CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977093

Paperless Safety Lifecycle

Stefan Hack*, Matthias Lange

R. STAHL Schaltgeräte GmbH, Am Bahnhof 30, 74638 Waldenburg
Stefan.Hack@Stahl.de

To ensure the functionality of safety systems in plants, maintenance is required. Plant operators are obliged to perform inspections, evaluate the results and archive the protocols.
Inspection plans and intervals vary deeply depending on the kind of equipment, the legal basis and the standards that are taken into account. Safety integrated systems according to IEC 61508/61511 have to fulfil a certain safety integrity level (SIL). The proof-test interval amounts into the SIL calculation. A typical interval is twelve month, which leads to frequent inspections. Equipment for hazardous areas in terms of explosion protection also needs to be inspected periodically. Depending on national legislation, a typical interval can be 36 Month. Other equipment types, especially mechanical equipment also needs to be inspected periodically, e.g. pipe systems and pressure vessels.
Inspections in general lead to a huge amount of effort for all affected people due to many different issues.
Carrying out an inspection in a lowly digitalized environment can cost a lot of time, as checklists have to be administrated, printed, filled in, scanned and evaluated by many manual actions. The Digitalization offers opportunities for plant operators by introducing paperless workflows. Another opportunity is to reduce the effort that employees have in keeping all the different IT-systems resulting from the plant's life cycle up to date. In the engineering phase, CAE- and Engineering systems are in use to manage equipment. During the operation of the Plant, ERP-Systems and document management systems (DMS) must be taken into account. Double data input in all systems can cause mistakes, a poor data quality in general and it requires additional time. A highly digitalized environment can help the operator to solve the conflict between time, quality and costs.

1. Legal Requirements and Compliance

During the industrialization of Europe, the use of hazardous substances increased more and more. After several disasters, the European Union released the Directive 96/82/EG that is also known as "Seveso Directive", after the Seveso disaster and aimed at improving the safety of sites containing large quantities of dangerous substances. Since then, a growing number of laws, standards and compliance regulations has been implemented in all countries where production facilities of the chemical industry are resident.
The Seveso III-Directive requires a safety management system for the prevention of major accidents, which addresses, among others, "procedures for systematically identifying major hazards arising for normal and abnormal operation" as well as "adoption and implementation of procedures and instructions for safe operation, including maintenance, of plant, processes and equipment […]" (European Parliament, 2012).
In a risk-based approach, the initial risk of an identified hazard must be decreased to a tolerable one. This can be achieved with technical, organizational or electrical/electronical measures (Hauptmanns, 2013). With a continuously increasing level of automation, electronical measures became very common. Process Control Technology (PCT) can be used to mitigate hazards of different types: unsafe conditions in chemical reactions like increased pressure or temperature, leakage of substances harmful to the environment as well as hazards regarding operational health and safety in general. Along with electronical measures, also mechanical solutions like pressure relief valves are widespread.
To ensure a high reliability of PCT-based and mechanical safety functions, the international standard for functional safety in the process industry, IEC 61511, provides a design basis. For plant operators, compliance to the IEC 61511 is a possibility to prove the usage of state of the art safety management systems.

Paper Received: 23 February 2019; Revised: 5 May 2019; Accepted: 30 June 2019

Please cite this article as: Hack S., Lange M., 2019, Paperless Safety Lifecycle, Chemical Engineering Transactions, 77, 553-558
DOI:10.3303/CET1977093

When flammable substances are part of a process, areas within the plants can be classified as hazardous areas. Within these zones, only certified equipment can be installed and used. In Europe, national law based on the directives 2014/34/EU (equipment manufacturer) and 1999/92/EG (operator) must be applied. In many other countries, compliance with the IEC standards 60079-14 and -17 for installation and maintenance is common.
Next to the functional safety and hazardous area requirements, there can be a lot of additional laws and regulations that operators must comply with. They affect complex systems as pressure vessels and pipes, but also more simple matters as lighting systems, electrical installations or even roller shutters and ladders.
All standards and laws that have been mentioned in this very brief overview have the common denominator, that they affect the whole lifecycle of the plant. During the operation phase, equipment- and regulation-specific, periodic inspections have to be performed and documented. The rising number of regulations cause additional time and effort for all people involved.

