SAFETY STATUS: AN INNOVATIVE CONCEPT FOR MAINTAINING THE SAFETY INTEGRITY LEVEL OF OPERATIONAL SAFETY SYSTEMS

PIERRE NININ, CYRILLE SALATKO & JÉRÉMIE VALBOM
CERN, Switzerland & ASSYSTEM Engineering & Operation Services, France.

ABSTRACT

The safety of industrial sites or large research facilities such as CERN (European Organization for Nuclear Research) is obtained by the combined actions of physical security, cyber-security and functional safety that jointly contribute to risk reduction. To deal with functional safety, the IEC 61508-61511-61513 standards are used for regulating design, development and maintenance of the Safety Instrumented Systems (SIS) that implement Safety Instrumented Functions. The SIF's performance is characterized by its Safety Integrity Level (SIL) determined through a risk analysis and conditioned by parameters related to the design, the staff's skills involved in its development, operation and maintenance or the compliance with repairing times. Heads of facility and SIS responsible persons have to continuously master the SIL performance. This is a responsible act to guarantee the risks reduction barriers efficiencies, considering criteria such as periodic testing, spare parts availability, components obsolescence, by-passes, changes control, system real-time status, physical and cyber protections. The **Safety Status** software imagined jointly by CERN and ASSYSTEM inherits both the CERN experience on the specification and operation of safety systems adapted to the specific risks of particle accelerators and experiments and the know-how developed by ASSYSTEM as a major player in the engineering of nuclear installations, particularly in the field of design and maintenance of critical security and control systems. **Safety Status** establishes a functional safety dashboard of each system updated automatically or manually with data coming from relevant sources such as maintenance management, document management or the SIS itself. Through a friendly interface, it displays an overview of all the useful information that illustrates the health of the SIS and the integrity of its safety functions. After introducing the concept, the paper presents the methodology, the main features of the software, and the experience feedback gained by its implementation on the CERN MEDICIS facility.

Keywords: safety system engineering, security global approach, SIS operation & maintenance.

1 INTRODUCTION

CERN, the European Organization for Nuclear Research, is an intergovernmental organization with over 22 member states. Its headquarter is in Geneva but its premises are located on both sides of the French-Swiss border. CERN's mission is to enable international collaboration in the field of high-energy particle physics research as well as to design, build and operate particle accelerators and the associated experimental areas. Currently more than 11 000 scientific researchers from institutes all over the world are using CERN's installations for their experiments.

The accelerator complex at CERN is a succession of machines with increasingly higher energies. Each machine injects the beam into the next one, which takes over to bring the beam to an even higher energy, and so on. The flagship of this complex is the Large Hadron Collider (LHC).

The ASSYSTEM Group has a leading position in engineering complex systems in constrained environments. ASSYSTEM's experts help major industrial and research actors to optimize their investments by designing, building, maintaining and, ultimately, dismantling power plants and industrial facilities. As a key part of ASSYSTEM, the Critical Security and Control Systems (CS&CS) department coordinates the activities of Automation,

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N1-139-149

Instrumentation & Control and SCADA, Operation & Maintenance of industrial systems, Security Systems (access control, CCTV, intrusion detection, etc.), Industrial Control Systems Cyber-security, Building Management Systems and Robotics.

1.1 CERN Safety Systems

The protection of the personnel against the risks raised by the CERN large scale accelerator and experimental facility is ensured by means of numerous dedicated safety systems covering aspects such as radiation protection, access control, access safety, laser protection, gas detection, fire detection, fire protection, audio systems, etc.

The users' community vary from a few people for a small experiment to hundreds of people accessing the Large Hadron Collider during a planned maintenance. The challenge for the group responsible for the safety systems is to ensure a full performance on a 24 h/365 d basis but also in the long term, as the lifetime of a CERN facility is usually over 25 years.

