**White Paper**

# Integrity Management automatisierter Produktionsanlagen

LeiKon GmbH




LeiKon GmbH

Kaiserstraße 100

52134 Herzogenrath

www.leikon.de

©LeiKon GmbH 01/2022

## Was uns umtreibt

Die Ausfallsicherheit von Produktionsanlagen ist eine wichtige Voraussetzung zur Sicherstellung und Optimierung der Wertschöpfung in der Prozessindustrie. Einen wesentlichen Einfluss auf die Ausfallsicherheit hat die Integrität der Anlagen-Assets sowie der eingesetzten OT- und IT-Systemtechnik zur Automatisierung, Überwachung und Optimierung der Produktion.

Die Gewährleistung der Integrität kann durch eine systematische **Integrity Management Methodik** gewährleistet werden. Die Methodik sorgt dafür, dass die Anlagen-Assets sowie die eingesetzte Systemtechnik der Bedeutung des Begriffs Integrität entsprechend:

- unversehrt
- intakt und
- vollständig

betrieben werden.

Eine Methodik zur Sicherstellung der Integrität einer automatisierten Produktionsanlage, sowie die Nutzung von Werkzeugen zur regelbasierten, autonomen Überwachung der Integrität ist ein wesentlicher Bestandteil eines unternehmensweiten „Reliability Managements“. **Das Ziel ist die Reduktion ungeplanter Anlagenausfälle gegen Null und die Minimierung des Aufwands zur Erreichung dieses Ziels**.

## Anwendungsdomänen

Die Wahrung der Integrität einer automatisierten Produktionsanlage umfasst drei Anwendungsdomänen:



**Operational Integrity** – Erhöhung der Ausfallsicherheit von Produktionsanlagen durch innovative Diagnosen smarter Devices und durch automatisierte, kontinuierliche Überprüfungen von korrekten Systemeinstellungen von OT/IT-Systemen.



**Connected Systems Integrity** – Reduzierter Aufwand und Vermeidung von Fehlern bei der Konfiguration und dauerhaften Pflege vernetzter OT/IT-Systeme zur Datenanalyse, Anlagenüberwachung und Prozessoptimierung.



**Engineering Data Integrity** – Automatisierter Aufbau eines Smart Plant Repository mit selbstständiger Erkennung von Veränderungen eingesetzter Assets und deren Parametereinstellungen. Darauf aufbauend ein automatisierter kontinuierlicher Abgleich von Engineering Vorgaben mit der installierten Basis.

Anwendungen innerhalb der drei Domänen sind vielfältig. Es vereint sie aber, dass geänderte, fehlerhafte oder unvollständige Systemeinstellungen und Konfigurationen auf Basis von Regeln automatisiert detektiert werden können. **Eine Integrity Management Methodik kann werkzeug-unterstützt aufgebaut und betrieben werden**.

## Integrity Anwendungen

Anwendungen des Integrity Managements umfassen viele Bereiche im Umfeld der OT und IT-Infrastruktur eines Produktionsunternehmens. Sie lassen sich in die nachfolgend beschriebenen Anwendungsgebiete weiter differenzieren.

## Operational Integrity



**Integrity of Smart Devices** – Smarte Sensoren und Aktoren verfügen über eine Vielzahl an Einstellungen und Diagnoseinformationen, die Informationen über den gesamten Lebenszyklus eines Geräts enthalten. **Diese Gerätedaten können automatisiert ausgelesen, mit Sollvorgaben abgeglichen und über gehobene Algorithmen ausgewertet werden.** Damit sind Life Cycle Management Prozesse und auch Condition Monitoring Anwendungen zur prädiktiven Instandhaltung ohne zusätzlichen Engineeringaufwand anwendbar. Über Regeln können relevante Geräteparameter zyklisch ausgelesen und Auswertetools im geforderten Datenformat zur Verfügung gestellt werden. Die Auswertungen können dabei entweder lokal von eigenen Experten oder in Kooperation mit Geräteherstellern über Servicevereinbarungen und Cloud-Anbindungen erfolgen.

