ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

SAFETY INSTRUMENTED SYSTEMS AND THE AWAKE PLASMA CONTROL AS A USE CASE

E. Blanco Vinuela, B. Fernandez Adiego, R. Speroni, CERN, Geneva, Switzerland
F.H. Braunmueller, Max Plank Institute, Munich, Germany

Abstract

Safety is likely the most critical concern in many process industries, yet there is a general uncertainty on the proper engineering to reduce the risks and ensure the safety of persons or material at the same time as providing the process control system. Some of the reasons for this misperception are unclear requirements, lack of functional safety engineering knowledge or incorrect protection functionalities attributed to the BPCS (Basic Process Control System). Occasionally the control engineers are not aware of the hazards inherent to an industrial process and this causes an incorrect design of the overall controls. This paper illustrates the engineering of the SIS (Safety Instrumented System) and the BPCS of the plasma vapour controls of the AWAKE R&D project, the first proton-driven plasma wakefield acceleration experiment in the world. The controls design and implementation refers to the IEC61511/ISA84 standard, including technological choices, design, operation and maintenance. Finally, the publication reveals the usual difficulties appearing in these kind of industrial installations and the actions to be taken to ensure the proper functional safety system design.

INTRODUCTION

The Proton Driven Plasma Wakefield Acceleration Experiment (AWAKE) is an accelerator R&D project based at CERN. It is a proof-of-principle experiment investigating the use of plasma wakefields driven by a proton bunch to accelerate charged particles. It is the world's first proton-driven plasma wakefield acceleration experiment and it constitutes an international scientific collaboration involving 14 institutes. The acceleration technique could lead to future colliders of high energy but of a much reduced length when compared to proposed linear accelerators [1].

The facility (Fig. 1) was successfully commissioned between June and November 2016 and the experiment took its first data in the final week of accelerator operations at CERN in 2016.

The control system of this experiment must ensure smooth working conditions of the plasma while ensuring strict control requirements during warm up and stability during normal operation. Special care was taken to bring the process to a safe state when detecting a hazardous event.

This paper shows the engineering lifecycle of the SIS (Safety Instrumented System) and introduces the BPCS (Basic Process Control System) of the AWAKE plasma vapour The major focus is given to functional safety aspects. The goal is to illustrate the issues found and how to overcome them, especially when dealing when predefined instrumentation and a lack of data to make the safety calculations.

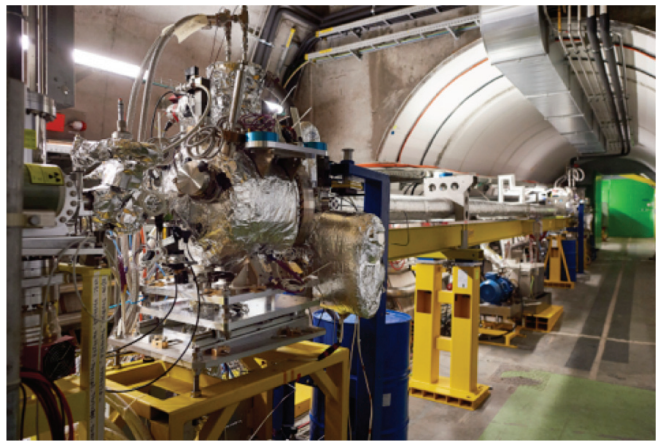

Figure 1: AWAKE plasma cell in the tunnel.

AWAKE Experiment and Its Plasma Cell

The use of plasma to accelerate particles is a potential alternative to traditional accelerating methods that rely on radio-frequency electromagnetic cavities. The AWAKE experiment injects a "drive" bunch of protons from CERN's SPS accelerator into a plasma column created by ionising a gas with a laser. When this bunch interacts with the plasma, it splits into a series of smaller bunches, in a process called self-modulation. As these shorter bunches move through the plasma, they generate a strong wakefield. It is the process of self-modulation that the AWAKE team is investigating, and from which it can infer the creation of the wakefield.

Two independent vapour sources are connected at each end of the 10 metre long plasma cell and are used to provide a flow of hot rubidium (Rb) vapour through the plasma cell during the experiment. The vapour is used to create the rubidium plasma required for wakefield generation within the plasma cell. The Rb flow is achieved by accurately controlling the temperature of the rubidium in each vapour source Rb reservoir. These control temperatures define the upstream and downstream Rb evaporation rates which set the net flow within the plasma cell. In addition, Rb vapour flows into an expansion chamber where it is condensed and solidified ready for recovery.

