Dive Computers:
The Need for Validation and Standards

Arne Sieber
Milena Stoianova
IMEGO AB
Arvid Hedvalls Backe 4
P.O. Box 53071
SE-40014 Göteborg, SWEDEN

Ewald Jöbstl
QM- Jöbstl
Gritzenkogel 6
8052 Graz, AUSTRIA

Elaine Azzopardi
Martin D.J. Sayer
NERC National Facility for Scientific Diving
Dunstaffnage Marine Laboratory
Oban, Argyll, SCOTLAND PA37 1QA, UNITED KINGDOM

Matthias F. Wagner
Frankfurt University of Applied Sciences
Nibelungenplatz 1
D-60318 Frankfurt, GERMANY

Dive computer validation is currently a widely discussed topic for which there is no uniform procedure for testing and validation. Many dive computer manufacturers claim that their products are personal protective equipment. However, dive computers are not listed in the directive for personal protective equipment (PPE Directive 89/686/EEC). EN13319 is one European normative that is frequently applied during CE certification of dive computers. This normative only addresses accuracy and precision of depth sensor and built-in clock/timer – decompression calculations are explicitly excluded from the standard. This overview of normatives and standards suggests those that might be applicable for dive computer validation. The concept of functional safety is discussed. A short market survey is included which presents how dive computer manufacturers certify their CE products. Validation and testing of a dive computer is also of utmost importance for liability considerations, because they are used for decompression planning and, as such, can be classified as personal protective equipment category III. We provide these considerations on dive computer validation for a new tailored normative or standard that will harmonize worldwide dive computer testing and validation procedures and lead to a higher functional safety of these devices.

INTRODUCTION

Over the past two decades dive computers (DCs) have become almost universally accepted in the recreational diving sector for the management of decompression. In fact, many dive centers now may not accept customers who do not use a dive computer. The permissible use of DCs in commercial diving varies between countries and industry sectors. However, many countries currently legislate against their use for commercial diving possibly because of a present lack of information on many computer models as to how they compute decompression. This, in turn, may promote a perception of a lack of dependable safety. This uncertainty is difficult to counter, mainly because there are no standards or normatives specifically for DCs that would allow an assessment of their functional safety. This paper does not compare different decompression models; instead it reviews the available normatives, standards and directives, their implementation by certain manufacturers, and the functional safety of DCs in general.

DIVE COMPUTER EVOLUTION

During the period of diving where decompression theory became better understood and the first decompression tables were developed (e.g., Boycott et al., 1908), divers were surface-supplied and their decompression monitored by a surface crew. In the mid-1940s, self-contained underwater breathing apparatus (scuba) developed and allowed divers to become independent from the surface. Divers then also became responsible for the monitoring and control of their decompression obligations. This introduced new levels of complexity compared to traditional hardhat diving because divers could now move freely in a three-dimensional space, frequently resulting in multilevel dives.

Initially divers used tables, depth gauges and bottom timers as tools to monitor their decompression status. Such tables were used for no-decompression diving, where an immediate and safe return to surface was possible. Once the no-decompression times were exceeded, staged decompression stops had to be included during ascent. When it came to repetitive multilevel diving, using tables effectively became impossible because of the inability to calculate accurately the decompression debt for a near infinite number of possible profile combinations. In order to address this, repeat tables tended to base calculations on the maximum depth achieved during the dive series; as a result, the subsequent dives carried heavy time penalties, either resulting in excessively short diving times or requiring a long surface interval in order to return to a single dive decompression schedule.

The early history of DCs was reviewed by Huggins (1989), who described the developmental process from commissioning of the first DC by the U.S. Navy in 1951, through to the 1980s where commercially available units ran on similar hardware and were recognizable with those DCs in use today. Nearly all DCs available today are able to perform calculations with enriched O_2 gas mixtures. Some can be also used with trimix and many modern computers have the facility to program several gas mixtures into the dive plan. More sophisticated DCs include additional features like a compass, an integration of cylinder pressure read out (either by hard connections or, in some cases, wireless), a color display and mixed-gas decompression schedules. A more detailed summary of the dive computer evolution can be found in Bourdelet (2007).

Lang and Angelini (2009) described the future of DCs. A summary of features that they identified as of interest from the diving physiology point of view included the measurement of heart rate, skin temperature, O_2 saturation (Kuch et al., 2010) and inert gas bubble detection. Some recently introduced models are also equipped with color screens, while some are incorporated in the diving mask with heads-up displays (Datamask, Oceanic, US) (Koss et al., 2011). In the future, navigational aids will include underwater geo-referencing (Kuch et al., 2009; Gamroth et al., 2011; Kuch et al., 2011).

In 1988, a dive computer workshop examined the safety of DCs, their evaluation and the guidelines for their use (Lang and Hamilton, 1989). More specifically, the topics discussed included which decompression models should be used, how validation should be carried out, what are the acceptable risks, what limits should be given for DCs, what should happen in the case of a DC failure and operational reliability. Even 23 years later, most of these questions are still not answered for past or present DC models, and still form the basis for study.

As early as 1988 it was pointed out that standardization of DCs would be ideal (Osterhout, 1989) and suggested for:

1. the type of information displayed;
2. the manner in which the information is displayed;
3. the manner in which information is recalled;
4. the decompression models employed; and,
5. a uniform means of telling when a computer is in a failure mode.

