DOI 10.5162/sensoren2016/P7.9

Online Certification of Sensors and Sensor Networks

Dr. Julian Wolf, Werner Varro
TÜV SÜD Product Service GmbH
Ridlerstr. 65, 80339 München, Germany

Abstract

More and more complex sensors and sensor networks in safety-critical application domains on the one hand and the dynamic and highly adaptive properties of such networks on the other hand require new methodologies and concepts for certification. To overcome these challenges, TÜV SÜD introduces an approach for a modular online certification of sensors and sensor networks. Extensive experience from different pilot studies enables the generation of a body of rules, while collected reliability data on multiple sensor types serve as (additional) input for certification. The presented approach of a certification platform is also applicable in the context of Industry 4.0.

Keywords: Certification, Sensor Networks, Safety, Reliability

Introduction and Motivation

The ongoing development and usage of more and more complex sensors and sensor networks in safety-critical application domains becomes a challenging topic for future certification methodologies. Instead of central instrumentation and control systems as they are common today, decentralized self-learning systems will be deployed, which are dynamically adapting to their environment and optimizing workloads. Regarding “Smart Home”, “Smart Grid” or “Smart Factory” as well as the dynamic and highly adaptive properties of sensor networks, the classic approach for a certification of safe electric and electronic systems is only applicable to a certain degree. On the other hand, a certification of such sensor networks will remain a necessary precondition for placing on the market, CE-label and operation in the EU.

The changing basic requirements for the evaluation of sensor networks – from static to dynamic certification – make it necessary to develop new certification methodologies. Based on these different requirements, TÜV SÜD has developed mechanisms for a modular online certification of sensors and sensor networks (see Fig. 1). The experience from different pilot studies enables the generation of a body of rules for the modular approach of a real-time certification. Collected reliability data of certain sensor types serve as an important parameter for the application of this methodology – always guaranteeing a high level of security and privacy.

In this paper, we will show on the one hand the TÜV SÜD vision of a modular certification of future sensor systems according to adapted requirements and show details on dedicated example scenarios. On the other hand, we focus on the applicability of our methodology in the context of Industry 4.0. But at first, we will start with a summary of lessons learned from our recent pilot studies.

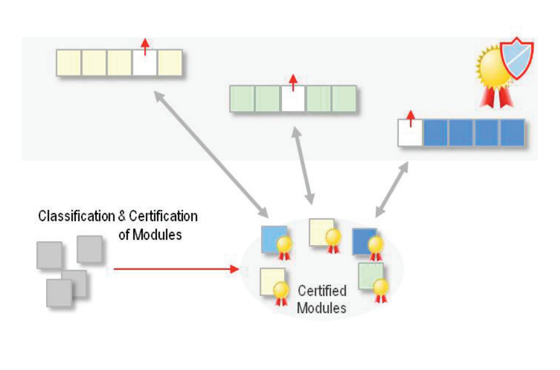

Fig. 1: Modular certification of dynamically configurable systems.

Lessons Learned from Pilot Studies

To gain a wide range of experiences, TÜV SÜD has been conducting pilot studies on different sensor network projects. During the classic certification process of these pilot studies, TÜV SÜD has been facing challenges which are typical for any safety-critical application using sensor networks. One central point is the reliability of the data provided by the sensors:

- Can the data of qualified or non-qualified sensors be used as a decision base for safety critical issues?
- Is it necessary to have homogeneous or heterogeneous redundancies on every position?

Another issue is also concerning the communication technologies in sensor networks:

- How can a real-time capable reliable communication with limited message latencies be guaranteed?
- Can environmental influences on communication be excluded?

A typical property of sensor networks is their configurability with sensors entering or leaving the network:

- How can safety be guaranteed without the knowledge on all involved network elements?
- Which criteria have to be fulfilled by a new participant in the network?
- Is the current configuration safe and CE compliant?