2. Functional Safety

The base norm for functional safety is IEC 61508. There are further standards derived from this standard. For the chemical industry, the relevant standard is (IEC 61511-1, 2016). It sets out practices in the engineering of Safety Integrated Functions, which are a combination of sensors, logic modules and final elements. A safety integrated function must fulfil a certain safety integrity level (SIL) depending from the risk that should be mitigated.
National standards and recommendations make functional safety more concrete, e.g. in Germany the VDI/VDE 2180 standard or several recommendations of the NAMUR.
To determine the SIL of a safety function, the probability of failure on demand has to be calculated, which depends on the structure of the safety function (e.g. redundant sensors or final elements) and the failure rates as well as a proof test interval.

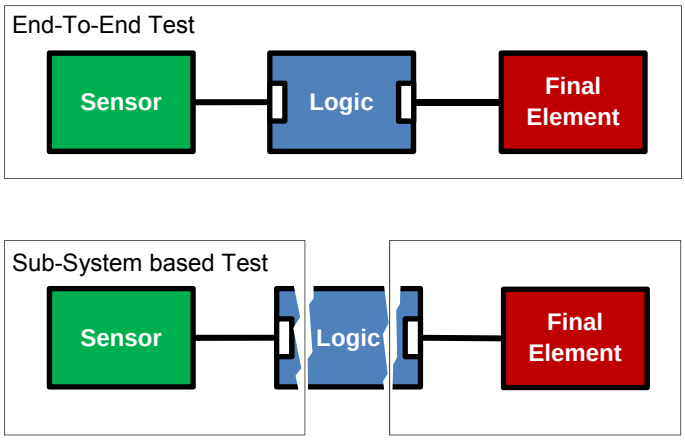

Figure 1: End-To-End and Subsystem-based Test Procedures

The testing (or periodic inspection) is required to detect dangerous faults that can disrupt or even prevent the safety function (NA 106, 2018). The interval depends on the SIL-calculation, but a typical interval is twelve month. For each safety function, a test specification (or inspection plan) has to be created that describes all steps in detail. In addition, all inspections have to be documented to prove that inspections have been performed. According to (IEC 61511-1, 2016), a protocol must include

- a description of all performed tests
- the date
- the name of the inspector
- the serial number or another unique identification number of the equipment
- the result of the inspection.

The concrete test procedure depends on the equipment type and the structure of the safety function. A temperature transmitter has another test procedure than an overfill protection.
The effort caused by the inspection of Safety Integrated Functions is not only due to the actual time that is taken by the inspector to perform the inspection. It is also caused by the creation of equipment-specific test

protocols, by the scheduling the inspection, by providing manuals and other documents, by archiving and evaluating the results.
A site with 600 Safety Integrated Functions requires the scheduling of 600 inspections if the testing is done in and “End-to-End” fashion. To perform an inspection, the corresponding protocol must be selected and printed. The inspector takes the protocol with him, fills in the results after performing the inspection and signs the protocol. Afterwards, the protocol must be filed down in a folder. When a protocol consists of five sheets of paper, 3,000 sheets of paper must be filed down each year. Within ten years, 30,000 sheets of paper have to be archived. The generation of key performance indicators or the tracking of bad inspection results is hardly possible.
In the age of the digitalization and the internet of things, this approach seems rather old fashioned and ineffective. In a digital environment, inspection protocols could be generated out of reusable blocks. By using variables, equipment properties like the serial number can be matched directly into the protocol. The scheduling and the selection of the corresponding protocol can be performed automatically based on an algorithm. Furthermore, by using tablet pcs and an electronic signature, it is no longer necessary to print the protocols. Inspection-relevant documentation can also be transferred to the tablet and will be available in field. After the inspection, protocols can be evaluated and archived automatically.