The testing of the initial analog DCs was relatively straight forward, as there were rather simple means to check for correct function. This could include hyperbaric testing or, for example in the case of an analog pneumatic pure mechanical design, testing for correct gas diffusion rates. In the age of the microcontrollers, the situation became more difficult (Sieber et al., 2010). Hardware testing is a relatively easy task, as simple tests are usually sufficient to prove the correct function, however the critical point is how to standardize software. With the increasing amount of features, the complexity of dive computer software increases exponentially. The first electronic DCs had simple algorithms and data output; the latest ones have many advanced features like graphic color screens, large memory, compass, etc. and current trends are driving towards the development of real-time operating systems running on the microprocessor. In addition, with the increasing use and development of DC features run and controlled by software there comes an increasing risk of failure of one or more of the components so software testing efforts have to increase.

DIVE COMPUTER SAFETY

When considering the best and safest DC, reviewers mainly address its features and implemented decompression model. If one compares different DCs directly, one might expect to witness different readings: for example, one computer might indicate that a diver is still within no-decompression limits and can safely return to the surface without decompression stops, while other computers using a different model to calculate the decompression might show a ceiling warning and require stops (Huggins, 2012). However, given these differences, it then becomes difficult to comprehend that all of the computers on the market could be correct and provide a similar level of decompression protection if, and when, they give such wide-ranging outputs. It is important then to understand that each decompression algorithm carries a certain level of risk for DCS. Therefore, it is too simplistic to say one computer is right and the other wrong; rather the more conservative computer has a lower probability of DCS (pDCS). If one compares the pDCS for a variety of dive profiles, a few minutes more or less on a dive within recreational limits does not change pDCS to a large extent and in some circumstances could be ignored.

In a recent study to compare the features of DCs, they were tested in a hyperbaric chamber and the depth readings (i.e., the computer depth interpretations of the measured pressure) were compared (Azzopardi and Sayer, 2010; 2011), while Denoble (2010) wrote a popular article about DCs and decompression safety.

However, the aim of the present paper, is not to look at different decompression models of DCs and decompression safety, but to examine the functional safety of such devices and describe the normatives and directives that are available to give guidance throughout the development, validation and certification process of a dive computer.

Is a dive computer a safety-critical system?

An important question in this respect is whether a dive computer is a safety-critical system or not. A DC gives information about the dive depth and the dive time but also suggests how to perform a dive, i.e., when to ascend, ascent rate, and the decompression schedule to follow. While technical divers and commercial divers tend to use tables, depth gauges and timers to carry out dives, recreational divers value the advantages of DCs that provide continuous tracking of tissue tensions and are able to calculate decompression schedules with wide flexibility such as for multilevel or repetitive dive profiles. These divers often dive and ascend according to the DC indications. It is obvious that if incorrect indications given to the diver, DCS, or in worst case, even death, can occur.

Therefore, the answer should be that a dive computer is a safety-critical system. This conclusion is also strengthened by a large number of manufacturers categorizing their DCs as personal protective equipment (PPE).

Obvious versus non-obvious failures

One might argue that for redundancy purposes a diver should always carry backup instruments, i.e., a timer, a depth gauge and a table, or a second dive computer, to be able to safely surface in the case of a failure of the primary dive computer. This is a good approach but can only be usefully applied if a failure of a dive computer is recognized by the diver (see Osterhout comments above).

One fundamental point in functional safety is that a failure should be obvious to the diver, so that he/she can take appropriate measures. If a failure remains undetected, the consequences can be serious. An example of a way in which such a non-obvious failure could occur is given thus: if battery life is not sufficient at the start of a dive, then it could cause resetting of the DC so displaying an incorrect total dive time and therefore an incorrect decompression. Another example might be that the DC is programmed to calculate decompression using a different percentage gas to that actually used, which would obviously have a large impact on decompression safety. There are many permutations of DC use/failure that may fall into this category of non-obvious risk unless precautions are taken to make sure it cannot happen.

Functional safety

Functional safety is part of the overall safety relating to the system under development. Safety in general is an emergent property of a system that must not endanger human life. The safety of system components, hardware and software alone is meaningless. In most cases reliability is a necessary prerequisite for safety. Therefore, design methods of reliability engineering are not sufficient for the design of safety critical systems (Leveson, 1995). Applied to DCs functional safety not only means that the device performs according to the requirements, but also that in case of a failure, no harm occurs.

CE certification of DCs

CE marking introduced by European Community legislation is a key indicator of a product's compliance with the EU legislation requiring the protection of the public interest by having safe, healthy and reliably functioning products in the common market. Two types of standardization requirements apply to specific product groups. First, the New Approach Directives set up mandatory basic safety requirements for expressly listed groups of products that need to be CE certified. Where a CE certification is required for a certain product category, the manufacturer is under the legal obligation to carry out assessment of that product with the Directives' requirements. The second set of requirements is found in the so called "harmonized standards" adopted by the European Standards Organization that bear the designation "EN" before the standard number. While the Directives are binding on the manufacturer as to the hazards to be addressed and the outcome to be achieved, the harmonized standards are voluntary but they detail the technical means for verifying compliance with the safety and health requirements of the Directives and therefore are largely complied with by the industry.

In agreement with the preceding argument, DCs are indispensable means to ensure the health and the safety of divers. However, DCs as a product do not fall into any of the broadly formulated product groups covered by the Directives that require CE certification. Certification of DCs is needed because several of their key components need to be CE certified. Therefore, certification of DCs is made according to several Directives and EN standards that will be briefly described below.

The CE certification of a DC occurs in several stages. First, it is the manufacturer's responsibility to correctly identify the set of standards that the product has to meet. Having done that, in a second step, the essential product-specific requirements need to be identified and the assessment of conformity with them planned.