CERN being monitored by the French and Swiss Nuclear Regulatory Body, it has to permanently be able to demonstrate that the risk raised by the particles accelerators operation and the experiments are fully mastered by adequate systems and procedures. In this context, the IEC 61508 standard has been adopted in the nineties as the main reference to design functional safety systems and more particularly its two sectorial application standards: the IEC 61511 and IEC 61513 dedicated to SIS in the respective sectors of the processing and the nuclear industries [1–3].

For the past 20 years CERN's knowledge of functional safety applied to the design of numerous large scale safety systems and return of experience has increased, allowing to focus now on the last stage of the lifecycle: the operation and more particularly on the factors influencing the confidence that a system can achieve its safety mission at any time. During this period, ASSYSTEM and CERN have been collaborating through activities aimed at designing, developing and maintaining critical control systems such as radiological monitoring, cooling and ventilation, access control or personal protection systems. This collaboration has enabled the **Safety Status** concept to emerge, taking advantage of the amazing playing field formed by CERN's systems and the experiences of the authors in the fields of engineering, operation and maintenance of these critical systems.

2 SAFETY STATUS CONCEPT

The **Safety Status** concept imagined jointly by CERN and ASSYSTEM establishes a dashboard of the functional safety aspects of every system. It is based on a methodology and a software tool allowing updating automatically or manually the data coming from relevant sources. Its main objective is to monitor the efficiency of the critical systems.

2.1 Underlying concept data

The safety of industrial sites of large research facilities, such as CERN, is obtained by the combined actions of physical security, cyber-security and functional safety that jointly contribute to risk reduction [4–6]. To deal with functional safety, the IEC 61508-61511-61513 standards are currently used for regulating design, development and maintenance of the Safety Instrumented Systems (SIS) that implement Safety Instrumented Functions (SIF). The SIF's performance is characterized by its Safety Integrity Level (SIL) determined through a risk analysis expressed as a Risk Reduction Factor (RRF). Regarding the safety point of view, the SIL concept, deals with several parameters [7, 8]. Some have to be taken into account during the engineering phases of the SIS (design, implementation and validation) and others are impacting the operation and maintenance phases. Here's a non-exhaustive list of such parameters: Probability of Failure on Demand or per Hour (PFD / PFH), maintenance efficiency such as Mean Time To Repair (MTTR) or Mean Down Time (MDT), operation critical delays such as Process Safety Time (PST), failures categories (λ_{DU} / λ_{DD} / λ_{S}) and the corresponding Safe Failure Fraction (SFF), Common Cause Factor β (CCF), Hardware Fault Tolerance (HFT) with impact on SIF implementation architectures, Diagnostic Coverage capabilities (DC) and Test Interval (Ti).

Beside those quantitative items, unitary criteria are linked to the engineering phase of the SIS and to the way it will be operated and maintained. Nevertheless, before detailing those criteria, the next paragraph will introduce the four major factors, which will be used to classify all relevant items that influence safety integrity.

2.2 The motorcycling example

The concept can be illustrated (Fig. 1) by the parameters that must be verified for the safe use of a motorcycle to go from point A to point B:

- The capacity of the driver to ride the motorcycle (detention of a valid driving licence, sobriety, knowledge of the traffic rules);
- The general state of the vehicle and its technical capability (inspections, revisions, state of the tires, of the brakes);
- The safety of the chosen road and the absence of dangers along the path (lighting, surface, security rails, road markings, road signs);
- The reliability of the motorcycle model based on its design and its manufacturing (quality of the initial engineering, absence of additional assemblies, no modification of the mechanical characteristics or the engine).

The above-mentioned points raise the four questions that are necessary to qualify the mission: 'Is the vehicle correctly operated?', 'Is it correctly maintained?', 'Is the environment