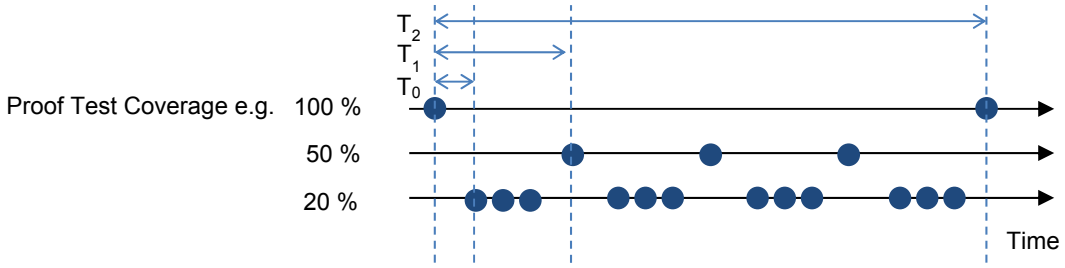

Figure 2: Flexible inspection concept with different intervals and proof test coverage (NA 106,2018)

A digital solution has the potential to greatly reduce the effort.
A digital inspection organization also facilitates the introduction of a sub-system based proof testing strategy (NAMUR NA 106, 2018). The previously described End-to-End strategy from sensor to actuator entails additional effort and a disruption of production. A sub-system based strategy has the aim to ensure the longest possible plant operation, not interrupted by any test, while maintaining the necessary safety integrity. This can be achieved by adding further test methods with different test intervals and test steps to a safety integrated function. In Figure 2, an inspection concept is displayed with three different inspection types. Inspections that are more frequent have a lower proof test coverage but do not require a shutdown. Inspections that require a shutdown have the highest proof test coverage but a long interval. The downside of this strategy is a more complex scheduling of inspections and inspection plans with variants depending on the coverage, but a digital algorithm-based inspection management system can mitigate this additional effort.

3. Hazardous Area Inspections

In areas of a site where flammable gasses, liquids or dust can be released, only certified ex-equipment may be installed and used. To maintain safety regarding explosions during the lifecycle, inspections are required.
The inspection concept differs from functional safety and depends on national law. Often, the inspection concept for hazardous areas is based on the standard (IEC 60079-17, 2013), which is briefly described in the following paragraph. Inspection concepts for hazardous areas also have been described by (Oberhem, 2007).
There are three different inspection types with different test coverages: visual, close and detail inspection. Detail inspections require the opening of enclosures, which can often only be done during a shutdown. Inspections have to be performed during the lifecycle, starting with the commissioning of a site. During operation, the inspections have to be done either on a fixed interval (typically 36 month) or continuously, if skilled personnel visits the installation on a regular basis. Independently of this strategy, samples of the equipment should be inspected additionally. The inspection procedures depend on the type of protection the equipment has been certified for.
Also, a history of all maintenance activities with the reason for each activity has to be provided. A list with all defects must be kept. In case of the continuous supervision strategy, the effectiveness must be verified.
Compared to functional safety, the situation is similar: for each equipment, periodic inspections have to be scheduled. An inspection plan has to be generated, taken to the field, signed and archived.

