THE APPLICATION OF SIL

POSITION PAPER OF THE SIL PLATFORM

NEN

SIL Platform

1. The Application of SIL: Position Paper of the SIL Platform

What is the SIL Platform?	The SIL Platform is an independent group of experienced users or adopters of the SIL philosophy, according to the IEC standards 61508:2010 and 61511:2003, in the Dutch process industry. The SIL Platform is linked to the Royal Dutch national standardization committee NEC 65 that follows the international work of IEC/TC65, industrial measurement, control and automation. At the time of release of this document, 40 people, representing end-users, engineering companies, suppliers, manufacturers and consultancy firms, are a member of the SIL Platform.
Why issue a SIL statement?	It is the intention of the SIL Platform to issue a SIL related document. The objective of this document is to inform the market and create awareness about specific issues with the application of SIL in the process industry. The document provides basic information about the implementation of SIL, the relevant terminology, and focuses specifically on the SIL verification process to establish an adequate integrity of SIL loops.
What are the basics of SIL implementation?	It is common practice to operate process plants at maximum performance, optimum capacity and minimum risk levels. Key Performance Indicators are used to measure and control realistic targets and objectives. A means of quantifying risk has been introduced a decade ago and is expressed as SIL (Safety Integrity Level). SIL can basically be seen as a numeral indication, scaled from SIL1 to SIL4, of the magnitude of the risk level. Relative to this, it also corresponds to the integrity level of a safety system that reduces the risk. During a hazard and operability study (HAZOP), potential risks per process node are identified and will have to be verified as correct and complete. HAZOP is a structured and systematic examination of a planned or existing process or operation, so as to be able to identify and evaluate any hazards. The next step consists of a risk assessment, also known as a SIL Classification that, due to verification requirements, needs to be separate from the HAZOP activity. In this classification, activity, company, process type, risk graphs or risk matrices are used as a reference. No further action is required when risks are classified as 'acceptable'. When a risk is not acceptable, the magnitude in factors of ten is established. SIL 1 means that the risk of that process node is a factor ten too high. At SIL 2, the risk level is a factor 100 too high, and so on. The consequence of the SIL classification is that when a hazard node has a risk level of SIL 2, you are obliged to reduce that risk by a factor of at least 100 for it to become acceptable. This factor is called the risk reduction factor (RRF). SIL related risk reduction is, by definition, achieved with electric, electronic or programmable electronic (E/E/PE) safety systems. The process is monitored by the so-called sensing element, usually a measuring transmitter. When the process exceeds a specific safety value, an output element would have to influence it in such a way that the process at risk is brought back to a safe state. A logic solver is programmed to change an output state to a valve or relays contact (final element), when an input exceeds a pre-set value. The connected sensing element, logic solver and final element are called the safety loop and perform the safety instrumented function (SIF). These components collectively form the safety instrumented system, or SIS. By definition, the Safety Integrity Level, SIL, is related to the Safety Instrumented Function SIF, and not to the individual components.

Continued on next page

How do I establish an adequate SIL implementation?	During the SIL Classification process, SIL levels are linked to specific process hazards, which in turn set the demands for the integrity of the safety instrumented function (SIF) and the related equipment. It should be clear that HAZOP, SIL Classification and SIL Verification would have to be treated with equal high level importance and quality. In the following chapters of this document, we will focus on the value and sources of failure rate data, instrument certification, statistical calculations, test principles, interpretation of diagnostic data, i.e. the loop design, failure analysis and number crunching that leads to the proof of the safety loop's integrity.
Which subjects are dealt with in this position paper?	This position paper deals with the following subjects: 2. Systematic design approach, page 3 3. Instrument failure data, page 5 4. Use of Diagnostic Coverage (DC) factor and Safe Failure Fraction (SFF), page 6 5. Hardware safety integrity architectural constraints, page 9 6. Proof tests of Safety Instrumented Systems, page 11 7. Safety Life Cycle Management, page 14