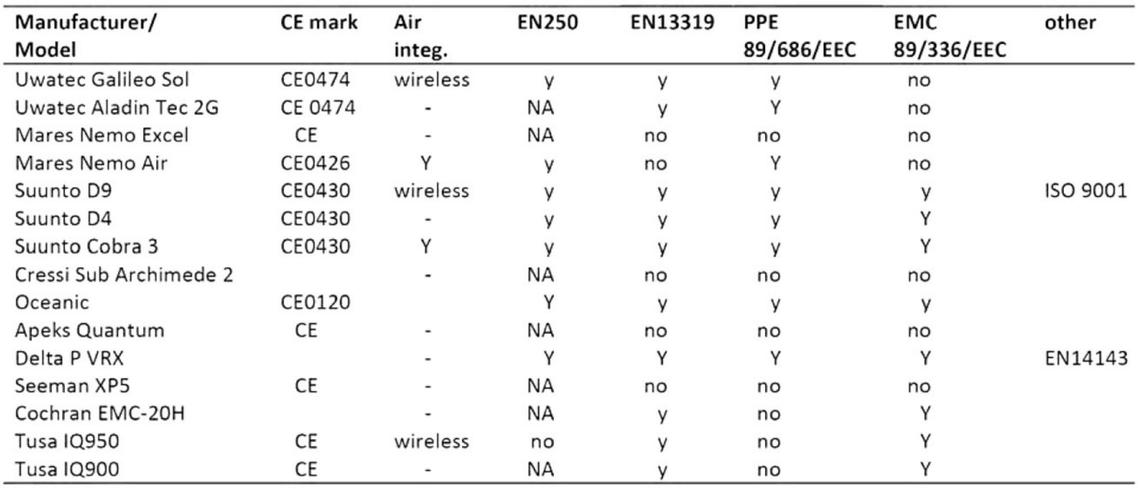
An intrinsic part of the CE marking process is the testing of the DC and the conformity of the parts covered by the Directives with the legal requirements for their safe functioning and use. Risk assessment is a key component of the assessment stage. It is at this stage that the manufacturer has to verify via the Directive whether for compliance certification a "Notified Body" has to be involved or not in order to reach compliance certification. Such certification by a third party is required for certain products that are likely to seriously endanger or affect the public interest from a health and/or safety perspective. However, ultimately the manufacturers affix the CE marking to their products, thereby assuming the sole responsibility for standards compliance. Thus, in case of a diving accident, the manufacturers will be held liable for the faulty performance of their product or component parts thereof.

Performing the tests does not complete the CE certification process. The manufacturer also needs to draw up technical documentation detailing the checks performed and the results obtained. In case of an accident, this documentation will serve as evidence of conformity with the essential safety requirements and will make it possible to identify the cause of the accident to the equipment or to the diver.

A visual inspection of the DCs sold in the European Economic Area and their user manuals (Table 1) shows that only one manufacturer wholly complies with the requirements for CE certification and carries out checks for conformity with all relevant directives and harmonized standards. The safety of DCs is not guaranteed to the full extent because of two types of omissions made on the part of the manufacturers. First, some manufacturers confine their tests to a number of Directive requirements, then fail to perform tests on crucial parts covered by other Directives.

For example, the EN13319 and the Electromagnetic Capability (EMC) directive, which should be used when certifying a dive computer, are only referenced by a few manufacturers. Some manufacturers categorize their dive computer as PPE, even though this is not mandatory and is only applicable where a cylinder pressure gauge is included within a DC, whereby it then needs to be tested according to EN250 and thus falling under the PPE directive. Most manufacturers of DCs with air integration follow the directive and categorize their devices as PPE. Some of them, however, state explicitly that the directive for PPE is applied solely to the cylinder pressure gauge (e.g., Mares). It is important to note that in the case where a manufacturer declares a DC as PPE, it falls under category III, which means that for CE certification a Notified Body has to be involved.

Table 1. Visual inspection of some DC models and their manuals for CE mark and normative/directive compliance (NA: not applicable).



Manufacturer/ Model	CE mark	Air integ.	EN250	EN13319	PPE 89/686/EEC	EMC 89/336/EEC	other
Uwatec Galileo Sol	CE0474	wireless	y	y	y	no	
Uwatec Aladin Tec 2G	CE 0474	-	NA	y	Y	no	
Mares Nemo Excel	CE	-	NA	no	no	no	
Mares Nemo Air	CE0426	Y	y	no	Y	no	
Suunto D9	CE0430	wireless	y	y	y	y	ISO 9001
Suunto D4	CE0430	-	y	y	y	Y	
Suunto Cobra 3	CE0430	Y	y	y	y	Y	
Cressi Sub Archimede 2		-	NA	no	no	no	
Oceanic	CE0120		Y	y	y	y	
Apeks Quantum	CE	-	NA	no	no	no	
Delta P VRX		-	Y	Y	Y	Y	EN14143
Seeman XP5	CE	-	NA	no	no	no	
Cochran EMC-20H		-	NA	y	no	Y	
Tusa IQ950	CE	wireless	no	y	no	Y	
Tusa IQ900	CE	-	NA	y	no	Y	

For example, in the manual of their recently launched DC model IQ-950, the manufacturer TUSA notes that the CE mark is used to identify conformity to the EMC directive 89/336/EEC and is designed to comply with EN13319. However, this dive computer also features air integration and so should also be certified according to EN250; it therefore falls under the PPE directive.

