White Paper

Digitalization of Production

- Integrity Management

LeiKon GmbH



LeiKon GmbH

Kaiserstraße 100

52134 Herzogenrath

Germany

www.leikon.de

©LeiKon GmbH 07/2023

Motivation

The reliability of production plants is an important prerequisite for securing and optimizing the production in the process industry. The integrity of the plant assets and the OT and IT system technology used to automate, monitor, and optimize production have a significant influence on the required reliability.

The integrity of distributed data pools is more than typically handled in IT security concepts where just the integrity of transferred data is treated.

Integrity can be guaranteed by a systematic **integrity management methodology**. The methodology ensures that the data pools related to plant assets as well as to the IT/OT system technology correspond to the overall meaning of the term integrity:

- unharmed
- consistent
- intact and
- complete.

A methodology for ensuring the integrity of an automated production plant, as well as the use of tools for monitoring the integrity, is an essential component of a company-wide "Reliability Management". **The overall goal is to reduce unplanned plant failures to zero and to minimize the effort required to achieve this goal.**

Application domains

Maintaining the integrity of an automated production plant involves three application domains:



Operational Integrity – Increasing the reliability of production plants through innovative diagnostics of smart devices and automated, continuous checks of the correct system settings of OT/IT systems.



Connected Systems Integrity – Reduced effort and avoidance of errors in the configuration and permanent maintenance of networked OT/IT systems for data analysis, plant monitoring, and process optimization.



Engineering Data Integrity – Automated creation of a Smart Plant Repository with automatic detection of changes in the assets used and their parameter settings. Based on this, an automated continuous comparison of engineering specifications with the installed base.

Applications within the three domains are diverse. However, they are common by the fact that incorrect, changed, or incomplete system settings and configurations can be detected automatically on the basis of rules. **An integrity management methodology can be set up and operated with tool support.**

Integrity applications

Integrity management applications cover many areas of the OT and IT infrastructure of a production company. They can be further differentiated into the application areas described below.

Operational Integrity



Integrity of Smart Devices – Smart sensors and actuators have numerous settings and diagnostic information that contain information about the entire life cycle of a device. **These devices data can be read out automatically, compared with target specifications, and evaluated using sophisticated algorithms.** This means, that life cycle management processes and condition monitoring applications for predictive maintenance can be used without additional engineering effort. Rules can be used to cyclically read out relevant device parameters in order to provide relevant data to evaluation tools in the required data format. The evaluations can be carried out either locally by the company's own experts or in cooperation with device manufacturers via service agreements and cloud connections. **One example is SAM VALVE MANAGEMENT**, provided by Samson AG for advanced valve diagnostics. They use the integrity methodology, developed by LeiKon, to provide health reports to customers for downtime preparations using a fully automated tool chain starting from gathering data out of the field up to final asset health reports.

Integrity of OT/IT Systems – Settings of field devices, process control systems, or superordinate applications are automatically checked for consistency, absence of errors, and completeness on the basis of rules, either cyclically or event-driven. Single configuration parameters or parameter combinations are compared with target specifications or with settings from the past. Typical application examples are:

- **SCAN & ANALYSE Device Settings**: Are the settings of devices complete, consistent, and implemented according to the configuration specifications?
- **SCAN & ANALYSE Safety Settings**: Are safety-relevant configuration parameters, that can restrict the function of a sensor or actuator, set correctly according to the specifications?
- **SCAN & ANALYSE DCS Configuration Settings:** Are there any settings in the process control system that differ from standard operation? These analyses include, for example:
  - Parameter settings that unintentionally deactivate sensors, actuators, or controllers (bypass, simulation mode, manual mode, ...)
  - Combinations of parameter settings that are impermissible or lead to unwanted actions in combination.
  - Changes of alarm limits or alarm deactivations

The devices and parameters to be monitored are automatically explored and identified, and then checked for specific states, changes, or deviations from specifications on the basis of configurable rules. The results of the monitoring functions are visualized using interactive dashboards and made available via automatically generated reports. Subsequently, the detected deviations can be specifically analyzed and corrected if necessary. **The evaluations are typically used during shift handovers or at regular production meetings**. Pro-active notifications should be used in case of failure-critical discrepancies.

Connected Systems Integrity

The OT/IT system landscape typically consists on the one hand of process automation technology, dominated by process control systems and programmable logic controllers, and on the other hand of superordinate systems for production management, data analysis, and process optimization. The configurations of data points in OT systems and superordinate IT systems have many overlaps and must be kept permanently consistent. **Rules can be used to automatically create configurations of the superordinate IT systems and permanently synchronize them without manual effort.** The fully automatic configuration maintenance of networked OT/IT systems, such as process data archives, tools for alarm management, or controller performance monitoring applications, can be ensured by continuous integrity assurance.

Engineering Data Integrity

Engineering Data Integrity is based on the motto: "The truth is in the target system." The goal of these types of applications is the automated Management of Change (MoC) of a "Smart Plant Repository". **The repository is used to constantly compare the currently installed assets and their configuration settings with engineering documents and project planning specifications.**

Continuous integrity checks for data consistency between planning documents or maintenance tools and the existing plant reality ("as built") are made possible. The reverse documentation and the configuration comparison are also the basis for "reverse documentation" in migration projects.