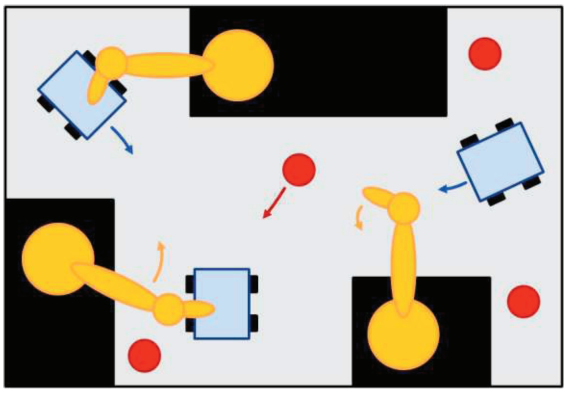

Fig. 2: Example scenario for a highly automated production line with interactions between industrial robots (yellow), automated guided vehicles (blue) and manual workers (red).

A typical safety-critical application can be a highly automated production line including interactions between machines, automated guided vehicles, industrial robots and manual workers, as depicted in Fig. 2. All moving systems and humans participation in this scenario can be equipped with multiple reliable sensors to enable a safe man-machine interaction. The need for a certified, dynamically reconfigurable sensor network is obvious.

Evaluation of the application and modified risk assessment

As a first step, a deep evaluation of the application is required. Especially the dependence of the measured sensor values from each other must be taken into account.

To analyze the risks of a sensor networks its specific properties and characteristics must be regarded. Compared to a classic hazard and risk assessment as defined in the ISO/IEC 31010 and functional safety standards DIN EN 61508, DIN EN 62061 or EN ISO 13849-1 for machinery, some evaluation parameters, like the probability, frequency and duration of a hazardous event as well as the potentials for its avoidance need to be adapted. The dynamic configurability of sensor networks, i.e. its potential to add or remove components also during operation, has to be considered during the hazard and risk analysis. There must be assumptions made on foreseeable use cases and the constraints of usage must be determined and documented to guarantee conformity in every configuration.

Creation of a system model and estimation of failure rates

The creation of a system model enables a detailed derivation of properties concerning functionality and reliability. Based on outcomes of the hazard and risk analysis, there are several specific requirements on sensor networks which have to be fulfilled. On the one hand, these requirements concern availability and fault rates, on the other hand interoperability and data integrity. If the sensor network uses non-qualified sensor components, these requirements must be even higher.

Concerning **availability**, there must be reliably experienced data on the fault rates of deployed sensors. These data can allow statistic predictions and forecasts of further sensor behaviour. Also the course of fault rates during operation time and its gradient are useful criteria. If the availability of sensors cannot be guaranteed to a sufficient level (as required by the results of the risk analysis), other measures must be applied: In case of correlating values, other sensors have to serve as a substitute for a failed component. By this, redundancies can be identified in the model and used to increase also the level of reliability in a sensor network. However, if there is still a failure in the system, it has to be detected within a specific time frame to introduce convenient countermeasures immediately: An online self-diagnosis with degradation possibilities must be realized.

To guarantee **interoperability** in sensor networks, a defined interface for the registration of new sensor components is required (e.g. as specified in ISO/IEC 29182). As soon as a sensor is connected to an existing network, a signature of the sensor specification can allow predictions on the future behaviour of the whole system, including failure rates and probabilities. A clustering of different sensors can dynamically increase (or decrease) the reliability and the safety integrity class of a whole

DOI 10.5162/sensoren2016/P7.9

sensor network. These data and status parameters can also be derived from detailed component models.

Regarding **data integrity**, a correct transmission without modification must be guaranteed. The requirements on the diversity of communication protocols depend on the results of the hazard and risk analysis: In case of low SIL levels and a usage of qualified sensors in a sensor network, it can be sufficient to implement homogeneous redundant communications. Otherwise, diverse redundancy will be indispensable. Another important issue in this context is the data precision and real-time capability of the network: On the one hand, it must be guaranteed that sensor values have only a limited deviation. On the other hand, the latency of data transmission must not overrun a defined limit.

A guarantee of **safety and CE compliance** mainly depends on a fulfilment of the SIL requirements, which have been determined in a risk assessment. This also includes the degree of protection against dust and liquids as well as a proof of correct behaviour in typical environments (concerning vibration, environmental temperature etc.). All these confirmations and its corresponding parameters must be deposited within the system to be checked during operation.

