an automotive system is, that there is no driver operating a vehicle, but a clinician operating the HEV, as well as a patient being ventilated. The safety goals (step 4) correspond to the prevention of the hazard circumstances listed in Table 1. In the last step, the monitoring system is developed according to the monitoring concept of the previous section (see Figure 4).

Accordingly, the safety-relevant sensors will be designed redundantly and connected to the functional computer. The safety critical sensors are both the pressure sensors for inhale, exhale and buffer as well as the gas concentration sensors for O₂ and CO₂. The inhale and exhale sensors are selected because they monitor the pressure of the gas produced in the vicinity of the patient. The buffer pressure sensor is also selected because in the event of a malfunction, an overpressure

is created which can only be relieved by the mechanical relief valves or regulated down by the inhale valve. These valves alleviate the overpressure to a large degree, but may not completely avoided a harmful overpressure to be applied to the patient. The gas concentration sensors are relevant for the control of the correct gas concentration for the patient, therefore these must also be implemented in a dual-channel configuration.

According to the EGAS concept, there must also be a functional computer and smart watchdog, which monitor both the functionality of the sensors and each other with regard to correct functionality. Moreover, they have to be capable of initiating error reactions (see Figure 4) when facing errors. The monitoring system developed for the HEV can then be implemented using dedicated safety hardware such as the Infineon AURIX system [10], showing the applicability of the proposed approach in the medical device industry.

Table 1: ASIL classifications of possible hazard circumstances.

Hazard Circumstance	S	E	C	ASIL
Increased Respiratory Rate	3	4	3	D
Decreased Respiratory Rate	3	4	3	D
Increased Pressure	3	4	3	D
Decreased Pressure	3	4	3	D
Increased Volume	3	4	3	D
Decreased Volume	3	4	3	D
Pneumatic Unit Failure	3	4	1	B

5 Conclusion

Investigating the similarities and differences in the regulatory landscape between different industries, in particularly in terms of functional safety potentially offers promising synergies for the medical devices industry. By applying well-established concepts from the automotive sector such as the (adapted) EGAS concepts to medical devices, readily available tools and methods may be reused and adapted. Albeit the differences in the regulatory landscape and the various open issues, the EGAS system offers an attractive alternative approach for functional safety of medical devices, as shown in this article and demonstrated by means of the HEV ventilator. Challenges and advantages in terms of hardware and software as well as in the applicability of the general methodology will be further investigated in future research projects.

Figure 4: EGAS monitoring concept for the HEV.

Author Statement

Research funding: This work was supported by European Union – European Regional Development Fund, the Federal Government and Land Schleswig-Holstein, Project: “Diagnose- und Therapieverfahren für die Individualisierte Medizintechnik (IMTE)”, Project No. 12420002 as well as the “Cross-Innovation-Center - TANDEM Phase III”, Project No. 124 20 003. **Conflict of interest:** Authors state no conflict of interest.

References

- [1] EN ISO 14971:2019-12 Medical devices — Application of risk management to medical devices. 2019.
- [2] Metzger J, Reinhardt P. (2013, January 10). Funktionale Sicherheit bei Medizinprodukten. DeviceMed. Retrieved July 12, 2021, from <https://www.devicemed.de/funktionale-sicherheit-bei-medizinprodukten-a-390462/>.
- [3] Groschmann M, Hirz M, Fabian J. Efficient application of multi-core processors as substitute of the E-Gas (Etc) monitoring concept. SAI Computing Conference 2016: 913-918.
- [4] IEC 60601-1:2005-12 Medical electrical equipment - Part 1: General requirements for basic safety and essential performance. 2005.
- [5] Medical Device Regulation (EU) 2017/745 (Appendix I, Section 3-4). 2017.
- [6] ISO 26262-(1-12):2018-12 (Road vehicles — Functional safety), ISO, 2018.
- [7] Funktionale Sicherheit (FuSi) – die ASIL-Klassifikation. (n. d.). Retrieved on 5. July 2021, by <https://www.i-q.de/iso-26262/fusi-asil-klassifikationen>.
- [8] Nägler, Kranawetter, Strobl, Rehm, Staib, Veldten. Standardisiertes EGAS Überwachungskonzept für Benzin und Diesel Motorsteuerungen Version 6.0. 2015.
- [9] Buytaert J, Abud A, Allport P, Álvarez A, Akiba A, Francisco O, et al. The HEV Ventilator. 2020.
- [10] 32-bit AURIX™ TriCore™ Microcontroller. (n.d.). Infineon Technologies AG. Retrieved July 12, 2021, from <https://www.infineon.com/cms/de/product/microcontroller/32-bit-tricore-microcontroller/>.