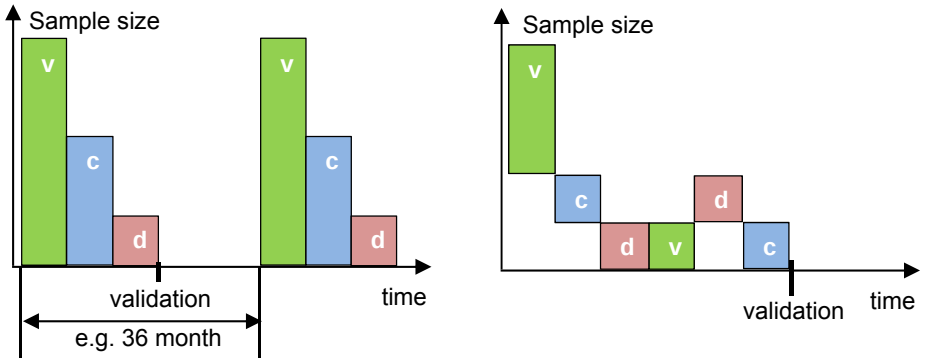

Figure 3: Periodic and continuous supervision inspection strategy

The effort depends on the strategy. When periodic inspections are performed in a fixed interval, a large number of protocols have to be generated, but the inspections can be done in a short period. The downside is that additional shutdowns will be necessary. By implementing the concept of continuous supervision, inspections can be done along with other, non-explosion protection related maintenance measures. This prevents shutdowns, but the organizational effort is bigger. The scheduling, the evaluation of results, the tracking of key performance indicators and the documentation in general grows more complex.
By using an algorithm-based software solution, it is possible to handle this complexity and to keep all benefits from the concept of continuous supervision. The effectiveness of the inspection concept can be verified automatically. As all inspections get reported back to the system, the person in charge can quickly get an overview for all sites, whether the target quotes of visual, close and detail inspections have been fulfilled or not.

4. Further Inspection Types and Inspection Concepts

In chemical plants, the list of equipment that has to be inspected periodically is very long: Lightning protection systems, pressure vessels, elevators, emergency generators, emergency lighting systems, central control rooms, just to name a few. The principle is always similar: a set of objects has to be inspected in a given interval using defined inspection plans, the protocols should be kept as records.
With the growing amount of regulations, there is a risk of over-inspecting a plant and causing loss of production. By using one central system for the administration of all inspection concepts, different inspection types can be combined more easily and can be performed during the same shutdown. In addition, redundant checks that are required to be compliant to different regulations can be detected.

5. Lifecycle and Documentation

The identification of major hazards is part of a risk assessment that is usually performed during the early stages of a plant's lifecycle. Figure 4 displays a simplified lifecycle, software systems and documents involved in a partly digitalized environment.
Based on the results, safety systems are designed during the engineering phase. After the commissioning, the operation phase of the plant starts. The inspection concept must be implemented and it must be verified that periodic inspections take place. Between the different stages, there is a gap concerning information and documentation, as each stage includes different people using different IT-Systems. The result of the risk assessment is often a folder that lists hazards and measures to reduce the risk for a certain section of the plant. In case of technical measures, engineers use CAE-systems. This includes the necessary equipment, the combination to loops and the creation of drawings. Operation manuals and certificates are delivered by the equipment manufacturers. After the commissioning of a plant, many larger enterprises use Enterprise Resource Planning (ERP) systems. The scheduling of maintenance, inspections and shutdown is typically part of the ERP system. When inspections are performed, checklists or plans as well as manuals, certificates and other documents are required. The gap between the systems now prevents a lean inspection process: to get all required information, the people involved have to query the engineering system for drawing and equipment specification, the ERP system for scheduling, document management systems or network drives for checklists and manuals. After the inspection, a protocol has to be signed and archived. If a change is detected during the inspection, all systems have to be updated to maintain the data integrity. Depending on the plant's size and the number of the installed equipment, this can cost a lot of additional time and effort.