Methodology for an Online Certification of Sensors and Sensor Networks

To overcome the challenges on the certification of complex future sensor systems, TÜV SÜD has developed a methodology for an online certification of sensors and sensor networks. Focusing on the changed properties of these systems, it must be regarded as a completely different way of certification: Instead of an enclosed evaluation and certification process before bringing the system into service, the online certification can be seen as a continuous process accompanying the whole operation time of a product. By this, a dynamic reconfiguration does not require a full recertification of the whole system, which would be necessary when following the classic approach. Instead, each addition, removal or replacement of sensor components, will initiate an online update process of the certification. Based on the results of this process, the operator of the system can see after only a few seconds if the reconfigured system still complies with all requirements for a further safe operation or if additional steps are necessary.

The fundament of this methodology is the TÜV SÜD online certification platform including a sensor reliability database as well as a body of rules for the modular certification.

TÜV SÜD Sensor Reliability Database

The knowledge of sensor reliability data is always an important input factor during a certification process. However, it is challenging as well to derive meaningful and proper data on a special sensor type of a defined production batch. An estimation of failure rates based on commonly used standards, like SN 29500[1] will often be difficult and inaccurate.

Therefore, the idea of our approach goes one step beyond: The TÜV SÜD sensor reliability database (see Fig. 3) will collect sensor information and failure rates from sensor and component manufacturers as well as from sensor network operators. In this context, algorithms on big data analytics must be included. This huge amount of field data for every different type of sensor (even according to specific production batches) can be used for a reliable certification baseline. By this, even a prediction of the expected residual operation time of sensors and sensor clusters in the network can be imaginable.

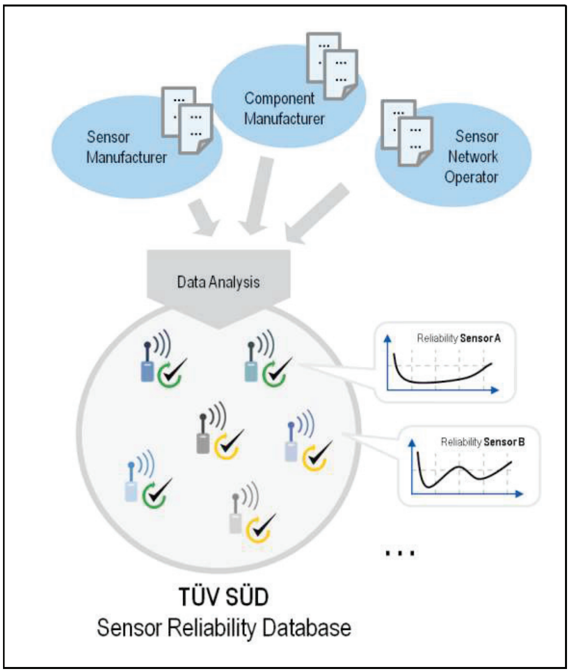

Fig. 3: Overview of the TÜV SÜD Sensor Reliability Database

TÜV SÜD Body of Rules for Modular Certification

Besides the reliability database, the TÜV SÜD certification platform includes a body of rules for modular certification (see Fig. 4).

[1] Siemens AG standard for the reliability prediction of electronic and electromechanical components