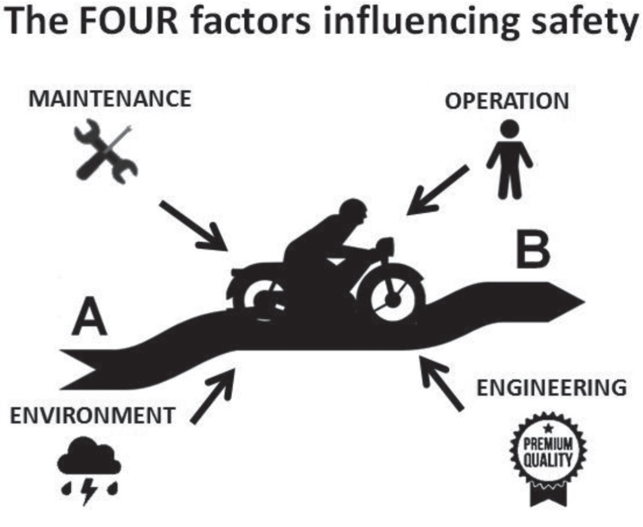

Figure 1: Factors influencing safety.

safe?', 'Is the vehicle known for its robustness and reliability?'. Answering « YES » to the above questions will give confidence for a safe trip between points A and B.

2.3 The Safety Status concept

The **Safety Status** concept is based exactly on the same approach, considering that the SIS security missions allow an effective risk reduction from an 'unacceptable' to an 'acceptable' level and that the success of these missions depends directly on the four factors introduced in the example of the motorcycle: *Operation*, *Maintenance*, *Environment* and *Engineering*. To manage the update of the status regarding the four factors, some categories have been introduced. The categories act as normalization interfaces allowing the connection between the raw data of the underlying criteria and the four factors imposed at the top of the dashboard. Additionally, three statuses are performed to bring accurate synthesis:

- *Availability*: an image of the SIS availability based on an automatic uptime data source;
- *Integrity*: a safety integrity state as a Boolean information based on few criteria with direct impact on the effective SIL level;
- *Vulnerability:* an illustration of the on-going vulnerability of the SIS, built from the operational status for physical security and cyber-security systems that are used to protect the SIS components [9].

Table 1 illustrates the complexity of the environment that shall be considered to ensure that the performances of the SIS are preserved once it has been commissioned and switch to operation and maintenance phase.

Table 1: Details of 20 categories that are associated with the four main factors and for each category some relevant underlying criteria are listed..

Operation	**Maintenance**	**Environment**	**Engineering**
Operation HR (operator training and skills, team organization, on-call service, contractors, etc.)	***Maintenance HR*** (maintenance team skills, operational on-call service, etc.)	***Cyber-security*** (efficiency of network protection devices, security patches deployment, etc.)	***Organizational*** (project team, change control process, IEC safety life cycle compliance, etc.),
Operation documentation (guidelines up to date, emergency procedures available in control room, etc.)	***Maintenance Documentation*** (reflex form available, preventive maintenance schedule, etc.)	***Physical security*** (integrity of the physical barriers, access control and intrusion systems efficiency, etc.)	***Detailed design*** (redundancy, common mode failure, diversity, single failure criteria, etc.)
Process Alarms (efficient monitoring of process alarms, ongoing alarm, etc.)	***Preventive maintenance*** (compliance of scheduling, etc.)	***Utilities*** (IT networks, electrical supplies, racks cooling, etc.)	***Validation*** (tests strategy, operational test platform, etc.)

(*Continued*)

Table 1: *(Continued)*

Operation	Maintenance	Environment	Engineering
By-pass Management (on-going applied by-pass, existing process to manage by-passes, etc.)	***Corrective Maintenance*** (on-going failure, CMMS system available and suitable policy, etc.)	***External hazards*** (flood, earthquakes, terrorism, etc.)	***Baseline documentation*** (safety studies, specifications, detailed design, electrical drawings, etc.)
	Spare parts management (management process efficiency, full stock, etc.)		***Configuration management*** (EDM, software versioning tool, etc.)
	Obsolescence (detection and mitigation plan, technology intelligence, etc.)		
	Technical Alarms (correct state of technical alarms systems, on-going alarm, etc.)		

Figure 2 illustrates the corresponding data hierarchy that has been established, by the mean of configurable weights, to link the criteria with main categories and at the end to manage the way those categories are impacting the main four factors.