However, manufacturers often wrongly seek compliance with requirements for a product that they do not integrate in their DC. Suunto references EN250 for their D4, even though no cylinder pressure gauge is included and so does not fall under the umbrella of PPE. It is also interesting to note that only a few manufacturers state compliance with EMC directive 89/336/EEC, even though this is mandatory, and in cases where a wireless cylinder transmitter is included, a Notified Body has to be involved. Oceanic does not provide information about CE and normative/directive compliance in the manuals, but do that in a separate document that is valid for all of their DCs.

DIVE COMPUTER CERTIFICATION: STANDARDS AND NORMATIVES

Applied standards

As discussed, there are several standards applied to DCs today, however, there is no standard written specifically for DCs to meet. In general, there are no obligatory guidelines to follow, nor are there any suggestions concerning validation of DCs. As previously noted, it is only when a DC is integrated with a cylinder pressure gauge that it has to be certified according to EN250 and the PPE Directive become mandatory.

The EMC Directive (89/336/EEC)

Like the PPE Directive, the EMC Directive intends to establish a free movement of goods within the EC, hence providing an environment for reliable operation of electrical and electronic equipment. This Directive covers nearly all electrical and electronic appliances and requires that it neither causes excessive electronic interference nor is unduly susceptible to it. It provides for harmonizing legislation to ensure that standards adopted throughout the EC are compatible. Equipment must be manufactured so that it does not generate a level of disturbance that will prevent other equipment from operating properly and does not itself suffer from interference. In cases where radio transmitter/receivers are included, like in a DC with a wireless cylinder pressure transmitter or featuring a Bluetooth-based PC interface, the DC must be subject to an EC-type examination by a Notified Body. The EMC directive also provides that the device be properly CE marked.

EN250:2000

EN250:2000 is a standard for respiratory equipment and includes the use of open-circuit, self-contained, compressed-air diving apparatus. Requirements, testing and CE marking fall under the PPE directive. In general, the standard mainly addresses breathing regulators but it also covers cylinder pressure gauges which, referring to section 5.8.1, are considered to be part of the respiratory equipment. Within section 5.8.2 of that standard, the required accuracy and measurement range of a pressure gauge is addressed.

EN13319:2000

EN13319:2000 addresses depth gauges and combined depth and time measuring devices and as such provides functional and safety requirements and test methods. Chapter 4.1 deals with depth and 4.2 with time measurement. This standard suggests using a gauge factor, where 1 bar pressure correlates to 10 m depth [4.1.1]. Chapter 4.2 addresses accuracy of time measurement and specifies how the dive time is measured by providing a threshold depth of 1.6 m for automatic dive time counting start and stop. Further topics that are within the scope of this standard are, for example, water-tightness, sea water resistance, and operability.

Information on decompression obligations displayed by equipment covered by the standard is explicitly excluded from its scope [EN13319:2000, 1]. This standard also refers to ISO1413: Horology – shock-resistant watches. The standard was prepared by the CEN/TC136 group for “Sports, playground and other recreational equipment.” Many manufacturers categorize their DCs as PPE, thus it is interesting to note, that EN13319:2000 is not listed in the official journal of titles and references harmonized standards under Directive 89/686/EEC for PPE.

PPE Directive 89/686/EEC

One main aim of this directive is to harmonize products by ensuring a high level of protection and safety for citizens in specific circumstances and free circulation throughout Europe. The PPE Directive is ratified by each country in Europe. For the CE certification of Category III PPE a Notified Body is mandatory. All Notified Bodies are listed on the European Commission’s New Approach Notified and Designated Organizations (NANDO) Information System.

The Directive on PPE aims to harmonize and streamline existing national requirements on PPE and establishes a minimum set of standards to ensure the safe use of equipment. The provisions governing the design and the manufacture of PPE are considered fundamental to the achievement of its aim and they should be distinguished by any national or Community rules that relate to the use of such equipment. Therefore, compliance with the PPE Directive is a stepping stone and absolute prerequisite for safety. The Directive and the related normatives create an obligation for PPE manufacturers to duly test the reliability of their products prior to marketing and sale, and to inform the consumer of having done so by placing correct CE marking on each individual appliance.

Article 8 brings together PPE covered by the Directive into three distinct groups and their relevant conformity assessment procedures: Simple designs (Category I), neither simple nor complex designs (Category II) and complex designs (Category III). For category II and III a Type examination by a Notified Body is required. Further category III products also require a quality control system for the final product and a production-quality monitoring system.

Many parts of diving equipment fall under the PPE directive and need to be tested according to underlying normatives: Examples are respiratory equipment (EN250:2002), buoyancy compensators (EN1809:1999), combined buoyancy and rescue devices (EN12628:2001), respiratory equipment for compressed nitrox and oxygen (EN13949:2004) and rebreathers (EN14143:2004) or drysuits (EN14225-2:2005).

Surprisingly, DCs, which are used by many divers as indicators for decompression obligations and used to perform a decompression schedule or stay within the no-decompression limits, are not listed in the PPE directive under section 3.11 - additional requirements specific to particular risks – safety devices for diving equipment.

ISO9001 compliance is often stated by DC manufacturers. ISO9001 is a general quality assurance standard that addresses the control of the quality of general development and production. However, it is not a specific safety standard, nor does it take into account the complexity of software development.