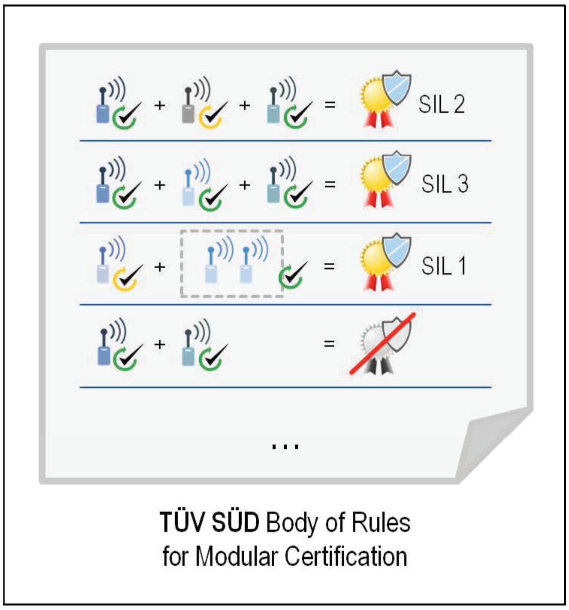

Fig. 4: TÜV SÜD Body of Rules for Modular Certification

Based on applicable standards and principles, rules are defined to allow a check of modified conditions according to the dedicated requirements. When a specific sensor in the network fails, other sensors might adopt its tasks and serve as substitute dynamically – if the relevant requirements on reliability or safety are met. As soon as new sensors enter the network, the properties of these sensors must be taken into account and evaluated to determine if the required functionalities can be maintained. The body of rules defines the fundament for a confirmation or refusal of online certifications.

Example: Online certification of a dynamic sensor network

To demonstrate the functionality of our certification approach, we will show and describe each single step for an example system in detail:

Initial certification

Precondition for the online certification is the availability of a specification of the sensor network including the results of the risk analysis and all relevant conditions for a proper operation. The TÜV SÜD certification platform will receive this specification along with the current status information of each sensor component (for details, see Fig. 5). The communication protocols will be adapted to commonly used standards for sensor networks, like ISO/IEC 29182. An encrypted communication to the sensor network guarantees the fulfilment of high security requirements.

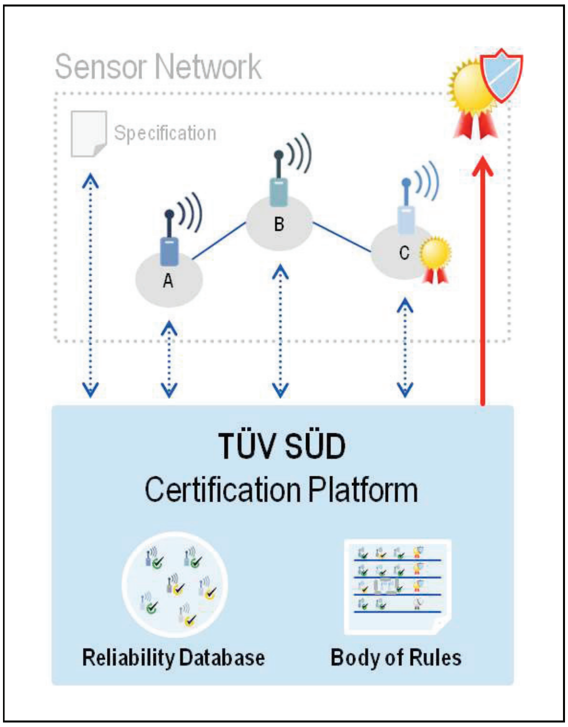

Fig. 5: Steps for the initial certification of an example sensor network

The sensor network will not necessarily consist of only qualified or certified components (sensor C in the example shown in Fig. 5). Also standard sensors (sensors A and B in the example) might be used without a guarantee of a certain reliability level.

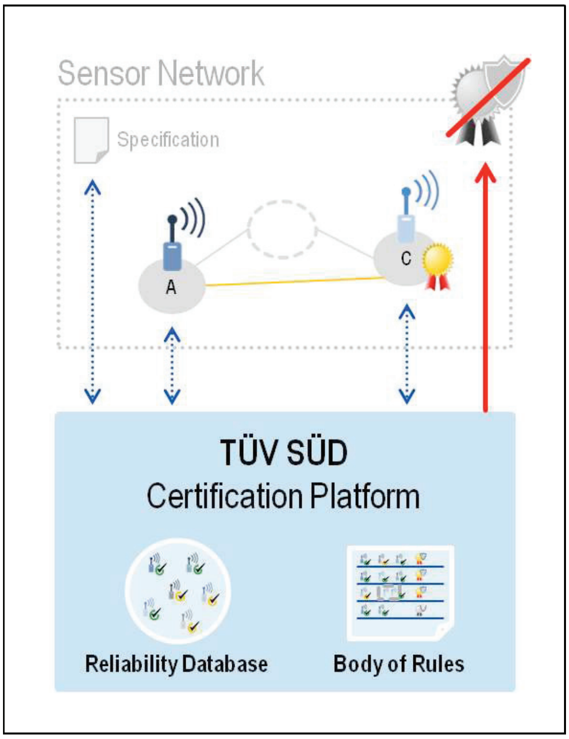

Fig. 6: Re-certification after reconfiguration of the sensor network caused by a failure of one sensor