**Integrity of OT/IT Systems** – Einstellungen von Feldgeräten, Prozessleitsystemen oder übergeordneten Anwendungen werden auf Basis von Regeln automatisch zyklisch oder ereignisgetrieben auf Konsistenz, Fehlerfreiheit und Vollständigkeit überprüft. Einzelparameter und Parameterkombinationen werden sowohl mit Sollvorgaben als auch mit Einstellungen aus der Vergangenheit verglichen. Typische Anwendungsbeispiele sind:

- **SCAN & ANALYSE Device Settings**: Sind die Einstellungen von Geräten vollständig, konsistent und entsprechend den Konfigurationsvorgaben umgesetzt?
- **SCAN & ANALYSE Safety Settings**: Sind sicherheitsrelevante Konfigurationsparameter, die die Funktion eines Sensors oder Aktors einschränken können, den Vorgaben entsprechend richtig eingestellt?
- **SCAN & ANALYSE DCS Configuration Settings:** Sind zum aktuellen Zeitpunkt vom Normalbetrieb abweichende Einstellungen im Prozessleitsystem vorhanden? Dazu zählen z.B.:
  - Parametereinstellungen, die Sensoren, Aktoren oder Regler unbeabsichtigt deaktivieren (Bypass, Simulationsmodus, Handbetrieb, …)
  - Kombinationen von Parametereinstellungen, die unerlaubt sind oder im Zusammenspiel zu ungewollten Verhaltensweisen führen
  - Veränderungen von Alarmgrenzen oder Alarmdeaktivierungen

Die zu überwachenden Geräte und Parameter werden automatisiert erkundet und identifiziert, um sie anschließend auf Basis einstellbarer Regeln auf bestimmte Zustände, Veränderungen oder Abweichungen von Vorgaben hin zu überprüfen. Die Ergebnisse der Überwachungsfunktionen werden mit Hilfe interaktiver Dashboards visualisiert und über automatisch generierte Reports zur Verfügung gestellt. Anschließend können die detektierten Abweichungen gezielt analysiert und bei Bedarf korrigiert werden. Die Auswertungen werden typischerweise bei Schichtübergaben oder bei regelmäßig stattfindenden Betriebsbesprechungen genutzt. Bei Ausfall-kritischen Unstimmigkeiten sollten pro-aktive Benachrichtigungen genutzt werden.

## Connected Systems Integrity

Die OT/IT-Systemlandschaft besteht typischerweise einerseits aus der Prozessautomatisierung, dominiert durch Prozessleitsysteme und speicherprogrammierbaren Steuerungen, und andererseits aus übergeordneten Systemen für Produktionsmanagement, Datenanalyse und Prozessoptimierung. Die Konfigurationen von Datenpunkten in OT-Systemen und übergeordneten IT-Systemen weisen hohe Überschneidungen auf und müssen dauerhaft konsistent gehalten werden. **Über Regeln können Konfigurationen der übergeordneten IT-Systeme automatisch erstellt und dauerhaft ohne manuellen Aufwand abgeglichen werden**. Die vollautomatische Konfigurationspflege vernetzter OT/IT-Systeme, wie beispielweise Prozessdatenarchive, Werkzeuge zum Alarm Management oder Controller Performance Monitoring Anwendungen, kann durch eine kontinuierliche Integritätssicherung sichergestellt werden.

## Engineering Data Integrity

Engineering Data Integrity beruht auf dem Motto: „Die Wahrheit liegt im Zielsystem.“ Das Ziel dieser Anwendungen ist der automatisierte Aufbau und Änderungsmanagementprozess (MOC) eines „Smart Plant Repositories“. **Das Repository dient einem stetigen Abgleich der aktuell installierten Assets und deren Konfigurationseinstellungen mit Engineeringdokumenten und Projektierungsvorgaben**.