2. Systematic design approach

What is a systematic design approach?	A systematic design approach is aimed at eliminating the occurrence of systematic failures. Systematic failures deterministically relate to a certain cause, which can only be eliminated by a modification of the design, or the manufacturing process, operational procedures or other relevant factors.
Why is a systematic design approach important?	Studies show that the majority of control system failures leading to incidents are caused by failures that could have been prevented if a systematic risk-based design approach had been used throughout the lifecycle of the system. See "Out of Control", published by HSE, for details.
What are the pitfalls in establishing a systematic design approach?	*Incomplete specifications* Engineers are trained to provide solutions. However, this may lead to a drive to proceed to the design phase before a complete set of specifications has been obtained. The studies mentioned above indicate that 44% of incidents can be attributed to inadequacies in the specification of the control system. The most frequently occurring short-comings are: • A poor hazard analysis of the equipment under control • An inadequate assessment of the impact of failure modes of the control system on the specification *Too much focus on calculations* Reliability engineering is based on statistics. Calculating the PFD involves values for certain factors, e.g. the diagnostic coverage and the common cause failure, that are subjected to certain conditions. The calculation of the PFD will only result in a valid result if these conditions are met The validity of these assumed conditions should be verified carefully, in relation to the actual conditions under which the system will operate.
How do I establish a systematic design approach?	*Management involvement* Management involvement is critical in establishing a systematic design approach and must occur in each phase in the safety lifecycle. Management is responsible for: • Defining the policy and strategy for achieving safety • Evaluating the achievement of safety • Organizing communication within the organization • Introducing a safety management system to ensure that wherever safety instrumented systems are used, people have the ability to place and/or maintain the process in a safe state • Training the people involved in safety lifecycle activities, in order to ensure their competence • Implementing procedures for design, validation and assessment activities

Continued on next page

2. Systematic design approach *continued*

Adequate specifications

An important and normative requirement is the 'Safety Requirement Specification', called SRS. The SRS is a very important document, as all relevant data concerning each particular SIF, including detailed data of each element and a diagram of the Safety Loop, have to be collected and mentioned.

This Safety Requirement Specifications should be:

- Clear
- Precise
- Verifiable
- Maintainable
- Feasible

The specifications should be written so that they are easily understood by anyone using them. The specifications should cover all phases of the safety lifecycle.

The safety requirements (SRS: 61511-1, 10.3.1) shall, for example, include:

- A description of the safety instrumented function
- A definition of the safe state of the process
- The response time for a safety instrumented function for bringing the process to a safe state
- The mode of operation (demand / continuous)
- De-energize (or in specific cases, energize) to trip
- The requirements for resetting the SIS after a shutdown
- The software requirements
- The environmental conditions (temperature, EMC, Shock, vibration, electrostatic discharge, etc.)
- Common cause (beta factor) data
- Proof test time
- Mean time to repair (MTTR)

3. Instrument failure data

What is instrument failure data?	Instrument failure data is information on expected reliability and integrity of each element in a SIF-loop provided by the manufacturer. It consists of four different parameters: dangerous detected and undetected failures as well as safe detected and undetected failures (resp. λ_{dd}, λ_{du}, λ_{sd}, λ_{su}). It is expressed in number of failures in time, in which time can be expressed in hours or years.
Why is instrument failure data important?	Instrument failure data is used when calculating the safety integrity of safety instrumented functions.
What are the pitfalls in using instrument failure data?	The biggest pitfall in using instrument failure data is applying the numbers as exact parameters. Using instrument failure data requires an assessment of the validity of the provided data under the actual operational conditions. The following aspects influence the validity of the provided data. *Limited sources* In practice, manufacturers determine instrument failure data by using information from various sources. One such source is returned instruments or devices. However, only a small portion of failed instruments is returned to the manufacturer. This leads to unrealistic instrument failure data. *Operating conditions* Instrument failure data are determined under certain operating conditions. When the actual operating conditions (e.g. the presence of chemical agents, or the occurrence of extreme temperatures) differ from the operating conditions under which the failure data is determined, then the failure data will not reflect reality. *Misfit with actual use of instrument or device* Instrument failure data might express other information than what is relevant for the particular usage of the instrument or device. For instance, a device that is claimed to be able to switch over 10^7 times in its lifecycle might only need to be de-energized after more than 5 years of operation. It may very well occur that the device remains in its energized position due to remnant magnetic energy. Clearly, for this application, the instrument failure data does not provide the relevant information.

Continued on next page

3. Instrument failure data *continued*

How do I correctly apply instrument failure data?