The need for a consolidated DC safety standard

As a rule, CE marking certifies compliance of a product as a whole with the essential safety and health requirements of the Directives that require CE marking. It is beneficial for consumers as it boosts their confidence in the products circulating within the common market and creates trust that corporate compliance and control procedures are in place and functioning. This leads to growth of the markets and to consumer satisfaction.

CE marking of the DCs currently on the market only partially tells the consumer the real story. It creates the wrong impression that the DC as a whole is CE tested and certified but this might not always be the case. Therefore, there is a need to unify the requirements for safety performance of DCs as a whole.

At the same time, CE marking creates the rebuttable presumption that the products on the market satisfy the safety requirements of the Directives and thus, irrespective of incomplete safety checks, in the case of diving accidents the presumption shifts the burden of proof of non-conformity and non-reliability of the DC from the producer to the consumer. As standard compatibility assessment of DCs is rarely described in detail in the user manuals, it might be unreasonably difficult for a non-technically trained diver to successfully plead his case in court. Thus a consolidated standard for DC safety should level the playing field between manufacturers and consumers.

CE marking and compliance also impacts on competition between the DC manufacturers. CE self-assessment and verifications by a Notified Body account for considerable costs in the value chain of the final product. This results in higher manufacturing costs and higher consumer prices. Non-compliance with CE Directives safety requirements constitutes a competitive advantage in terms of lower costs and better final prices. This, however, comes at the cost of divers' health and safety and is unacceptable.

Protection mechanisms from non-CE certified products

Protection exists against products that do not meet the CE Directives on safety and health requirements. It takes the form of control conducted by the competent national authorities and where non-conformity is found the circulation of the product in the EEA area might be prohibited and the products withdrawn. This can be coupled with fines and in some Member States like the UK, for example, depending on the gravity of the violation, imprisonment might be likely.

DCs AS SAFETY-CRITICAL SYSTEMS

As a DC gives may give an indications as how to handle decompression obligations and, in the case of malfunction, has the potential to endanger human life, it is evident that DCs are typical safety-critical systems (SCS). Some manufacturers seem to share this opinion and already categorize their DCs as PPE.

For most it is accepted that DCs are SCS with typical challenges with respect to their development (Leveson, 1995, 2004; Knight, 2002; Hollnagel et al., 2006). The increasingly important directive that is lacking in terms of DC development is that of comprehensive safety standards.

A dive computer is an active system, subject to functional safety requirements as defined by the IEC61508 standard. This standard had been designed originally as an application-independent standard that could spawn industry-specific derivative standards. One of its major strengths is the focus on safety as a system issue (Herrmann, 1999). The main mechanism through which IEC61508 enhances safety of a system is risk reduction.

IEC61508 is a meta standard and, as such, does not give direct guidelines on testing like EN250 or EN13991, which are very specific in their recommendations. The standard describes a general development life cycle required for building a safe system. The general life cycle defined in the IEC61508 standard covers all major issues of a system composed of hardware and software (Figure 1).

For example, in aviation, space applications or in nuclear power stations, SCS often comply with EN61508. However, they do so by complying with specific standards, which are derived from EN61508. Such a specific interpretation of EN61508 is necessary in order to map the peculiar requirements of a certain field on the development life cycle.

In EN14143:2004, a standard for rebreathers, compliance with EN61508 is required. However, because of the broad nature of this meta standard and the lack of more specific tailoring to the application field, the standard is rarely, if at all, applied. As a consequence, the CEN/TC79 committee is presently discussing removing EN61508 from EN14143, which makes CE compliance easier to achieve for manufacturers, but is clearly a step back from what concerns mandatory functional safety.

When revisiting consideration of DCs as safety critical systems, EN61508 could work as a tool to accomplish functional safety but, similarly to the example above, a direct application without tailoring is not practical and/or will lead to various interpretations by manufacturers. This is, however, contrary to one of the PPE directives' main aims focusing on harmonized standards. A tailored version of EN61508 addressing DCs should, rather than providing only measures and guidance to test a final product, define a comprehensive life cycle. Further, it has to be taken into account that compared with development teams in the aerospace, nuclear or automotive industries, development teams for dive computer systems are comparatively small. Therefore, an adaptation of the IEC61508 towards development efforts of SCS in small groups is essential.