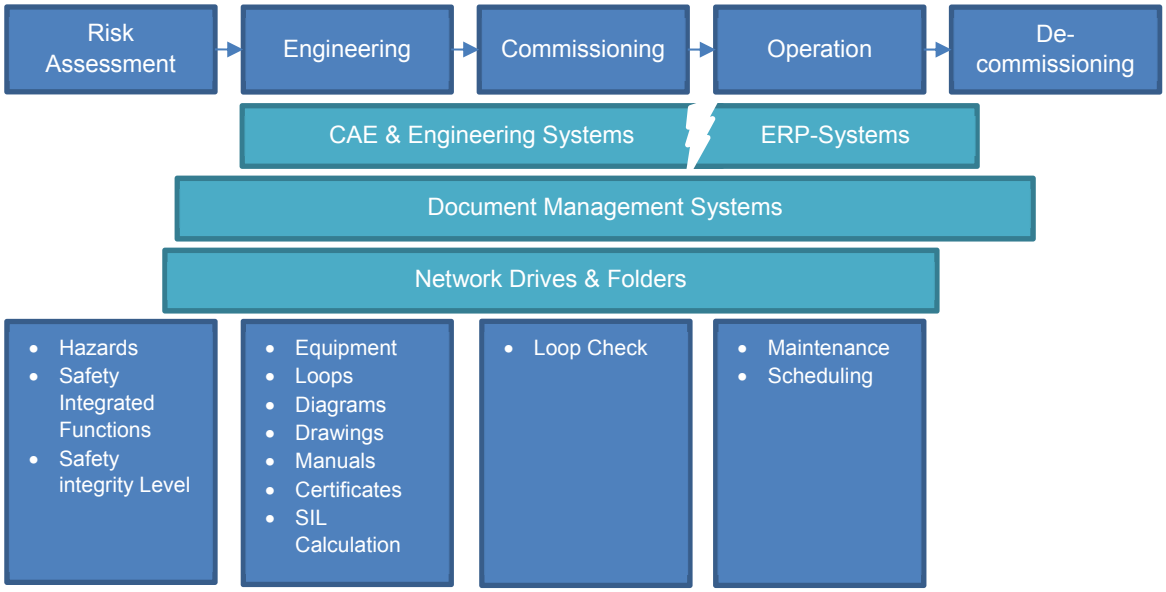

Figure 4: Simplified lifecycle, related IT-systems and documents

6. Closing the Gap by implementing a central Data Hub

The next level of digitalization can be reached by adding a flexible and integrateable software system that can be connected to the established systems by using bidirectional interfaces. In Addition, documents from network drives can be integrated. Inspection plans and checklists that are required for inspections as described in section 2, 3 and 4 can be broken down into reusable blocks and then recombined into inspection plans. To this central Data hub, tablet PCs can be connected to do paperless inspections.

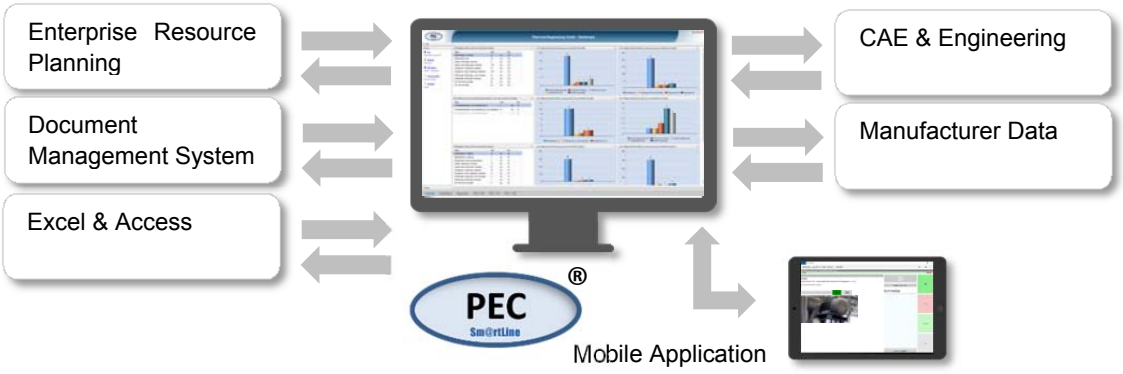

Figure 5: The SmartLine Plant Engineering Center ® (PEC) System as an example for a central data hub with bidirectional interfaces and the possibility to perform inspections paperless over the entire lifecycle

7. Implementation and Return on Investment Consideration

Implementing a central data hub for a paperless lifecycle management system will have initial costs, which depend on the IT-landscape and the data quality of a site. Usually there are two scenarios.
In the first scenario, data is mostly available in form of paper sheets. Engineering data has been printed and archived into folders: equipment registers, drawings, certificates and manuals. It is also widespread that there are PDF-documents of these files stored on network drives. Inspection plans are also either available as printable documents and usually will be filed in a folder after the inspection. To go paperless, the equipment register and all associated files have to be imported into the system. Inspection plans and checklists must be recreated. During this process, a standardization can take place to reduce the number of plans by merging similar procedures from different plans to one procedure.