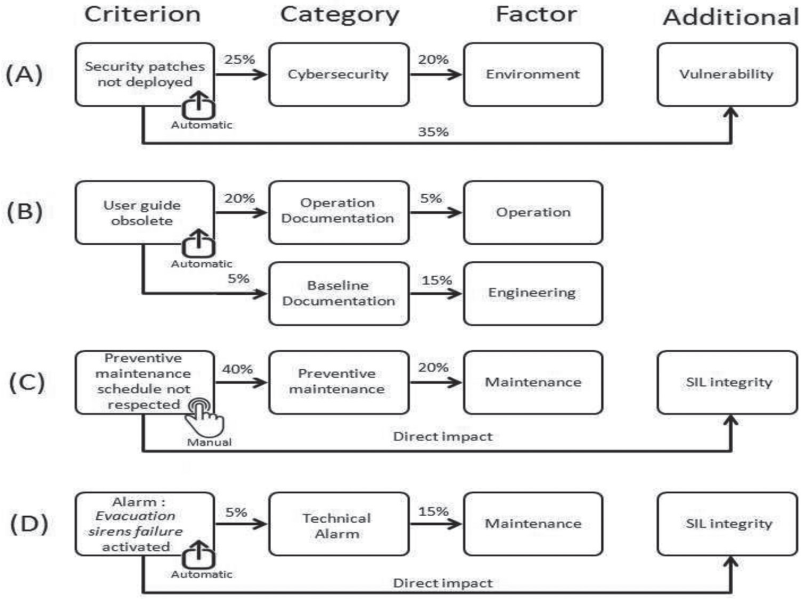

Figure 2: Safety status: weighting samples.

Case (A): an automatic event detects that the security patches has not been deployed. It has a weighted impact to cyber-security category (25%) that lead to degrade the *Environment* quotation to which it contributes for 5% (25% x 20%). The same criterion also impacts the *Vulnerability* status up to 35%.

Case (B): EDM tool brings an automatic alert concerning the obsolete status of an operation document (user guide). This impacts the *Operation* factor through the operation documentation category up to 1% (20% x 5%). The same criterion impacts also the *Engineering* factor through the baseline documentation of the SIS up to 0,75% (5% x 15%).

Case (C): a preventive maintenance slot has been missed. This manual entry event leads to degrade the *Maintenance* factor to which it contributes up to 8% (40% x 20%). And it impacts directly the SIL capability of the SIS because of non-compliance with the Test Interval imposed by the SIL target.

Case (D): from the analysis of the system, performed during an initial Audit stage, process and technical alarms were extracted. These alarms can be considered critical or not according to the alarm management strategy. If the alarms have an influence on the safety system then they are included in the criteria to be evaluated. The case (D) emphasizes the criteria attached to the activation of the alarm '*Evacuation sirens failure*'. This criterion is associated with the technical alarm category itself linked to the *Maintenance* factor. The sirens are in a critical chain and no interlock is expected in case of failure. So a direct result of this alarm is a non-compliance with SIL requirements (*Integrity* status) because the SIS will no longer ensure its protection mission. Notice that if the failure has been taken into account in the design of the safety treatment (forced interlock in case of siren failure) the same alarm would have no impact on the *Integrity* status; then the link between criterion 'Alarm: *Evacuation sirens failure* activated' and SIL level would not be present.

2.4 Presentation of the Safety Status data flows

Figure 3 illustrates the data flows allowing to update the tool. The data sources are either automatic or manual. The correlation and computation stages allow treatments that take into

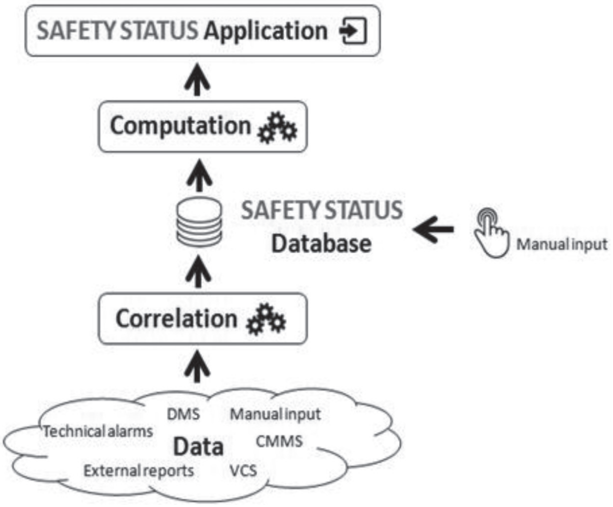

Figure 3: Safety status: the data flows and treatments.

account the specificities of the audited system as well as of its operation and maintenance requirements (see previous Fig. 2).