Instrument failure data should not be used as exact parameters, but should be used along with all relevant operational conditions. One should always consider to what extent the provided instrument failure data is valid under the operational conditions under which the instrument or device will be used.
Instrument failure data should be considered relative to the systematic failures and systematic capability (SC). Systematic Failures are failures that, related in a deterministic way to a certain cause, can only be eliminated by a modification of the design or manufacturing process, operational procedures, documentation or other relevant factors. SC is defined as a measure, expressed on a scale from SIL 1 to 4 (SC 1 to 4), the confidence of the systematic safety integrity of an element meeting the requirements of the specified target SIL, with regard to the specified element safety function (when the element/device is applied in accordance with the instructions specified in the relevant Safety Manual for the element/device). The Safety Manual, provided by the manufacturer, contains all required information, on a Safety Related element and how to use it in a particular process application within the mentioned specifications as well as all information about calculations and an assessment of the Systematic Capability and FSM (Functional Safety Management).

Every SIF needs to comply with four main requirements as stated in the standards:

1. Random Hardware failures. In the total safety loop expressed in the PFD figure and indicating the achieved SIL.
2. Systematic failures. (Software/Production/Testing/Modifications etc.) Expressed in the Systematic Capability (SC 1 – 4).
3. Architectural constraints. A normative quality factor concerning the hardware failure data.
4. Functional Safety Management (FSM) system implemented in the manufacturer's production facilities of the elements used in the safety loops. It is practical that manufactures have a site assessment report with an ISO 9001/2/3 certificate, complete with extensive Modification and Product test procedures.

4. Use of Diagnostic Coverage (DC) factor and Safe Failure Fraction (SFF)

What are the DC and the SFF?

The Diagnostic Coverage factor is defined by IEC 61511-1 (section 3.2.15) as the ratio of the detected failure rate to the total failure rate of the component, or subsystem, as detected by diagnostic tests. The diagnostic coverage does not include any faults detected by proof tests. The formula for DC is:

$DC = (\lambda_{sd} + \lambda_{dd}) / (\lambda_{sd} + \lambda_{dd} + \lambda_{su} + \lambda_{du})$

Where:

λ_{sd} = safe detected failure rate
λ_{su} = safe undetected failure rate
λ_{dd} = dangerous detected failure rate
λ_{du} = dangerous undetected failure rate

The following distinction can be made for safety applications:

$DC_s = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$.
$DC_d = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$.

The Safe Failure Fraction (SFF) is defined by IEC 61511-1 (section 3.2.65.1) as the fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure. The SFF is similarly defined by IEC 61508-4 (section 3.6.15) as a property of a safety related element, which is defined by the ratio of the average failure rates of safe plus dangerous detected and safe plus dangerous failures. The SFF can therefore be seen as a kind of quality factor of the derived failure figures. The formula for SFF is:

$SFF = (\lambda_{sd} + \lambda_{su} + \lambda_{dd}) / (\lambda_{sd} + \lambda_{dd} + \lambda_{su} + \lambda_{du})$.

Please note that the only difference between DC and SFF is de component λ_{su}. For mechanical devices, DC = 0 by definition, and SFF = $\lambda_{su} / (\lambda_{su} + \lambda_{du})$; in this case, a high SFF will imply a relatively high spurious trip rate!

Why are the DC and the SFF important?

The DC factor is used to split the overall failure rate components into detected and undetected components. A vendor may publish the DC (or DC_s and DC_d) and the overall safe and dangerous failure rates, or he may publish the individual failure rates (λ_{sd}, λ_{dd}, λ_{su}, λ_{du}). The latter is favored.

The SFF is used to define the Hardware Fault Tolerance, i.e. the required hardware redundancy. A vendor may publish the SFF and the overall safe and dangerous failure rates, but the individual failure rates should always be published.

The individual failure rates and the factors DC and SFF are used to calculate the average value of the Probability of Failure on Demand (PFDavg). This value demonstrates the integrity of the safety loop that performs the Safety Instrumented Function (SIF). Component failures of a SIF may result in a safe process condition (i.e. a spurious shutdown) or a dangerous process condition. Component failures of a SIF may be detected (or not) by the SIF before a process demand occurs.