Industrial Control System

The control system must ensure proper operation of the facility and is composed of: (1) a basic process control system (BPCS): maintaining the whole system in an isothermal, avoiding cold spots and possible intermediate Rb condensation, (2) a safety instrumented system (SIS): providing a safe environment during operation with rubidium by detecting

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

hazardous events and setting the process to a safe state. The SIS design requires a very specific engineering practise [2].

AWAKE PLASMA CELL OPERATING CONDITIONS

The plasma nominal working temperature of about 220 °C is reached by the circulation of Rb gas and the use of several electrical heaters.

The transients and normal operation regimes create challenges for the control system including: (1) keeping the the 10 meters plasma cell as isothermal as possible without noticeable gradients in temperatures, avoiding cold spots and possible intermediate Rb condensation, (2) avoiding temperature dispersion larger than 0.05 °C in some specific places and (3) providing a safe environment during operation with rubidium (Fig. 2).

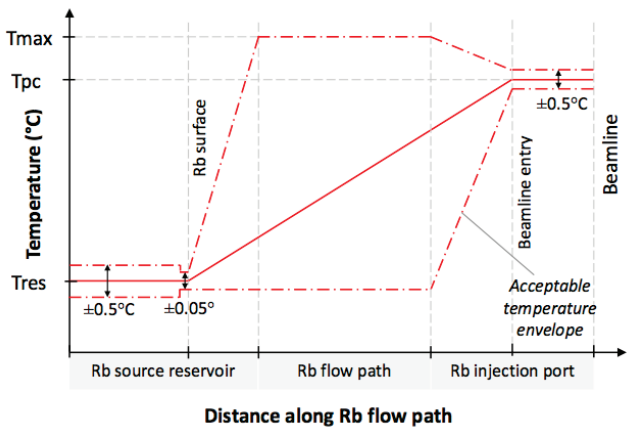

Figure 2: Temperature profile required between reservoir and plasma cell.

Potential Hazards Identification

The procedure to identify and quantify potential sources of harm will be introduced later. Here, the focus is set on listing the identified hazards: (1) the beam induced ionising radiation, (2) the class 4 laser used to ionise the plasma and to drive the electron source areas and, finally, (3) the presence of rubidium [3].

ESSENTIALS TO ENGINEER THE SIS

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs [4]. A widely accepted definition of safety is freedom from unacceptable risk of physical injury or damage to health caused directly or indirectly. The functional safety is practically executed by a SIS as this is designed to prevent or mitigate hazardous events by taking the process to a safe state when predetermined conditions are violated. Any SIS is composed of a combination of logic solver(s), sensor(s), and final element(s). Engineering the SIS is an activity rather standardised but, unfortunately, standards focus on "what" must be done rather than "how" which does not facilitate the final design and implementation.

Safety Lifecycle Engineering

The design lifecycle of a safety system is described in the IEC 61508 [4], IEC 61511 [5] and its associated ANSI/ISA-84.01 [6] standards, the last two customised to the process industry. The lifecycle could be condensed in three main steps: (1) analysis, (2) realisation and (3) operation. Industry records show that up to 40% of accidents are caused by incorrect specifications and this is why the initial phase of the project is of paramount importance. A proper conceptual process and/or machine design together with a hazard analysis and risk assessment must start well before the control equipment is chosen. In this manner, most of the hazards can be suppressed by a correct design of the process.

Analysis The very first activity is the identification of hazards associated with an industrial process. Two factors must be assigned in all identified hazardous events: probability of the event and severity or consequences of that event. Those will be used to assess the level of risk involved. Several techniques can be used, e.g. Hazard and Operability (HAZOP), Failure Modes and Effect Analysis (FMEA) or Fault Tree Analysis among others, and the optimal selection depends on distinct parameters such as cost, organisation structure, adaptability, complexity and usability among others.

Then there must be an analysis with the goal of eliminating the hazardous events, mitigating their consequences or reducing their occurrence likelihood by including protection layers. This is usually done by including process and/or equipment modifications. A Layer Of Protection Analysis (LOPA) approach is usually employed here.