The main flows and treatments that are shown on the Fig. 3 concern:

- The manual input of events done by the user. A dynamic form guides the user through questions that help target the criterion concerned by the input.
- The automatic data acquisition obtained by the mean of dedicated interfaces with external systems such as the EDM tool, the SIS alarm system, CMMS, network statuses.
- The correlation level that corresponds to the necessary formatting and pre-processing operations to import raw data in the database.
- The computation level where are applied the association and weighting strategies to the criteria and the categories upon factors.

3 METHODOLOGY

The deployment of **Safety Status** on a SIS is a three stages process: Audit stage, Configuration stage and Tool operation. This methodology implies a strong knowledge of the normative concepts, an understanding of the design of the SIS and its operating and maintenance environment. The previous data hierarchy (Fig. 2) and data flows (Fig. 3) structure the way that the information should be collected during an initial Audit stage and the way the collected information should be recorded in the tool.

Figure 4 gives an illustration of the overall concept and the way it can help to improve the operational safety and security achievable levels at the given time.

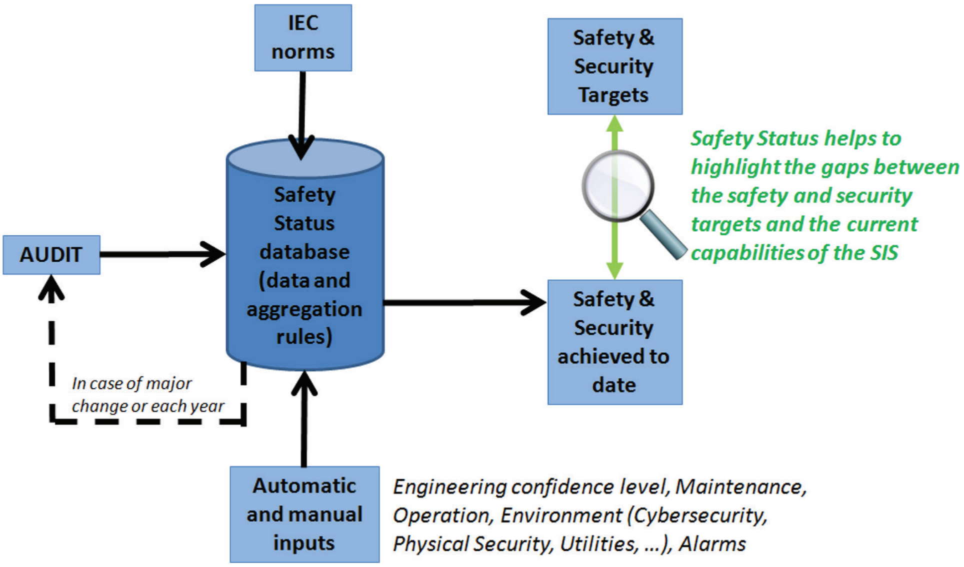
IEC norms
Safety & Security Targets
Safety Status helps to highlight the gaps between the safety and security targets and the current capabilities of the SIS
AUDIT
Safety Status database (data and aggregation rules)
Safety & Security achieved to date
In case of major change or each year
Automatic and manual inputs
Engineering confidence level, Maintenance, Operation, Environment (Cybersecurity, Physical Security, Utilities, ...), Alarms

Figure 4: Safety status: the virtuous circle.