Continued on next page

4. Use of Diagnostic Coverage (DC) factor and Safe Failure Fraction (SFF) *continued*

What are the pitfalls of using the DC and SFF?

Detected failures
When the SFF is used in SIL verification calculations, the assumption is that dangerous detected failures may be considered as safe failures (i.e. the process is forced into the safe condition, or the operator is taking alternative action). This is in practice not always the case. An example is a transmitter, which automatically detects an internal failure (usually called BAD_PV). The question is what the Safety Instrumented System should do when a BAD_PV is detected? Will it alarm or will it trip? Tripping is safe, but these spurious trips reduce plant availability. Alarming may be safe under certain conditions: when the operator has the time and means available to adequately respond to these critical alarms within the process time. If this is not the case, a trip shall follow, as the SFF is used with that assumption in the calculations.

Accuracy of failure rate data
The failure rate data, the DC factor(s) and SFF are usually determined by the instrument vendor or, upon the request of the instrument vendor, by independent organizations like TÜV or Exida, based on laboratory tests or (mathematical) Failure Modes, Effects & Diagnostics Analysis (FMEDA). Laboratory tests cannot accurately determine the failure rate parameters, while the real-life condition of a SIF cannot be accurately simulated in a laboratory test. In real-life, a SIF is typically activated only once per 10 years (low demand operation) or during Proof Testing at regular intervals.

FMEDA
The FMEDA is a mathematical approach based on the instrument design with standard components and on extensive component failure databases. The impact of process conditions (e.g. vibration, temperature changes) is usually not included, however, failure effects of components are based on practical experience within vendor specified operating conditions. Sometimes the so-called “No-effect” failures or “No-part” failures were also included as safe failures (either detected or undetected). IEC-61508 (2010) explicitly requires that these failures should not play any part in the calculation of the diagnostic coverage or safe failure fraction (IEC-61508-2 (2010), Annex C). It is therefore required to verify that the FMEDA is based on the latest edition.

Proven in use
Alternatively end-users may collect failure rate data from practical experience, or use commercial databases based on practical experience (e.g. OREDA) and derive the DC factor and SFF from that data. Unfortunately that is only possible for instruments that have been in operation for about 10 years or more, for obvious reasons.

Continued on next page

4. Use of Diagnostic Coverage (DC) factor and Safe Failure Fraction (SFF) *continued*

How do I correctly use the DC and SFF?	• When estimating DC, credit may only be taken for diagnostic tests which are executed at, or above, the required frequencies (IEC-61508-2, sections 7.4.4.1.4 and 5). • By definition, the DC for mechanical equipment will be 0, and the SFF will be λ_{su} / total failure rate; in other words: a high SFF will imply a relatively high spurious trip rate. • If the SFF is used in your calculations, investigate if dangerous detected failures may indeed be treated as safe failures. • The SFF and DC should be based on IEC-61508 Edition 2.0 (2010), because it excludes the “No part” and “No effect” failures. Otherwise, the SFF and DC may have a too optimistic number.

5. Hardware safety integrity architectural constraints

What are hardware safety integrity architectural constraints?	Edition 2010 of the IEC 61508 defines 2 routes to establish the required Hardware Fault Tolerance (HFT). Route 1H is applicable for electronic systems, whereas Route 2H can be used for both electronic and mechanical equipment.
Why are hardware safety integrity architectural constraints important?	Next to the Probability of Failure on Demand (PFD) calculation to assure that the PFD of the loop is in line with the required SIL, the architectural constraints as defined in the IEC standard define the number of elements in the loop.
What are the pitfalls in establishing hardware safety integrity architectural constraints?	In Route 1H (IEC 61508-2 section 7.4.4.2), the Safe Failure Fraction (SFF) of the system is used to define the required HFT. As indicated above, the SFF is not really applicable to mechanical devices, which are usually seen as a final element. The new definition of the diagnostic test interval is specifically for electronic equipment, and does not apply for mechanical devices. In the low demand mode, the diagnostics test interval should be shorter than the Mean Time To Restore (MTTR) used in the calculation, minus the time to repair the detected failure. While the MTTR is often assumed as 8-24 hours, this is difficult to achieve for non-electronic equipment. Route 1H defines the HFT based on 2 tables, one for type A equipment and the other for type B equipment. With reference to IEC6108-2 (sections 7.4.4.1.2 and 7.4.4.1.3), the definition of type A or type B is based on the complexity of the element. Elements with microprocessors and software are B types. Mechanical equipment and electronic equipment without microprocessors and SW are basically A types. For mechanical equipment, this selection may also depend on your application, which will be carefully considered . For instance, a large size valve / actuator will usually close in dozens of seconds, and is considered as type A equipment. However, when the same equipment needs to close within a couple of seconds, there are no dependable failure data. The application now requires the equipment to be classified as type B equipment. Once both the SFF and type A or B are defined, the required HFT of the device can be found in the table.