Risk evaluation [R]		Probability of the hazardous event			
		1	2	3	4
Potential severity	A	A1	A2	A3	A4
	B	B1	B2	B3	B4
	C	C1	C2	C3	C4
	D	D1	D2	D3	D4

Figure 3: Risk evaluation table.

The risk evaluation reference table depicted in Fig. 3 shows the severity from A, minimal or negligible, to D, high or catastrophic and the probability of the hazardous event from 1, very low or extremely unlikely to occur, to 4, high or likely to happen several times during the assigned task. The colour zones reflect the acceptance of the risk, varying from acceptable and then no further protection actions are needed (green) to protection actions absolutely needed (orange and red).

The next step is the identification of what has to be done to reduce the probability of occurrence of the hazardous event. The result constitutes the safety instrumented functions. Once they are defined an associated **SIL** (Safety Integrity Level) must be assigned to them. A SIL defines the level of performance needed to achieve the user's process

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

safety objective, so basically this becomes a safety requirement.

Realisation The second phase comprises the design, installation and commissioning of the safety instrumented system. Two major design requirements to meet the specified SIL: the **hardware safety integrity**, quantify random hardware failures and comply with the architectural constraints, and the **systematic safety integrity**, required measures to reduce the systematic faults, e.g. environmental stresses, operator faults, software faults, etc.

In case of non safety certified equipment, several sources can be consulted to get proper figures such as the vendor specifications, maintenance records or other their-party databases where many references are recorded for different industries.

The installation is followed by a commissioning phase with a strict phase of acceptance tests verifying the correct functioning of the safety instrumented functions and ensuring a number of other requirements such as verifying the communication with the BPCS, proper display of events, safety devices tripped at defined requirements, proper shutdown sequences, etc. The phase is completed with the delivery of the SIS documentation.

Operation The SIS must be operated and maintained in a way that sustains the required safety integrity over time. This phase then includes the proof tests of the safety instrumented functions, the periodicity is usually a function of the required SIL, and the procedures for the plant operators. There is also a more elaborate procedure to handle the changes or modifications. This is also a critical point as many accidents are caused by a improper handle of modifications.

BASIC PROCESS CONTROL SYSTEM

The rubidium transits from the downstream flask to the plasma cell in a vapour state. The temperature must be homogenous in the whole system and this is done by the use of different electrical heaters controlled by PID (proportional, integral and derivative) feedback controllers. The temperatures are measured with standard PT100 sensors but with individual calibration to get the desired precision of 0.05 °C. The plasma nominal working temperature is about 220 °C and the stability of the temperature is also a hard constraint during nominal operation.

The resulting control system is based on the classical 3 layer automation pyramid architecture. The field layer contains all the measurement instruments and actuators (i.e. about 100 sensors of temperature, 6 pressure sensors, 8 OnOff valves and 17 PWM heaters). The control layer is based on a PLC (Programmable Logic Controller), the Siemens fail-safe S7-317F-2 PN/DP, which combines basic control with safety classified functionalities. The upper or supervisory layer is based on a commercial SCADA (Supervisory Control and Data Acquisition) system: WinCC OA from Siemens. The design of the control system is based on the UNICOS framework [7], a continuous process control framework based on the ISA-88 standard widely used in industry. The finite state machine located in the PLC (Fig. 4) drives the system to the nominal operation point respecting the strict requirements of temperature gradients.

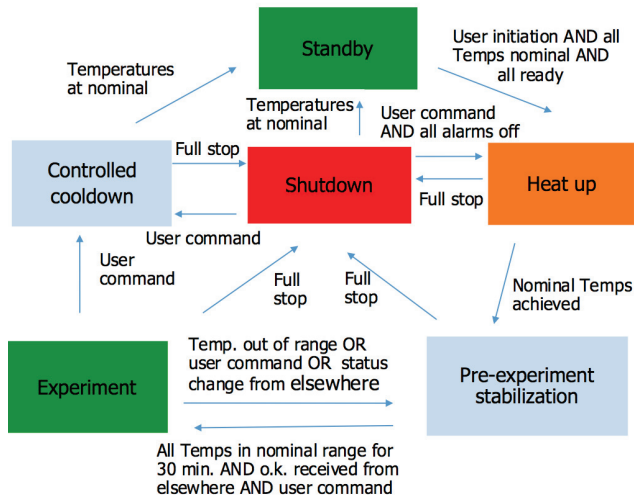

Figure 4: Vapour source simplified control system states.

