

Mission Softwarequalität

Branchenbericht Maschinenbau

Safety First!

Von der Gefährdungsanalyse zum automatisierten Funktionstest



Jungheinrich ist eines der international führenden Unternehmen im Bereich Flurförderzeug-, Lager- und Materialflusstechnik. Auf Basis des umfassenden Produktportfolios fungiert Jungheinrich auch als Generalunternehmer für komplette Logistiklösungen – unabhängig vom Automatisierungsgrad – und liefert von der Planung und Projektierung bis hin zur Realisierung und Integration maßgeschneiderte Lösungen für die komplette Intralogistik.

Die Ausgangssituation

Durch die Novellierung der „Maschinenrichtlinie“ der Europäischen Union wurde die Konformitätsvermutung mittels der DIN EN 954 aufgehoben. Alle in Verkehr gebrachten Maschinen mussten spätestens ab 2012 nach der neuen Maschinenrichtlinie (§ 2006/42/EG) entwickelt und getestet worden sein. Mit der neuen Maschinenrichtlinie wurde erstmals eine aus der IEC 61508 angeleitete B-Norm harmonisiert. Diese Normen zielen deutlicher als früher auf Prozesse wie Risikoanalysen, Entwicklungs- und Testprozesse.

Exkurs: Normen und Gesetze im Maschinenbau

Um im Europäischen Wirtschaftsraum (Europäische Union und assoziierte Staaten) Produkte auf den Markt bringen zu dürfen, ist es erforderlich, dass der Hersteller die Konformität mit den in der EU geltenden Gesetzen bescheinigt. In vielen Fällen ist hier eine Selbstbescheinigung des Herstellers ausreichend, dabei haften die Unterzeichner der Konformitätsbescheinigung persönlich für die gemachten Angaben.

Da die meist sehr allgemeinen Anforderungen der Europäischen Gesetze einen gewissen Interpretationsspielraum zulassen, ist es wirtschaftlich sinnvoller, sich auf Standards zu beziehen, die den Stand von Wissenschaft und Technik widerspiegeln. Idealerweise existiert für ein Produkt eine Fachnorm (C-Norm). Dort sind für eine Produktgruppe alle zu beachtenden Anforderungen und Tests beschrieben. C-Normen referenzieren i.d.R. andere Normen, insbesondere auch Normen, welche mit einem Gesetz harmonisiert sind.



```

source_index = ...
target_index = 0x10
target.value = query(source_index)

int(f"Validating: {source_index} <-> {index}")

```

1101 1001 1001 1011

1101 1001 1001 1011

„**Harmonisiert**“ bedeutet in diesem Zusammenhang: Werden die Anforderungen der Norm erfüllt, darf vermutet werden (**Konformitätsvermutung**), dass das Produkt auch konform zu den Anforderungen des Gesetzes ist.

Die harmonisierten Normen sind typischerweise sogenannte B-Normen, die von abstrakteren Normen abgeleitet wurden. Diese A-Normen beschreiben allgemeingültige Prozesse, Methoden und Verfahren. Sie haben keinen Bezug auf Produkte oder Produktgruppen.

Durch die Harmonisierung der ISO 13849 mit der Maschinenrichtlinie der Europäischen Union ergab sich die Chance, die Konformität der elektronischen Steuersysteme basierend auf einer individuellen Gefährdungsanalyse der Flurförderzeuge nachzuweisen und dabei auf die tatsächlichen Risiken zielgerichtet einzugehen. Dieses Vorgehen war auch deshalb erforderlich, weil die Novellierung der DIN EN 1175 erst im Jahr 2011 abgeschlossen wurde. Bis dahin stand für die Entwicklung neuer Produkte keine harmonisierte C-Norm mehr zur Verfügung.