Continued on next page

5. Hardware safety integrity architectural constraints *continued*

How do I correctly establish hardware safety integrity architectural constraints?	*Prior use data* The new route 2H (IEC 61508-2 section 7.4.4.3) is based on the prior use / proven in use, as also described in IEC 61511 version 2003. In applications requiring a SIL3 (either in high or low demand mode) or SIL2 in the high demand mode only, a hardware fault tolerance of 1 - and thus an 1oo2 configuration - is required (when the element is proven in use). Although the term “proven in use” is quite clear, the IEC sets specific requirements (IEC 61508-2, section 7.4.10). To “prove the use”, statistical data must be available for the same application, the same type of process, or application profile, and all aspects of the application and safety mission must be verified. E.g. in case failure data are available based on regular operation or regular switching and now the application requires the element to remain in the same position for a long time, then the term ‘proven in use’ can no longer be applied. The latter part also applies for route 1H, where dependable failure data are required (IEC 61508-2, section 7.4.9.3 – 5), dependable meaning that there must be enough confidence in the equipment being suitable for the application.

6. Proof tests of Safety Instrumented Systems

What are proof tests of Safety Instrumented Systems?	Proof tests are periodic tests, used for detecting dangerous hidden failures in a safety system.
Why are proof tests of Safety Instrumented Systems important?	Proof tests will reveal undetected faults in a safety instrumented system (if any) so that, if necessary, the system can be restored (as quickly as possible) to its initial designed functionality.
What are the pitfalls of performing proof tests of Safety Instrumented Systems?	*Using software calculation tools* Some advanced PFD calculation software programs can calculate the consequences of a Proof Test Coverage factor (abbr. PTC) < 100%, the PTC should be entered, as well as the SIF's lifetime. The mathematical model may, however, not fully represent the real situation, because a poor PFD due to bad testing in the mathematic model can be compensated for by more frequent (poor) proof tests.
How do I correctly perform adequate proof tests of Safety Instrumented Systems?	*Test interval* The proof test interval is related to the average PFD of the SIF. In order to meet the requirements of the determined target SIL of a SIF, the proof test interval may not exceed the test period used in the calculations (usually 1, 2, 3 or 4 years). *Tests* A complete, functional Proof Test (PTC of 100%, an entire process to process test) should always be the target. Sensors must be tested, if possible, by varying the process value. If separated channels are used, separate tests should be carried out for each channel. If valve leakage leads to the dangerous scenario, the valve tightness must also be proof tested. In case the process safety time is critical, the SIF response time must also be tested.

Continued on next page

6. Proof test of Safety Instrumented Systems *continued*

How do I correctly establish proof tests of Safety Instrumented Systems?

Safety Requirements Specification (SRS)

The Safety Requirements Specification must, besides standard design considerations, also contain the requirements, constraints, functions and facilities of each SIF, in order to enable the periodical proof testing of each SIF.

The proof test interval must be defined (based on maintenance procedures and PFD calculation).

Especially when on-line proof testing is required, test facilities must be an integral part of the SIF design, so as to be able to test for undetected failures. When test and/or bypass facilities are included in the SIF, they must comply with the following:

- The SIF must be designed in accordance with the maintenance and testing requirements defined in the safety requirement specifications.
- The operator must be alerted about any bypass that is part of the SIF via an alarm and/or operating procedure. The use of bypasses should be avoided as much as possible.