Within the concept of **multiple layers of protection** and mitigation, the BPCS is indeed one of these layers as well as the configured alarms (e.g. any temperature sensor passing a threshold of 250 °C) which the operators will get in their operation interfaces. However in this case, the BPCS will not take credit for the risk reduction. The credit for the reduction of probability of failure will be only taken by the SIS.

Directive 7.3.4 of the ANSI/ISA-84.01 standard states that the logic solver shall be separated from the BPCS although it opens the door to mixed architectures when properly designed and justified. As stated later, the logic solver for the safety instrumented system is the same PLC as the one used in BPCS. The UNICOS based control system also allows a native interface between the BPCS and the SIS implementation which aids in the operation of the control system. All diagnostics from the SIS are integrated in the BPCS so events and alarms are also visible to operators and maintenance teams.

SAFETY INSTRUMENTED SYSTEM

This section describes the three phases mentioned in the lifecycle of the AWAKE plasma cell SIS.

Analysis

The method employed to perform the **hazard analysis** was the FMEA technique as it was the most appropriate for this kind of processes. This procedure was conducted by process experts who could asses the associated dangers and the identified hazardous events may produce. The main results of the hazard analysis are summarised in Table 1. Note the results of the **risk assessment** in terms of probability and severity of the hazardous events (columns P and S) following

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

the risk evaluation table (Fig. 3). To facilitate the readers' comprehension, many hazards, which were identified and the prevention measures established at the design phase of the facility, are omitted but can be consulted in the project safety file [3].

Table 1: Hazard Analysis Summary

P	S	Hazard	Cause	Effect
1	D	Rb	Oxygen contact	Burning, fire
4	D	Beam	Collisions	Radiation injury
1	C	Laser	Exposure	Eye damage
1	C	Toxic	Overheating	Respiratory

The hazards related to the beam presence and laser operation are already handled by other safety system: the access control. The same applies to the over-temperature of the bath at 290 °C which could drive to the release of HF and COF2. This has been handled by the installation of an independent safety thermal switch as an independent protection mechanism. Therefore they are out the scope of this publication.

The facility contains rubidium, up to 3kg, within the AWAKE plasma cell and vapour sources. Depending on the experimental operating status, the Rb may be in solid form or in a mixture of liquid and vapour. Hazards associated with Rb include contact with water and air. While some risks associated to the hazards can be mitigated via proper installations, e.g. the removal of water sources from experimental area and proper training for the fire brigade interventions, others may not be possible to mitigate in advance. The consequences of rubidium contact with air (oxygen) are: (1) fire and explosion hazard due to hydrogen gas formation during reaction with water vapour, (2) chemical hazard due to the release of corrosive fumes leading to respiratory tract burns, skin burns and eye burn sand (3) heat and fire hazard due to energy given out from exothermic reactions [8].

Therefore the identified **harm** is a physical injury of the personnel close to the installation (burns), rubidium constitutes the **hazard** or potential source of harm and the **hazardous event** is the rubidium contact with air.

The most probable cause of rubidium being in contact with air is a failure of the vapour source structure leading to ingress of air into the plasma cell. The weakest point in that structure are the viewports which are designed to allow a laser-based measurement of the plasma. There are four in total, two in each extremity of the plasma cell. Figure 5 shows the front side of one extremity, the other symmetric viewport is located at the back and a similar structure is located in the other extremity.

The human presence close to the premises is possible in periods without beam or laser activities. A plausible scenario is the periodical rubidium loading and unloading activities or simply the equipment maintenance duties. Therefore, this risk may provoke an injury to personnel due to fire in experimental area as described in the safety file [3].

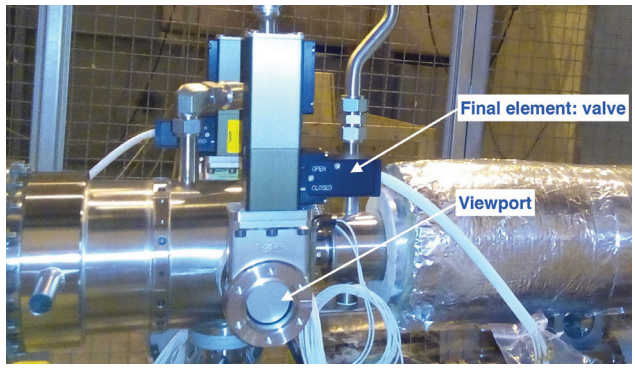

Figure 5: Plasma cell viewport.