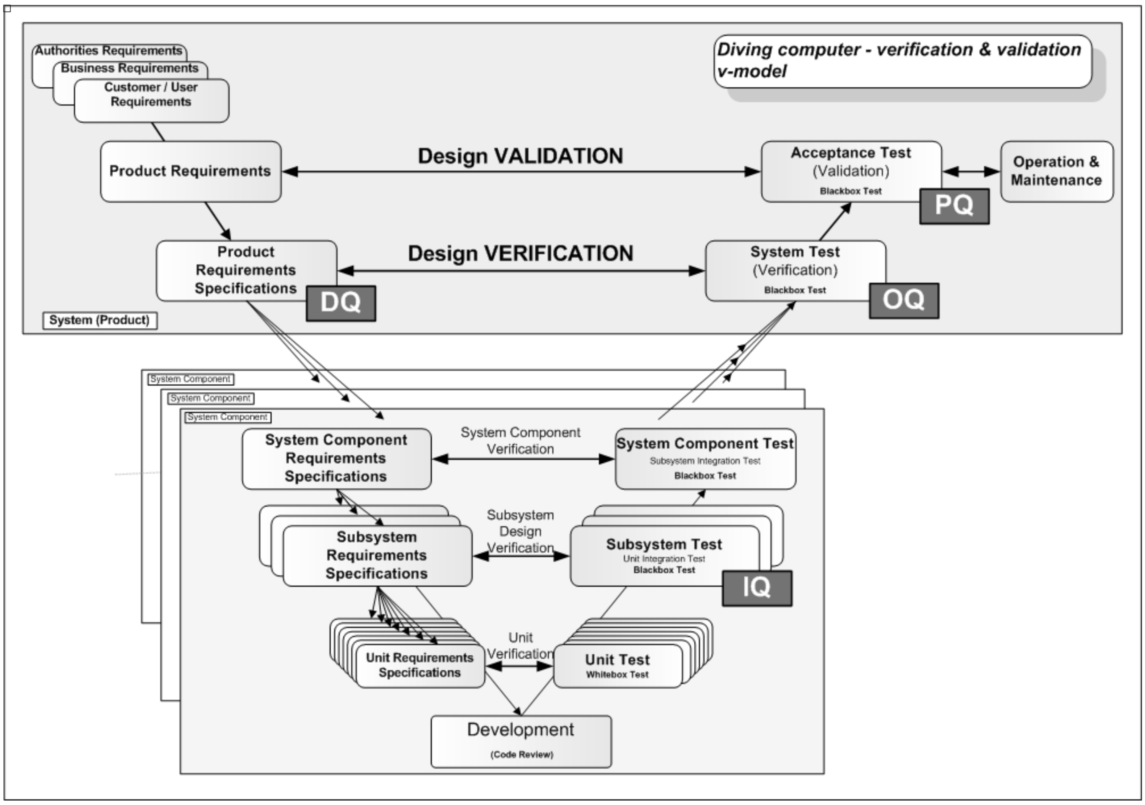

Diving computer - verification & validation v-model
Authorities Requirements
Business Requirements
Customer / User Requirements
Product Requirements
Design VALIDATION
Acceptance Test (Validation) Blackbox Test
PQ
Operation & Maintenance
Product Requirements Specifications
DQ
Design VERIFICATION
System Test (Verification) Blackbox Test
OQ
System (Product)
System Component
System Component
System Component
System Component Requirements Specifications
System Component Verification
System Component Test
Subsystem Integration Test
Blackbox Test
Subsystem Requirements Specifications
Subsystem Design Verification
Subsystem Test
Unit Integration Test
Blackbox Test
IQ
Unit Requirements Specifications
Unit Verification
Unit Test
Whitebox Test
Development
(Code Review)

Figure 1. Validation and verification using the V-model.

DCs COMPARED TO MEDICAL DEVICES

Compared with other products on the market, DCs bear a strong resemblance to medical devices. Medical devices are similar to DCs with regards to combinations of hard and software and the high risk involved through influencing life-threatening decisions. In contrast to DCs, medical devices have to fulfill a variety of standards to ensure safety for the patient and the user. Key documents are:

- 21CFR Part 820 Quality System Regulation (Medical Devices);
- EN/ISO13485:2003 Medical devices - Quality management systems - Requirements for regulatory purposes;
- IEC62304 Medical device software - Software life-cycle processes;

- ISO14971:2007 Medical devices - Application of risk management to medical devices;
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff January 11, 2002; and,
- GAMP5 Good Automated Manufacturing Practice Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture.

Quality-management system regulations: In the EU the international standard EN/ISO13485 applies in particular for regulatory purposes of quality management systems for medical devices and plays a central role. It is one of the essential requirements to fulfill for the CE declaration of conformity to ensure that the products concerned meet the provisions that apply to them. The U.S. laws for current good manufacturing practice (CGMP), in particular 21CFR Part 820 is probably in an adapted version the most suitable for a quality management system for DCs. It is based on the EN/ISO13485 but is clearly structured to fulfill the rules in an easier manner. The requirements within that chapter govern the methods to control development, manufacturing, packaging, labeling, user instructions, other documentation accompanying the product, storage, installation and maintenance of all finished devices intended for human use.

Software development processes: IEC60601-1-4 was the first international standard to deal with programmable electrical systems for medical devices and handles software. However, because of the limitation of active medical devices it was necessary to find a new approach. This was achieved in the IEC62304, which requires preventive measures to be taken during the whole life cycle of the software to reduce its associated risks.

One of the key issues in the development of DCs is reliable software. This can only be achieved if the development of the software follows well-established regulations ensuring that the whole process is under control. IEC62304 starts with the software development planning. The required tasks are related directly to the safety classification of the device under development, dependent on the risk/hazard associated with the device in the case of a malfunction.

This standard does not prescribe any specific life-cycle model but does provides a framework for life-cycle processes with the activities and tasks necessary for the safe design and maintenance of the software. There are several models for the software development process, each describing approaches to a variety of tasks or activities that take place during the development process. One of the most useful models is the V-Model. However, the IEC62304 is too demanding and complicated for DCs. Its enforcement would be a huge burden for a developer and manufacturer, especially for those working on a small scale. But it is essential that the structure of the IEC62304 be used to make the software of DC reliable and safe for the user.

Risk management process: A basic premise of IEC62304 is that the software is developed and maintained within a regulated environment. Therefore, the manufacturer should employ a quality-management system, and a risk-management process complying with ISO14971 Medical Devices - Application of Risk Management to Medical Devices.

Software has to be handled in a separate way. It is not easy to manage common hazards of software errors (bugs) within risk management. A major obstacle is that software errors do not occur randomly. In assessing the likelihood of a risk in software it must be assumed that probability in the risk analysis of occurrence is 100%. That is where the IEC62304 standard applies by requiring that processes, activities, and tasks are completed to establish and ensure safety by using preventive measures. Those measures should reduce the probability of errors in the code, i.e., wrong bits (8 bits = 1 byte) as well as wrong specifications.