3.1 First stage: the initial Audit

The Audit stage is done, if possible, during the commissioning phase to establish an initial picture of the system and of its environment. First of all the system safety missions are extracted from the risk analysis document as well as the expected integrity level for each safety objective. The Audit consists in reviewing the SIS compliance to the functional safety standards and more particularly to the criteria defined in Table 1 and moreover the identification of the ones that are not fulfilled. Some of the criteria are related to the system alarm strategy to catch relevant alarms, which could directly impact the factors. A special care is also given to the maintenance and operation organisation analysis as well as the system operating in its environment. In the end, more than 50 criteria particularly relevant for norms and regulations compliance are considered. The level of each criterion is evaluated using a suitable scale (boolean, fuzzy, proportional) and will be mapped to a 0-100 range during the Configuration stage.

The Audit's output information is the one related to the standards compliance and more particularly the identification of the non-compliances to the standards, the safety objectives of the SIS for each safety mission, the architecture of the SIS for each SIF (Reliability Block Diagrams representation), data related to the organization of the maintenance and the system environment. The Audit stage is the opportunity to fill the identified gaps and to set up the foundation to use **Safety Status**.

3.2 Second stage: Safety Status Configuration

The second stage consists in the definition of the data describing the SIS in **Safety Status**. From the data collected during the Audit, the final list of the relevant criteria and their weights shall be established. By default the application proposes standard associations of the criteria to the categories (and thus to the factors), but each criterion may be reviewed and reassigned. This work should be done for each safety mission. This stage is tedious, but will really highlight the strong and weak points of the system. By this means the correlation rules make it possible to adapt as closely as possible to the context of design and operation of the SIS in its environment. The following elements are considered: selection of the relevant criteria, identification of the available data sources (automated, manual, calculated), scaling of criteria, allocation of the criteria to the category and to the four factors (*Operation*, *Maintenance*, *Environment*, *Engineering*) as well as to the *Availability*, *Integrity* and *Vulnerability* aspects, weighting of the criteria in each category and in each factor, initialization of the data value for each criteria, development of the interfaces.

The development of the automatic interfaces is a critical stage that depends on the existence of monitoring and alarms systems, of a documentation management system, of a software versioning tool or of a maintenance management system as well as their interfacing capabilities and the consistency of the available data.

Forms to manually update criteria such as by-pass declaration, spare parts availability and obsolescence or versioning changes, are developed at this stage.

3.3 Third stage: Safety Status Operation

At this stage **Safety Status** is connected to its automatic and manual interfaces. All along the SIS operation and maintenance activities, the user updates the data of the applicable criteria.

In case of evolution of the SIS, according to the importance of the modification, it could lead to the need of a new audit stage to ensure that a rigorous engineering change process has been applied to cope with the system design impact, documentation update, testing or versioning.

4 APPLICATION

MEDICIS (MEDical Isotopes Collected from ISolde) is a new facility constructed at CERN to produce radioactive isotopes by irradiating specific material samples by means of a particle beam. The isotopes will be used for medical research to highlight specific biological cells for imaging, or to target them for destruction. A specific Personnel Protection System (PPS) has been designed to ensure the following 'Safety Missions' to protect the users against ionising **radiation**, **mechanical** hazards due to the displacement of handling robots, and against **electrical** high voltage and low voltage hazards.

CERN has mandated ASSYSTEM for the realization of the MEDICIS PPS. During the commissioning stage, when decided to apply the **Safety Status** stages to the new SIS, it's quickly appeared to both stakeholders the important added value of the concept as it investigates in detail all the aspects that will influence the performance of the SIS.

Information collected during the audit stage summarizes the safety parameters of the PPS, including elements such as the hazards to be covered with RRF targets, the Safety Missions including SILs targets, the list of the SIFs including their hardware and software architectures. It also characterizes the SIS, the localisation of its components and of the protected areas, its overall technical architecture and external interfaces to the network, its utilities, its alarm strategy, it's baseline documentation. Ultimately it collects other information on availability, accessibility and environmental constraints.