Table 2: IEC 61508 Low Demand SIL Determination

SIL	PFDav	TTR
SIL 4	PFDav < 10-4	TRR < 10000
SIL 3	10-4 < PFDavg < 10-3	TRR < 1000
SIL 2	10-3 < PFDavg < 10-2	TRR < 100
SIL 1	10-2 < PFDavg < 10-1	TRR < 10

Based on the results shown in Table 1 the required integrity level was **SIL 2**. The **safety instrumented function** is to isolate the rubidium inside the plasma cell by closing the valves behind the viewports once the vacuum pressure sensors detect a loss of vacuum which indicates a leak of the plasma cell. Table 2 shows the SIL associated with a probability of failure under demand (PFD) showing the target risk reduction (TRR). The mode of operation of the SIF is **Low Demand** due to the estimation by the process experts that the hazardous event occurrence is one or less per year.

This phase is completed by proper documentation which comprises at least the requirements, process information, required safety instrumented function and the associated SIL.

Realisation

A proper SIS must be engineered to cope with the identified and requested SIL 2. The approach taken follows the concept of ALARP (as low as reasonably practicable). The

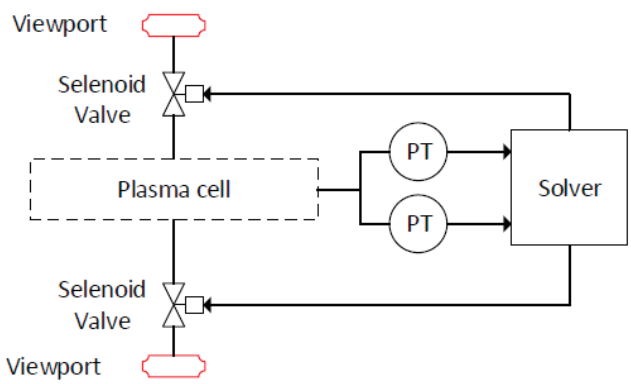

Figure 6: Safety instrumented function Loop.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

safety instrumented function is based on the detection of the presence of air in the rubidium plasma cell by a loss of the high vacuum (Fig. 6). In case of a viewport broken there will be a leak and external air will immediately enter in due to the difference in pressure. Therefore it was decided to use the vacuum pressure sensors as the measurement points. There are two pressure gauge controllers (*Pfeiffer TPG300*) which host two independent *Pirani* sensors each and provides, on top of the pressure engineering value, a binary output signal when a threshold is violated. The standard establishes that the sensors for the SIS shall be separated from the BPCS, although there is an exception which is relevant here, where redundant sensors are used and any failure in the BPCS will not affect the reading of those by the SIS.

The logic solver is a commercial available safety PLC (Siemens *S7-317-2 PN/DP*), these specific PLCs are safety classified as they are design for that purpose. To complete the chosen hardware the logic solver incorporates safety classified remote input/outputs cards (*F-DI 8x24VDC HF* and *F-DQ 4x24VDC/2A PM HF* respectively) plugged in an *ET200 card*. The communications between the logic solver and the remote I/O are done by Profinet using the safety protocol Profisafe which provides assurance to meet the required SIL. The use of a safety PLC among other possibilities (e.g. relays, solid-state systems...) is an evident choice as it allows a natural integration with the BPCS.

The final elements are a valve (*VAT 01032-CE44-X*) per viewport (four in total as there are two viewports in each plasma cell extremity).

As a consequence of this design 4 distinct pressure sensors will monitor the vacuum on the vapour cell. When any of the measurements detects a pressure higher than a predefined threshold of 0.002 mbar, the 4 valves must close to avoid further contact of rubidium with air. The safe state of the safety instrumented function is having the 4 valves closed. If there is a power supply failure or a control system failure, the 4 valves shall automatically move to the safe position.

To achieve the specified SIL 2, two main aspects must be taken into account: first, hardware safety requirements, which contains the hardware random failures and architecture constraints, and, second, systematic safety requirements with tries to minimise all systematic errors.

Hardware Safety Integrity The SIS is comprised of 3 distinct elements, sensors, logic solver and final element or actuator. The three components must be taken into account in the calculation to reach the SIL. Figure 7 shows the safety instrumented function with the real components.