DOI 10.5162/sensoren2016/P7.9

As soon as the certification platform has received all relevant information, reliability data on all deployed sensor types and production batches is internally provided by the reliability database to complement the sensor information. Based on these input factors the certification platform with its body of rules can decide if the sensor network fulfils all requirements according to its specifications. An online certification including a proof of the reached safety level and CE conformity can be assigned immediately and the network operator will be informed about the results.

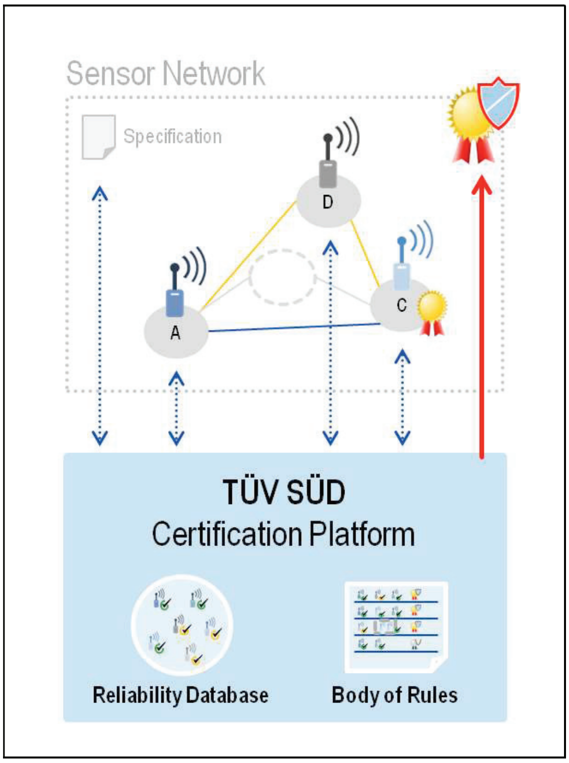

Fig. 7: Re-certification after reconfiguration of the sensor network caused by the integration of a new sensor element

Certification update on reconfiguration

If the sensor network is reconfigured, an update of the certification has to be performed in order to check if the necessary requirements are still fulfilled. Figure 6 shows an example scenario where one sensor fails (sensor B).

After the failure of this sensor, the certification platform has to initiate an update by checking the data of all residual sensors. As a first step, the specification will be taken into account in order to compare if the relevant requirements are still met. Working sensors might serve as a substitute when new communication paths can be established. If the failed sensor causes the non-compliance to the specification, the certificate must be revoked and the network operator will be informed. Moreover, the reliability database will be updated according to the current failure of the sensor. As can be seen, the information in the reliability database will continuously be improved according to field data.

Another scenario describing the adding of a new sensor element to the network is shown in Fig. 7. In this example the sensor element is a standard component which does not contain any qualification. In this case, the sensor element will first be evaluated according the relevant values from the reliability database. According to this information it will be checked against the requirements from the specification of the sensor network. If all requirements can be fulfilled, the online certification can be reassigned to the network.

Applicability in the Context of Industry 4.0

An important aspect of our online certification approach is also its applicability focusing on Industry 4.0. The basic challenge in this context is to establish dynamic configurable systems between machines and within machines. It is necessary to use the digital infrastructure and to enable a login and logoff of components like sensors, actors and modular machines. Focusing on this topic, the TÜV SÜD approach for modular certification was already introduced in [1]: A detailed risk assessment is performed on the level of the production process and defines specific requirements on a certification of the system. On this baseline, a detailed analysis of all interface parameters and safety architecture requirements can be provided by the TÜV SÜD certification platform in real-time.