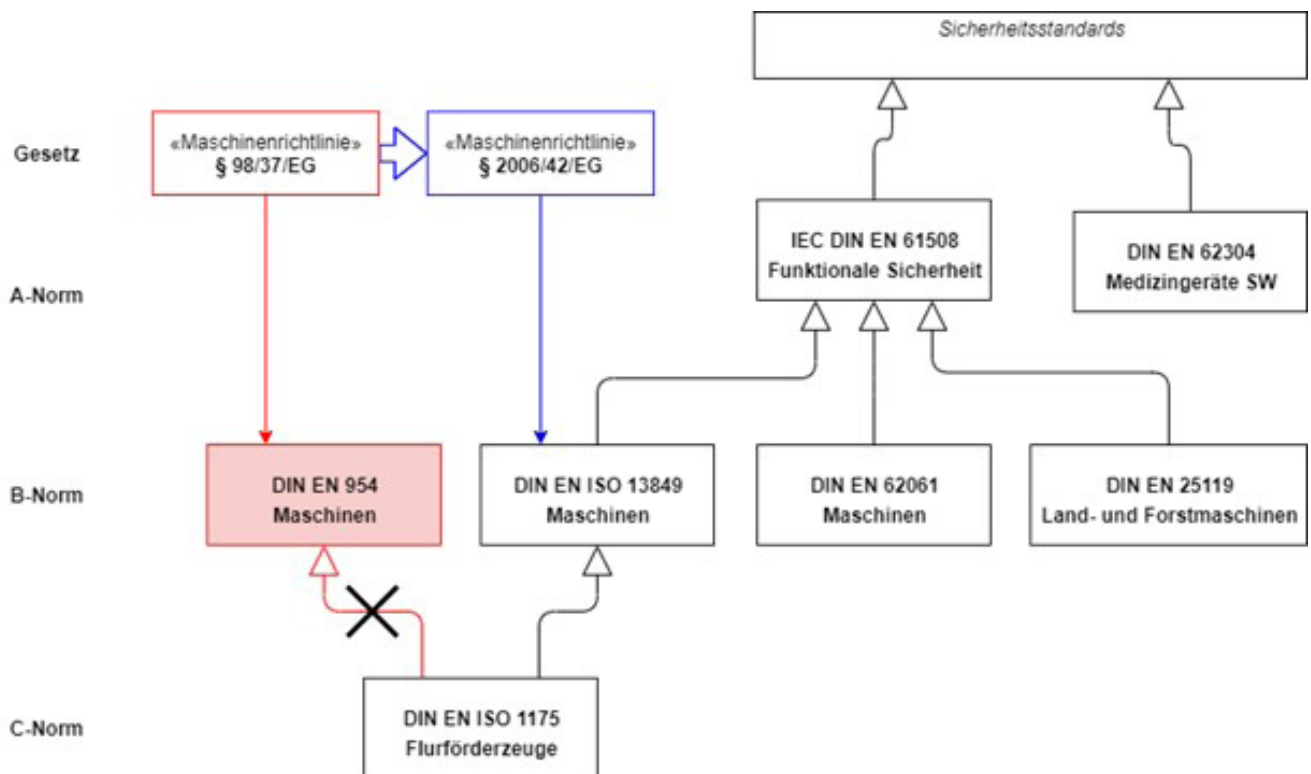


Abbildung: Zusammenhang zwischen Normen und Gesetzen.

Relevanter Ausschnitt für Flurförderzeuge ohne Anspruch auf Vollständigkeit oder Aktualität.

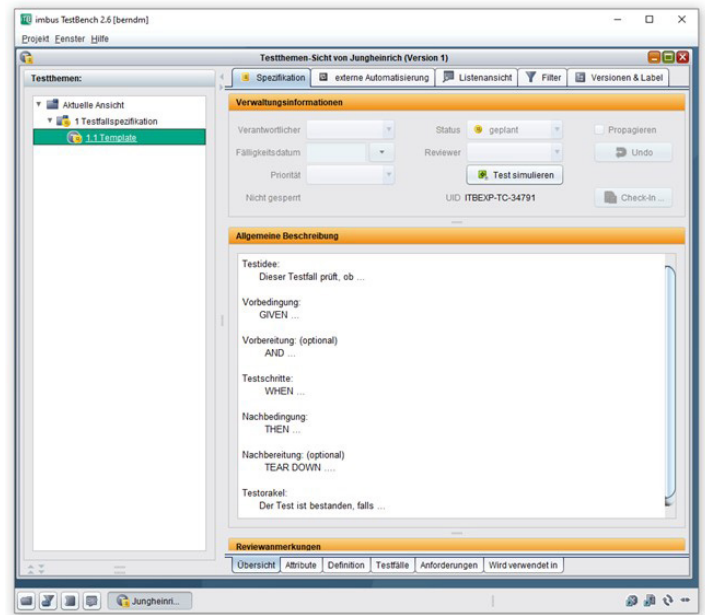
Aufgabenstellung und Umsetzung

Jungheinrich stand daher vor der Herausforderung, alle Flurförderzeug-Modelle bis zum Jahr 2012 normkonform zu überarbeiten und parallel alle Entwicklungs- und Testaktivitäten zu überprüfen und transparent zu dokumentieren. Wo nötig wurden Prozesse optimiert. Darüber hinaus war es notwendig, eine wirtschaftlich vorteilhafte Testlösung zu erarbeiten. Langfristig war dieses Ziel nur zu erreichen, indem man die Durchführung der Tests der Software automatisierte. Doch dazu waren zunächst einige vorbereitende Schritte notwendig:

Testmanagement

Zur Dokumentation der geplanten und durchgeführten Testfälle setzte Jungheinrich bereits vor 2012 auf die imbus TestBench. Zunächst wurde nun eine vom Fahrzeugmodell unabhängige Gliederung der Testthemen basierend auf den normativen Anforderungen erstellt. Dadurch wurde für alle Beteiligten in den verschiedenen Projekten ein klarer Wiedererkennungseffekt und hohe Akzeptanz erreicht.