Some remarks raised during the commissioning stage of the facility are listed below (each collected criterion has been rated within a defined scale):

- The status of the cyber-security protective measures, has been quoted at 100/100, as this aspect has been carefully considered in the design;
- The status of the baseline documentation is rated at 60/100, as some documents need to be updated in their as-build version;
- Another criterion is associated with the existence of an EDM system to follow the versioning of the SIS reference documents. It has been rated to 100/100 considering that all the project documentation is stored under the CERN's EDM tool (so-called EDMS) and that this tool will be used to manage the future documentation evolutions;
- A bad rating of 20/100 has been obtained for the obsolescence management plan as no obsolescence-processing plan has been studied yet. Furthermore, the version of the PLC is a model that will soon not be supported anymore by the manufacturer.
- The maintenance organization to date suffers of a lack of knowledge regarding to the interface with the radiological monitoring system. An evaluation at 25/100 only as been quoted for this criterion.

The 70 underlying criteria considered in the Audit of the MEDICIS PPS are linked with the categories introduced in Table 1: and their weighting has been tuned to take into account the MEDICIS specific context. As an example the 'Obsolescence management plan' poorly rated criterion represents 50% of the 'Obsolescence' category, which itself contributes for 10% to the *Maintenance* factor and degrades the three safety missions. The 25/100 rating due to the lack of knowledge of the radiological monitoring system affects the Radiological

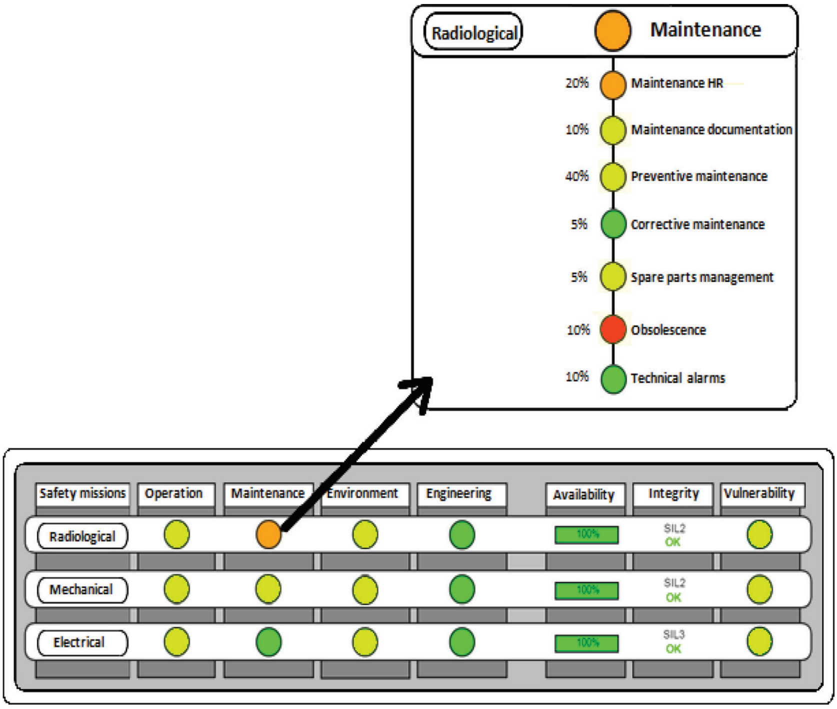

Figure 5: Safety Status: the MEDICIS HMI.

safety mission only. It also contributes to 30% of the ‘HR Maintenance’ category that itself contributes for 20% of the *Maintenance* factor. Those weighting factors are illustrated in Fig. 5 representing the Safety Status dashboard for the PPS MEDICIS.

On the Fig. 5, the *Environment* factor rating inherits the lack of technical measures that protect the racks housing the PPS components meaning the factor is not fully green. This affects at the same time the *Vulnerability* status. Figure 5 also illustrates the way the tool brings detailed information regarding the factors and additional statuses. By clicking on a colored item the user accesses the detail of the underlying categories that influence the chosen factor.

All of this illustrates how the data collected during the Audit allow the initialization of the parameters and also the organization of the information through the weighting of the criteria and their contribution to the factors summarized in the **Safety Status** dashboard.