A precondition for the establishment of a modular certification technique is the provision of relevant data to the certification platform. One useful basic concept was introduced by ZVEI in [2] describing “Industry 4.0 Components”: It comprises a component’s virtual mapping, which is stored in a so called “administration shell” (see Fig. 8). The main benefit of this concept is the possibility to provide data and functions easily. This might be data for maintenance purpose (e.g. CAD data, connection diagrams and manuals) or to enable a connection to other hardware and software components. The provided functions comprise e.g. (project) planning, configuration, operation, maintenance and complex functions of business logic. Using the administration shell with all the included information about integration, the concepts of modularity can be implemented properly.

Our presented approach for the online certification of sensors and sensor networks can be built on these concepts on Industry 4.0 components. Much of the existing data provided through the administration shell can be used as a baseline for the online certification.

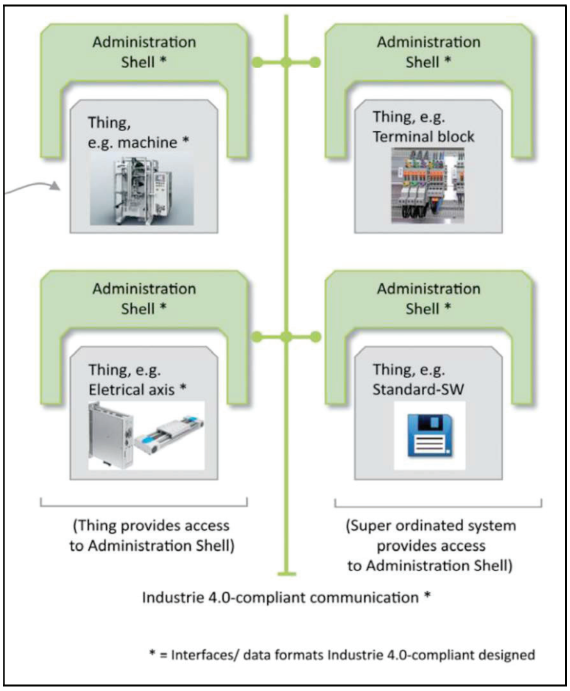
Administration Shell *
Thing, e.g. machine *
Administration Shell *
Thing, e.g. Terminal block
Administration Shell *
Thing, e.g. Eletrical axis *
Administration Shell *
Thing, e.g. Standard-SW
(Thing provides access to Administration Shell)
(Super ordinated system provides access to Administration Shell)
Industrie 4.0-compliant communication *
* = Interfaces/ data formats Industrie 4.0-compliant designed

Fig. 8: Administration shell of Industry 4.0 Components as described in [2].

In general, the dynamic principles of sensor networks are highly related to the modularity concepts of Industry 4.0. The replacement of sensor components will follow the same principles as machine modules and safety components, based on safety configuration requirements. In both areas of application only new components fulfilling an adequate level of safety can be accepted. Real-time safety analyses will verify the specified data with real-time sensor data and the proof of integrated sensors fulfilling the original specification is done automatically. A combination of safety & security aspects can be incorporated, too.

Conclusion

In this paper, we presented a new approach for the online certification of sensors and sensor networks. Regarding lessons learned from different pilot studies, we could show the changed requirements of dynamic and modular sensor networks and the necessity for new certification techniques. On this baseline, we introduced the TÜV SÜD platform for modular certification using a database of collected real-time reliability data and a dedicated body of rules. Along with different example scenarios we could explain the single certification steps on a sensor network. Finally, we explained the applicability of our approach in the context of Industry 4.0 and could show that our methodologies comply with existing concepts to complement one another.

Literaturnachweis

[1] "Industrie 4.0 – Modulare Zertifizierung für dynamisch konfigurierbare Industrie-Systeme", Positionspapier, TÜV SÜD Product Service GmbH, 11.2015

[2] „Industrie 4.0: The Industrie 4.0 Component", ZVEI - German Electrical and Electronic Manufacturers' Association, Version 1.0, April 2015