In the second scenario, all data is stored in IT-systems, as described in section 5. In this case, bidirectional interfaces have to be created to connect the engineering systems, the ERP systems and document management systems to the central data hub. Inspection plans must be recreated and standardized as in the first scenario. In both scenarios, a high initial effort is necessary. After establishing the system, the effort for standardization, evaluations, data synchronization and documentation as well as the inspection effort in general can be reduced by up to 30 percent. This value is the authors experience from working on several projects related to a paperless safety life cycle managed by a cooperation of the companies R. STAHL GmbH and AGU GmbH. Especially the evaluation can be improved greatly by creating email reports that can be automatically sent to a responsible person.
The return on investment is the permanent reduction of effort to maintain an effective and compliant inspection organization that ensures a high level of safety.

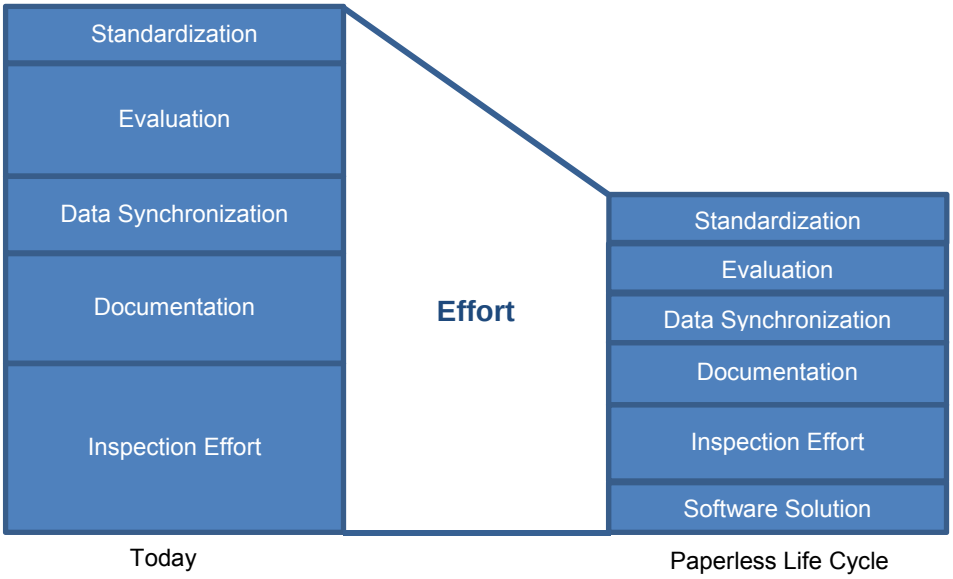

Figure 6: Return on Investment through reducing the Effort of an inspection organization

8. Conclusions

Digitalization and Internet of Things are trends that have been discussed a lot since the year 2000. The practical use of this technology is given depending on the industrial sector and the company size. In the beginning, many island solutions have been created, that are useful for a specific purpose. The next step is the integration of those islands, to break the barriers between systems and to further increase the productivity by creating lean processes.The number of regulations for safety systems and safety relevant plant parts has been growing within the last decades. To give an example: the IEC 61508-1 for functional safety started in 2002. With each new edition, the norm got more complex. Being compliant to the standard requires a growing effort. Smart technologies can help to compensate this ongoing trend.

References

Hauptmanns, Ulrich, 2013, Prozess- und Anlagensicherheit, Springer-Verlag, Berlin Heidelberg.
Oberhem, Heribert, 2007, Geprüft und für gut befunden, CHEMIE TECHNIK, November 2007, 12-14
IEC 60079-17 Ed. 5.0, 2013, EXPLOSIVE ATMOSPHERES – Part 17: Electrical installations inspections and maintenance
IEC 61511-1, 2016, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements
NAMUR NA 106, 2018, Flexible proof testing of field devices in safety systems, NAMUR Interessengemeinschaft Automatisierungstechnik in der Prozessindustrie e.V.
European Parliamant, 2012, Directive 2012/18/EU of the European Parliament and of The Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Diretive 96/82/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0018&from=DE> accessed 03.09.2018