Concerning the interfaces, in the case of MEDICIS, the following systems may provide automatic updates to the underlying criteria: the SIS itself by means of its process and technical alarms, the EDM system, the CMMS, the SVN versioning tool, the Zabbix® monitoring tool providing information of the architecture of the SIS and of its environment. Manual entries have to be done to declare events regarding spare parts movement, obsolescence detection and associated mitigation plan, by-pass management, update concerning the maintenance and operation organization or some physical security matters.

5 CONCLUSION

A 25 years experience using various safety standards raised a lot of questions and investigations to achieve the development of the CERN personnel protection systems. If some systems fall in a well-defined normative framework, some others that need the integration of several different technologies, require further efforts to ensure that they meet their safety objectives and one can immediately raise the question on how such complex safety system will evolve over time. The **Safety Status** concept brings it a practical answer, as of the commissioning stage of a safety system, with its Audit that checks the compliance to the norms of more than 70 safety criteria, identify possible drifts and set-up a 'starting point'. Through a comprehensive dashboard, it will inform overtime on the evolution of the safety system's integrity. The first Audit realized has shown the great potential of the concept. The **Safety Status** tool proves to be accurate and adaptable to the monitored system's context. Particular innovative characteristics of the concept are to take into account the physical environment of the system, the cyber-security and to consider selected criteria inherited from IEC norms. Beyond the methodology and functionalities provided by the tool, **Safety Status** helps to protect people, environment and industrial systems. The increasing of the digitalization in the industrial units will allow catching more easily automatic information to feed **Safety Status** and to increase its real time analytic capabilities, so let's look forward and go on deploying the methodology and the tool.

ACKNOWLEDGEMENTS

To the reviewers and to those who have always supported this innovative concept: E. Sanchez-Corral Mena, F. Valentini, T. Ladzinski, G. Desvergnes, J. Levesque, C. Joaquim.

REFERENCES

[1] International Standard IEC 61511 Edition 2.0, pp. 73–77, 2016.

[2] Valentini, F., Hakulinen, T., Hammouti, L., Ladzinski, T. & Ninin, P., Formal Methodology for Safety-Critical Systems Engineering at CERN, *Proceedings of ICALEPCS 2013*, San Francisco, USA, 2013.

[3] Scibile, L., Bartolome, R., Chouvelon, A., Grau, S., Ninin, P. & Trebulle, M., Experience using the Functional Safety principles to Design the CERN Safety Alarm Monitoring System, *Proceeding of ICALEPCS 2003*, Gyeongju, Korea, 2003.

[4] Ninin, P., IEC 61508 Experience For The Development of The LCH Functional Safety System and Future Perspectives CERN, *Proceedings of ICALEPCS 2009*, Kobe, Japan, 2009.

[5] Hakulinen, T., Lopez, X., Ninin, P. & Oser, P., Information Security Assessment of CERN Access and Safety Systems, *Proceedings of ICALEPCS 2015*, Melbourne, Australia, 2015.

[6] Hakulinen, T., Ninin, P., Nunes, R. & Riesco-Hernandez, T., Revisiting CERN safety system monitoring (SSM), *Proceedings of ICALEPCS 2013*, San Francisco, USA, 2013.

[7] Smith, D.J. & Simpson, K.G.L., *Safety Critical Systems*, Butterworth-Heinemann, 4 edn, 2016.

[8] Ciutat, F., *SIL, automatisme et sécurité - Intégrité et sureté du contrôle-commande industriel*, APTA éditions, 3rd edn, 2015.

[9] Pietre-Cambacedes, L., Fourastier, Y., Téa, F., Platel, L., Boucart, D., de Peslouan, N., Ragozin, O., Bock, P., Jabot, J-C., Sitbon, P., Bouissou, M., Billois, G., Kobes, P., Guyomard, F., Meynet, S., Demongeot, T., Duflot, F., Feuillet, M. & Lusseyran, T., *Cybersecurité des installations industrielles*, Cepadues editions, 2015.