Equation 1 is used to calculate the **probability of failure under demand** (PFD) of a single component. This formula provides an approximation of the PFD based on several factors such as the coverage (C) of the automatic tests, the interval of time between manual tests or proof test frequency (T), the failure rate of each device (λ_D) and the mean time to repair a single device when a failure occurs (MTTR). Two assumptions are made, C=0 as we do not consider any automatic diagnostic coverage and MTTR being insignificant with respect to the mean time to failure (MTTF).

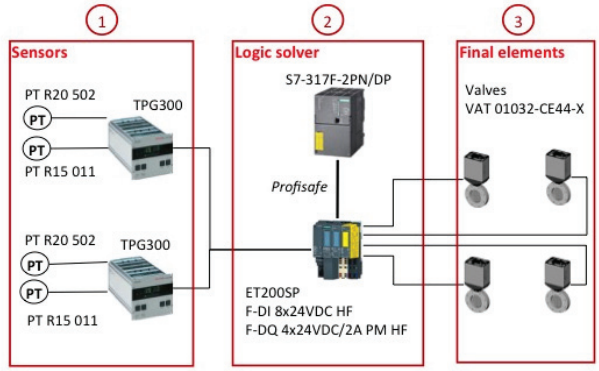

Figure 7: Safety instrumented function architecture.

$$PFD = \lambda_D * \frac{T}{2} \quad (1)$$

Equation 2 calculates the equivalent **probability of failure under demand** (PFD) of the architecture selected (Fig. 7).

$$PFD_{Total} = PFD_1 + PFD_2 + PFD_3 \quad (2)$$

The probability is the sum of the three components: sensors, logic solver and final element. Both TPG300 (together with the pressure sensors) are performing the same action, therefore they are consider as redundant architecture (1oo2: one-out-of-two) and represented as a parallel subsystem in the reliability block diagram (Fig. 8). Yet the TPG300 constitutes a **common case of failure** as it holds the two pressure sensors, and this is taken into account in the second term of the equation (3), where β represents the fraction of failures that have a common cause. The standard provides advice for the value of β using engineering judgement (IEC 61508-6 Annex D). In our case we assigned 25% being very conservative and considering the TPG300 as a field device. The device employed is not safety certified and so we used the manufacturer data. *Pfeiffer* provided a MTTF of 156 years for the TPG300 and this was confirmed by the vacuum experts and the maintenance records at CERN where handreds of these devices are installed.

Considering the relationship of $MTTF=1/\lambda_D$, a proof test frequency (T) of 4 weeks provided by the operation, the result of equation (3) is $PFD_1 = 6.15*10^{-5}$. This PFD of the sensor component corresponds to a SIL 4. Even reducing the test proof frequency to one year and a much more conservative MTTF for the TPG300, the PFD would be in the range of SIL2 thanks the 1002 architecture.

$$PFD_1 = \frac{\lambda_D^2 * T^2}{3} + \beta\frac{\lambda_D * T}{2} \quad (3)$$

This analysis reveals that from the hardware random failure point of view, the sensor component complies enterely with the SIL2 requirements.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

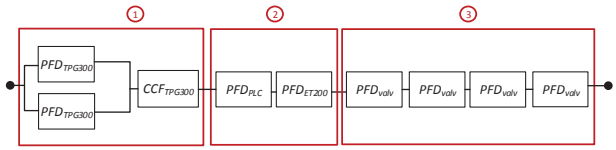

Figure 8: Reliability Block Diagram.

The second component, the logic solver has two separate subsystems, the PLC itself and the remote I/O system which are added as they are in series. The data for the analysis is given by the supplier as stated in the IEC 61511 standard as all components are safety classified. Therefore the whole logic solver, being a safety classified PLC, reaches a SIL3 from the SIEMENS documentation ($10^{-4} < \text{PFD}_2 < 10^{-3}$). Therefore the PDF_2 is not a limitation to reach the global SIL2 target from the random failures point of view.

For the final element, 4 valves need to be closed when a loss of vacuum occurs, therefore they are represented as a series of subsystems in the reliability block diagram and therefore calculated as 4 times the PFD of each valve. Due to the lack of information provided by the manufacturer, *VAT*, it was not possible to prove its SIL compliance, the only input provided by the supplier was the number of 50000 cycles until the first service, although this is not really relevant.