At the beginning of software development, the identification of hazards is a very important step where appropriate measures are needed to reduce the risk by implementing requirements to the software. The IEC62304 software risk-management process is intended to provide those additional requirements for the software during the design and development process when safety, effectiveness and quality of software are established.

The combination of IEC62304 and ISO14971 for risk management of DCs might be very useful, although a direct application might not be possible. Special interpretive tailoring of ISO14971 would be necessary.

From design control to validation: One often used model for the design of software, hardware, or combinations thereof, which shows the relations between design control, requirement specifications, testing, verification and validation is the V-model. As such, it simplifies the understanding of the complex systems associated with their development. The V-model is designed as a guide for planning and execution of development projects, taking into account the complete life cycle including verification and validation. Application of the V-model to a DC might require expansion to an interlaced model of many V-models for each system component and if applicable to the subsystems and units building an overall V-model for the final product.

PROPOSED DC LIFE CYCLE

Typically, a responsible manufacturer has a defined process for system development, usually conforming to a quality normative like ISO9001. For safety-critical systems this process has to be enhanced to fulfill the requirements of the safety life cycle of IEC61508.

In brief, the safety-critical life cycle consists of:

- Overall scope definition: All principal functions of a device are specified here. For a DC, this may include all the parameters displayed (e.g., depth, time, decompression obligations), how they are displayed, mechanical designs, performance parameters, operational ranges (depth, temperature), etc.
- Hazard and risk analysis. All imaginable hazards are listed and the corresponding risk is determined based on the expected probability. In the case of a DC, this list will include operational risks, such as a diver exceeding maximum depth or violation of decompression obligations, but will also system-related risks. These may include battery lifetime, water leakage or malfunction in hardware (such as a defective component). The most complex development part of a DC is software. Typically, a large part of the risk analysis is devoted to software malfunctions. One aim of the risk analysis is to also detect possible failure events.
- Safety requirements allocation: Based on hazard and risk analysis, the overall systems requirements are enhanced by including the safety requirements.
- Design and implementation phase: The hardware and software development takes place here. In parallel, verification and validation plans are established. Verification assures that requirements are preserved from one development phase to the next. Based on the hazard and risk analysis in the design and implementation phases,

measures have to be taken in order to either eliminate or, if not possible, to mediate the impact of a certain hazard. This also includes informing the user about the status of a system – like correctly operating in a failure mode.

- Validation phase: Validation checks the final product against the complete list of requirements, including safety. In the case of validation of a DC, one would not only check if the main functions, for instance, depth and time display are correct, but also what happens in the case of a software reset, hardware failure, or a simple supply voltage drop caused by an empty battery or corroded contacts.

The complete life cycle is documented in the so-called design history file or technical construction file. This file is a prerequisite for CE certification of PPE category III and has to be presented to the Notified Body involved. It is also important to understand that all of the documents are subject to modifications during the development following not only new requirements but also after the appearance of new safety related issues initiated during the design, implementation and validation phase. Guidelines for the implementation of the life cycle can also be found in normatives and regulations for medical systems. Guidelines for the V-model and the more recent V-model XT are one possible method of describing the life cycle. Another alternative was proposed by Fredriksen (2002), who enhanced the widely used Rational Unified Process (RUP) with a safety discipline to incorporate the demands of IEC61508. It is of utmost importance, however, that the life cycle is manageable by the rather small development teams. An ISO working group is currently addressing this topic by working on system engineering life cycles for small development teams. (INCOSE South Africa, pers. comm.)

Another useful document could be the FDA Guidance on General Principles of Software Validation (Final Guidance for Industry and FDA Staff January 11, 2002), which applies to medical device software and to automated process software.

It is clear that design for safety has to start early in the system's life cycle, during system requirements analysis. It is crucial for the safety of the planned system to close the semantic gap between all stakeholders in a development project (Doeben-Henisch and Wagner, 2007). When applied to the development of DCs, this means that all people involved in the DC development have to communicate about the overall requirements.

CONCLUSION

Products within certain groups in the EU require CE certification to be brought to market. It is the manufacturer’s obligation to categorize its equipment and apply the corresponding normative to ensure a maximum level of safety. DCs made by several manufacturers have been checked for references to CE certifications. While some manufacturers refer to a variety of normatives, others refer only to a few (Table 1). It is clear that there is no harmonized way of testing and certifying DCs, probably because currently there are no standards or normatives that specifically address them. It is also interesting to note that EN13319, a normative that could be used for certification of a dive computer, is only referenced by a few manufacturers.

A CE mark, even if the dive computer is categorized by the manufacturer as PPE, is no guarantee of safety from a functional safety point of view, even though products developed and certified according to the PPE directive should have been subject to a safety life cycle. This is misleading for the consumer, who is often not aware that there are no standards, normatives or guidelines specifically for DCs but considers the product to be safe, especially when a manufacturer claims that the device is a PPE and was tested accordingly.

To counter this problem, we have two suggestions: the first is that we suggest including DCs in the PPE directive under category III. This would make application of good manufacturing practices mandatory for DC manufacturers and therefore a safety life cycle for the complete development would have to be followed. This could increase the functional safety to a higher and more uniform level. The second suggestion is that the drafting of a normative, especially for DCs, should be discussed. Rather than being design restrictive by describing a "golden model for decompression theory" we believe that one should address functional safety. Also, it may be helpful to reference EN61508, although this is a broad standard and so derivation or tailoring is necessary in order to enable small developers' teams to fulfill certification requirements.