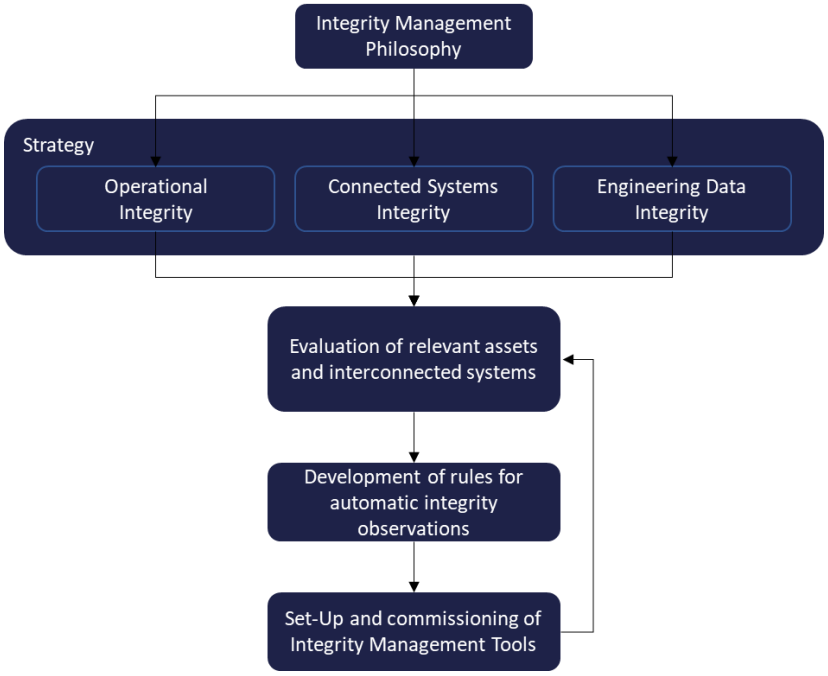
**Es werden kontinuierlich Integritätsüberprüfungen zur Datenkonsistenz zwischen Planungsdokumenten oder auch Instandhaltungswerkzeugen mit der vorhandenen Anlagenwirklichkeit („as built“) ermöglicht.** Die Rückdokumentation und der Konfigurationsabgleich sind zudem Basis für ein „Reverse Documentation“ bei Migrationsprojekten.



## Integrity Management Prozess

Auf Grund der besonderen und stark wachsenden Bedeutung bedarf das Integrity Management einer durchgehenden Systematik zur Planung und Umsetzung von Maßnahmen der Integritätssicherung. Angelehnt an Prozesse des Alarmmanagements nach IEC 62682 oder des Managements der funktionalen Sicherheit gemäß IEC 61511 umfasst ein systematischer Ansatz ein ganzheitliches Lebenszyklusmodell.

Für die identifizierten Wertschöpfungspotentiale werden anschließend Einsatzstrategien (z.B. tägliche Überwachung möglicher Parameterverstellungen oder monatliche Auswertung komplexer Gerätediagnosen) und die zu nutzenden Werkzeuge festgelegt.




Basis dieser Methode ist die Erarbeitung einer anlagen-, standort- oder unternehmensweiten **Integrity Management Philosophie**. Diese umfasst u.a. eine Beschreibung von Zielen, Verantwortungsbereichen und Methoden zur Einführung und nachhaltigen Nutzung des Integrity Managements.

Darauf aufbauend werden Kosten-Nutzen-Potentiale der drei Anwendungsdomänen **„Operational Integrity“, „Connected Systems Integrity“** und **„Engineering Data Integrity“** bewertet. Es werden die Kosten, die durch den Ausfall einzelner Assets entstehen, den Aufwendungen zur kontinuierlichen Integritätssicherung gegenübergestellt.

In einer Detailplanung werden für jede identifizierte Anwendung Regeln definiert. Diese legen fest, welche Daten aus Geräten und Systemen ausgelesen, anhand welcher Strukturinformationen diese Daten automatisch erkundet und wie diese Daten zur Auswertung aufbereitet werden sollen.

Nach Abschluss der Detailplanung werden die Regeln mit geeigneten Tools implementiert und in Betrieb genommen. Gemäß dem bewährten Zyklus „Plan-Do-Check-Act“ werden regelmäßig realisierte Anwendungen neu bewertet und neue Anwendungsfelder evaluiert.