Therefore the safety analysis for the final element component was inverted. The goal is to calculate the necessary characteristics of these valves to make the final SIF compliant with SIL2. Results are shown in table 3 considering the relationship of MTTF=$1/\lambda_D$, the proof test frequency (T) of 4 weeks provided by the operation, equation (4) and the boundaries to be compliant with SIL 2: $10^{-3} < \text{PFD}_{avg} < 10^{-2}$.

$$\lambda_{D_{valve}} = PFD_3/(2 * T) \tag{4}$$

Table 3: Valve SIL 2 PFD Boundaries

PFD_3	PFD_{valve}	λ_D	MTTF
10^{-2}	PFD_3/4=0.0025	$6.518*10^{-2}$	15.34
10^{-3}	PFD_3/4=0.00025	$6.518*10^{-3}$	154

From the safety point view, the 4 valves are potentially the devices which decrease the whole reliability of the SIF. The conclusion is that, imposing a proof test frequency of 4 weeks, the valves must have a MTTF larger than 15.34 years. This MTTF requirement could be alleviated by increasing the proof test frequency of the valves. To ensure the SIL and then accomplish the proposed proof test frequency the sequencer of the BPCS does not allow any experimental campaign without performing the compulsory test in the heat up phase (Fig. 4). In that phase, the proof test procedure should be carried out systematically (i.e. the valves are actuated in open-close sequences and the end-switches checked). This is an advantage of sharing the BPCS and SIS in the same control unit.

The architectural constrains based on hardware fault tolerance (HFT) and safe failure fraction (SFF), *Route* 1_H, have also been analysed. The IEC 61508 7.4.4.2.1 provides tabulations of the reached SIL with HFT and SFF inputs. Considering the valves being of type A (low complexity elements) and the given architecture with no redundancy or HFT=0, SIL 2 can be reached if the SFF is between 60% and 90%. SFF is defined as the ratio of the average rate of safe plus dangerous detected failures to the total average failure rate of the component. If the valve does not meet this SFF value then the HFT must be 1 (valve redundancy).

The sensor component, type B as it is considered as complex system, gets the same requirement for the SFF with HFT=1 (redundant TPG300). Alternatively, using the *Route* 2_H approach and the reliability data from users feedback, the component ratifies the required SIL 2.

Systematic Safety Integrity Systematic capability is a measure of the confidence that the systematic safety integrity of an element meets the requirements of the specific SIL and it is notated as SC in a scale from 1 to 4. The individual TPG300s are compliant with the SC1 requirements (e.g. failure detection by online monitoring, environmental stress, electromagnetic interference, etc.), therefore the sensors component can claim a SC2 as both separated and redundant TPG300 units behaves as a fault tolerant system.

For the solver component, Siemens guaranties the SIL 3 compliance for the systematic failures. In addition, the application software (PLC program) must meet the SIL 2 requirements according to the IEC 61511. This is a critical point as the quality of that software is crucial to ensure the safety instrumented function action. The PLC program was developed using the Siemens Distributed Safety Library and the Ladder PLC language as it is one of the standardised IEC 61131-3 languages with limited variability. When dealing with safety control systems special care is given to the safety program and this is why a formal verification method is applied. The SIF has been formally verified using model checking. For that purpose, the tool PLCVerif [9] developed at CERN has been applied. Model checking is a formal verification technique that takes a mathematical model of the system to be verified and a formalised requirement and can decide if the given requirement is satisfied.

Tests are done during installation and commissioning. The test approach follows the guidelines given by the ANSI/ISA-62381-2011 standard. A dedicated FAT (Factory Acceptance Test) is done in the lab where all safety instrumented functions are triggered and validated on top of all the requirements for the BPCS (i.e. I/O connectivity, actuators state in the different finite state machine, alarms and interlocks). This is followed by a SAT (Site Acceptance Test) where all is repeated when connected to the real plant.

Operation

The operation of the SIS and the BPCS is performed using interfaces (human-machine) where all control and process information can be monitored, this is provided by

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA01

the UNICOS framework where alarms, interlocks and events are shown to the operator. In contrast to the BPCS where some control parameters could be modified online, changes to the SIS application software can not be done through the interface. Proof testing (including Functional testing) must be done periodically in order to verify the correct operation of a SIS assessing the design SIL level. Contrary to the BPCS where many failures are self-revealing as the final control elements are highly solicited, the SIS final elements may be dormant and not used during long periods of time. The critical valves are functionally tested every four weeks.