Risk and hazard concerns associated with the use of a device allows DCs to be compared to medical devices. Therefore, normatives for medical devices like the IEC62304, ISO14971 and ISO13485 could also be used as a model for drafting a normative specific to DCs.

When it comes to a failure, we also suggest that the safety status of the DC must be displayed, in an unambiguous manner, to the diver. This is not a new suggestion, but has still not been delivered.

LITERATURE CITED

Azzopardi, E., and M.D.J. Sayer. 2010. A review of the technical specifications of 47 models of diving decompression computer. *Underwater Technology*, **29:** 63-72.

Azzopardi, E., and M.D.J. Sayer. 2011. DCs: Seeing isn't always believing. *Proceedings of the South Pacific Underwater Medicine Society 40th Annual Science Meeting*, p. 32. Abstract.

Bourdelet, P. 2007. *L'ordinateur de plongée*. Hyeres: Editions Turtle Prod. ISBN 978-2-9530430-2-0.

Boycott, A.E., G.C.C. Damant, and J.S. Haldane. 1908. Prevention of compressed-air illness. *Journal of Hygiene,* **8:** 342–425.

Denoble, P. 2010. The Validation of Dive Computer Decompression Safety. *Alert Diver,* Summer 2010.

Doeben-Henisch, G., and M.F. Wagner. 2007. Validation within safety critical systems engineering from a computational semiotics point of view. *Proceedings of AFRICON 2007*. September 26-28, 2007. pp.1-7. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

Fredriksen, R. 2002. Use of the Rational Unified Process for Development of Safety-Related Computer systems. M.Sc. thesis, Høgskolen i Østfold avdeling for infomatikk og Automatisering. Halden, Norway. 69 pp.

Gamroth, E., J. Kennedy, and C. Bradley. 2011. Design and testing of an acoustic ranging technique applicable for an underwater positioning system. *Journal of the Society for Underwater Technology*, **29(4):** 183-193.

Groves, G., and W. Munk. 1953. A decompression gauge for divers. SIO Reference Rept. 53-64. San Diego: University of California, Scripps Institution of Oceanography.

Herrmann, D.S. 1999. *Software Safety and Reliability*. Hoboken, NJ: Wiley. ISBN-13:978-0769502991.

Hollnagel, E., D.D. Woods, and N.G. Leveson. 2006. *Resilience Engineering: Concepts and Precepts*. Farnham, Surrey: Ashgate Publishing Limited. ISBN-13:978-0754646419.

Huggins, K.E. 1989. The history of underwater decompression devices and computers. In: Lang, M.A., and R.W. Hamilton, eds. *Proceedings of the AAUS Dive Computer Workshop.* USC Catalina Marine Science Center. Pp. 7-30. Costa Mesa, CA: American Academy of Underwater Sciences.

Huggins, K.E. 2012. Dive computer considerations. In: Blogg, S.L., M.A. Lang, and A. Møllerløkken, eds. *Proceedings of the Validation of Dive Computers Workshop*, 24 August 2011, Gdansk, Poland. Pp. 19-28. Trondheim: European Underwater and Baromedical Society.

Koss, B., and A. Sieber. 2011. Development of a Graphical Head-Up Display (HUD) for Rebreather Diving. *Underwater Technology,* **29(4):** 203-208.

Kuch, B., B. Koss, G. Butazzo, Z. Dujic, and A. Sieber. 2009. Underwater Navigation and Communication: A Novel GPS/GSM Dive Computer. Aberdeen: European Underwater and Baromedical Society. Abstract.

Kuch, B., B. Koss, G. Buttazzo, Z. Dujic, and A. Sieber. 2010. A novel wearable apnea dive computer for continuous plethysmographic monitoring of oxygen saturation and heart rate. *Diving and Hyperbaric Medicine*, **40(1):** 34 -39.

Kuch, B., S. Haasl, M. Wagner, G. Buttazzo, and A. Sieber. 2011. Preliminary report: Embedded platform for inertial based underwater navigation. 9th International Workshop on Intelligent Solutions in Embedded Systems, Regensburg, Germany

Lang, M.A., and R.W. Hamilton, eds. 1989. *Proceedings of the AAUS Dive Computer Workshop.* USC Catalina Marine Science Center. Costa Mesa, CA: American Academy of Underwater Sciences.

Lang, M.A., and S.A. Angelini. 2009. The Future of DCs. In: Lang, M.A., and A.O. Brubakk, eds. *The Future of Diving: 100 Years of Haldane and Beyond*. Pp. 91-100. Washington, DC: Smithsonian Institution Scholarly Press.

Leveson, N.G. 1995. *Safeware: System Safety and Computers*. Chicago: Addison Wesley Longmann. ISBN-13:978-0201119725.

Leveson, N.G. 2004. A systems-theoretic approach to safety in software intensive systems. *IEEE Transactions on Dependable and Secure Computing*, **1(1):** 66-86.

Osterhout, R. 1989. Discussion Session 1 Commentary. In: Lang, M.A., and R.W. Hamilton, eds. *Proceedings of the AAUS Dive Computer Workshop.* USC Catalina Marine Science Center. p 34. Costa Mesa, CA: American Academy of Underwater Sciences.

Sieber, A., B. Koss, and B. Kuch. 2010. Testing and Validation of Diving Computers. Istanbul: European Underwater and Baromedical Society. Abstract.