Maintenance procedures and proof test procedures

Proof tests must be documented in the maintenance procedures covering the following:

- When proof tests should be performed.
- The actions that need to be carried out for a SIF's proof test . Written proof test procedures must be developed in detail for every SIF, so as to be able to reveal any dangerous failures. These written test procedures must describe every step that is to be performed, and must include the correct operation of each sensor and final element, logic action and alarms and indications. The development of the proof test procedures is a very important tailor-made multidisciplinary activity, and must be conducted prior to initial startup.
- The actions and constraints necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (for example, when a system needs to be bypassed for testing or maintenance, what additional mitigation steps need to be implemented).
- Calibration of sensors.
- Test equipment used during normal maintenance activities is properly calibrated and maintained.

Continued on next page

6. Proof test of Safety Instrumented Systems *continued*

How do I correctly perform adequate proof tests of Safety Instrumented Systems?	*Proof testing* Periodic proof tests shall be conducted by means of written and approved proof test procedures. The entire SIF will be tested, including the sensor(s), the logic solver and the final element(s). Different parts of the SIF may require different test intervals, for example, the logic solver may require a different test interval than the sensors or final elements. Any deficiencies found during the proof testing must be repaired in a safe and timely manner. Any change to application logic requires full proof testing. Exceptions to this are tolerated when appropriate review and partial testing of changes are carried out to ensure that the changes have been correctly implemented. During proof testing, the SIF will also be visually inspected, to ensure that there is no unauthorized modification and no observable deterioration (for example, missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing and missing insulation). *Proof test documentation* The results of each proof test must be recorded, in order to prove that proof tests and inspections were completed as required. These records must include at least the following information: a) Description of the tests and inspections performed b) Dates of the tests and inspections c) Name of the person(s) who performed the tests, verifications and inspections d) Serial number, or other unique identifier of the system under test (for example, loop number, tag number, equipment number, and SIF number) e) Results of the tests and inspection (for example, “as-found” and “as-left” conditions) f) Corrective actions, if any g) Signed bypass document, with date and time, bypasses are added and removed

7. Safety Life Cycle Management

What is safety lifecycle management?	The safety lifecycle, by definition of the standard, covers the period that starts with the conceptual design to the moment that the safety system is taken out of service.
Why is safety lifecycle management important?	Integrity of a safety system is initially established during the design phase. This integrity might be compromised during any other phase of the lifecycle of the system, for instance, the operational phase. Safety life cycle management ensures that the integrity of a safety system is maintained throughout all phases of the lifecycle of the system or installation.
What are the pitfalls in establishing safety lifecycle management?	*Too little attention for safety integrity during later phases in the lifecycle* When management decides to adopt the SIL philosophy, most effort is spent on the design and during the installation phase. After commissioning and start-up begins the longest period with important SIL focus, the operational phase. The safety loop is often not inspected, tested and maintained as well as it was during the design phase. *Exceeding test intervals* Testing is performed to prove the SIF's adequate functioning. The test interval is directly related to the PFD values of the safety loop. Postponing the test beyond the original test interval immediately creates a non-acceptable risk in that loop.
How do I correctly establish safety lifecycle management?	*Fault analysis* When the tests show a failure, it is important to find out when the failure originally occurred, and what caused it. A detailed analysis is required. Are there any other devices in the installation that might have the same problem? *Repairs* The proof test is a periodic test performed to detect dangerous hidden failures in a safety system. Repair is required to restore the safety system back into a fully functional condition. Be aware that the effectiveness of the proof test will depend on both failure coverage and repair effectiveness. In practice, detecting 100 % of the hidden dangerous failures is not easily achieved. The target should be that all safety functions are checked according to the E/E/PE system safety requirements specification. *Company policy* It is important to have company procedures for embedding SIL proof tests as standard practices within the relevant departments. Finally, we wish to state that the application of SIL requires a continuous ACTIVITY throughout the entire lifecycle of a process installation.

AUTHORS

Willem van der Bijl	CH 01 & 07	Safety Consultant & M.D.	PRODUCA Consultancy BV
Henrie Verwey	CH 02	Sr. Safety Consultant	Verwey Safety Services
Hans van Dongen	CH 03	SIS & Alarm Management Guardian	Du Pont de Nemours
André Fijan	CH 04	Process Control & Safety Engineer	Fluor BV
Rens Wolters	CH 05	Application Specialist SIL/HIPPS	Mokveld Valves BV
Herman Jansen	CH 06	Process Safety Consultant	Consiltant BV

SIL Platform