Management of change (MOC) is another activity of crucial importance. Many accidents have been caused by an improper change on the SIS and/or BPCS. The procedure and guidelines are given by the ANSI/ISA-84.00.01 and essentially it is applicable to any change to the SIS. The changes must be properly documented and revised by all stakeholders to be sure that undesired effects are not introduced.

CONCLUSIONS

The safety instrumented system of the AWAKE plasma cell was conceived, designed and finally implemented in 2016 contributing to the success and safe operation of the AWAKE experiment. The engineering of the SIS was the use case of this publication with the aim of highlighting the significance of this kind of functional safety systems. The engineering lifecycle followed the standards IEC 61508 and specifically IEC 61511 for the process control industries.

During the first phases of the project it was clear that proper engineering of the facility was needed as a first measure to eliminate hazards which otherwise could jeopardise or complicate the design of the SIS. The risk analysis was conducted by process experts but needed several iterations with the CERN safety experts, the facility operation team and the control system engineers.

Many factors were taken into account during the SIS design, notably the architecture and the technology used, but also the compliance with the requirements for systematic safety integrity and in particular the avoidance of systematic failures in the logic by formal verification methods. Additional data could be used when calculating the SIL required, especially when instruments are not safety classified such as the case of the plasma cell, and many other high energy institutes installations also. This is a complexity which could be overcome by using other sources of information such as maintenance databases and experts experience, as shown in the publication. Apart from the instruments themselves, proof test coverage is crucial to meet the required SIL. The SIL calculations revealed a constraint on the valves used and, indeed, one of the improvements proposed is the change of the valves to be sure that they would achieve the required SIL, respecting the hardware and the systematic requirements. Use of non safety classified instruments is possible but many considerations must be taken into account such as hardware random and systematic failures as well as architectural constraints.

It must be clear that a BPCS will never act as a SIS although this is something that regularly happens on this kind of installations where engineers assimilate safety classified functionality to the BPCS with the risk that this may induce. However, it has been shown that it is possible to share the logic solver between BPCS and SIS. The overall engineering was facilitated by following the UNICOS standard which allows a rapid development of the BPCS and a standardised operation interface shared with the SIS.

During the operational phase, the management of change of the operational control system must be performed thoughtfully as a single modification may produce unpredictable collateral effects if not properly analysed and validated. Also the proof test frequency is of great importance as the SIL requirement must be kept in time. Finally, one important point for any organisation is to have a clear management of functional safety. This implies the establishment of the risk analysis standards within the institute, a proper workflow with clear organisation and resources and capabilities to assess and audit the SIS engineering.

ACKNOWLEDGEMENT

The authors want to thank the CERN AWAKE project team, the Max-Plank Institute and the consultancy firm Wright Design Limited for the fruitful collaboration in this project.

REFERENCES

[1] C. Bracco *et al.*, "AWAKE: A proton-driven plasma wakefield acceleration experiment at CERN", Nuclear and Particle Physics Proceedings, Volumes 273–275, April–June 2016, Pages 175–180.

[2] P. Gruhm, "Safety Instrumented Systems: Design, Analysis and Justification," ISA - The Instrumentation, Systems and Automation Society, Research Triangle Park, NC 27709, USA.

[3] C. Alanzeau *et al.*, "AWAKE safety file", CERN, Tech. Rep. 2016 EDMS 1730672.

[4] "IEC 61508", Technical report, International Electrotechnical Commission.

[5] "IEC 61511", Technical report, International Electrotechnical Commission.

[6] "ANSI/ISA-84.01 Application of Safety Instrumented Systems for the Process Industry" ANSI/ISA-81.01-1996.

[7] E. Blanco Vinuela, et al.," UNICOS evolution: CPC version 6", in Proc. of 12th ICALEPCS, 2011.

[8] P. Muggli "AWAKE rubidium material hazard analysis", CERN, Tech. Rep. 2016 EDMS 1730672.

[9] D. Darvas, B. Fernandez, E. Blanco Vinuela, "PLCverif: A tool to verify PLC programs based on model checking techniques", in Proc. 15th Int. Conf. on Accelerator and Large Experimental Physics Control Systems. JACoW, 2015, pp. 911–914.