Die in DOORS vorhandenen Anforderungen wurden über eine Anforderungsschnittstelle in imbus TestBench sichtbar gemacht. In der Testthemenstruktur erstellte Testfälle konnten so den Anforderungen aus DOORS zugeordnet werden. Die Testfälle wurden zunächst als Fließtext beschrieben. Dabei orientierten sich die nach dem ISTQB® Standard zertifizierten Tester an dessen Vorgaben. Hilfreich erwies sich dabei das folgende Template, das die Notation der Testfälle angelehnt an das (im Behavioral Driven Development, BDD) etablierte Gherkin-Format unterstützt:



Mit der Gherkin-Struktur konnten nun auch neue Projektmitarbeiter schnell eingearbeitet und eingesetzt werden, da hier u.a. auch die Messgeräte dokumentiert waren, die für die Durchführung von Soft- und Hardwaretests notwendig waren. Zeitverluste bei der Testvorbereitung waren damit weitgehend ausgeschlossen.

imbus Mitarbeiter unterstützen die Jungheinrich AG seit 2010 u. a. beim Test der Sicherheitsfunktionen in Flurförderzeugen. Zunächst waren basierend auf den Anforderungen und dem Design der Sicherheitsfunktionen Testfälle zu spezifizieren und anschließend durchzuführen.

Die Durchführung erfolgte in den ersten Projekten mit einer Vielzahl verschiedener Werkzeuge wie CANoe von Vector, Oszilloskopen und hauseigenen Tools zur Speicheranalyse und Manipulation des zu testenden Programms (Fault Insertion Test) direkt an bzw. auf den Fahrzeugen.

Testautomatisierung

Flurförderfahrzeuge müssen im Betrieb sicher sein. Der Ausfall eines Bauteils oder einer Fahrzeugkomponente darf nicht zu einer Gefährdung des Fahrzeugführers

oder anderer Beteiligter kommen. Um dies sicherzustellen, sind Flurförderfahrzeuge deshalb mit einer Reihe von Sicherheitsfunktionen ausgestattet. Die Aufgabe einer Sicherheitsfunktion besteht darin, während eines beliebigen Betriebszustandes auf Ausfälle (z.B. ein als fehlerhaft erkannter Sensorwert) zu reagieren und einen sicheren Betriebszustand zu halten oder herzustellen.

Beispiel: Sicherheitsfunktion Lenken

Wird während der Fahrt ein unplausibler Lenkwinkel eines Steer-by-Wire-Systems erkannt, so muss eine Sicherheitsfunktion das innerhalb von 100ms erkennen und anschließend das Flurförderzeug in einen sicheren Zustand überführen.

Für einen aussagekräftigen Test dieser Sicherheitsfunktion ist es einerseits erforderlich, korrekte Sensorwerte gezielt zu verfälschen, und andererseits die Reaktionszeit des Systems (typischerweise im 1 Millisekunden Bereich) zu messen.

Break-out vs. Simulation

Für jeden Test benötigt man Daten unterschiedlicher Äquivalenzklassen. Wie oben beschrieben sind Messwerte insbesondere Sensorwerte des Systems unter Test ein wesentlicher Input für deren Sicherheitsfunktionen. Um die Funktionalität der Sicherheitsfunktion vollständig zu prüfen, ist es erforderlich das korrekte Signal zu verändern.

Das kann man entweder durch eine Break-out Box realisieren, z.B. in dem man den Signalpfad unterbricht, diesen kurzschließt oder mit einem anderen alternativen Signal beaufschlagt. Hierbei wird erwartet, dass der prototypische Sensor ein korrektes Signal erzeugt.

Alternativ kann man das Signal des Sensors – Spannungswerte, Stromwerte oder digitale Signale – auch simulieren.

Es stellte sich heraus, dass die Simulation dieser Werte weniger aufwändig, sicherer und damit auch kosten-

günstiger ist als die Ausstattung eines echten Fahrzeugs mit Break-out-Boxen und Manipulationsequipment.

Zur Simulation des Restfahrzeuges (das ist die Summe aller Eingangswerte) wurden Hard- und Software von National Instruments™ verwendet, da hier sowohl eine große Bandbreite an analogen und digitalen Modulen zur Signalgenerierung und Messung vorhanden ist als auch unterschiedliche Bussysteme und sogar proprietäre digitale Sensorsignale via FPGA realisiert werden können.

Nach anfänglichen projektspezifischen Softwarelösungen in LabVIEW wurde vom Jungheinrich Testteam eine weiter verbesserte Testarchitektur entwickelt.

imbus programmierte den Kommunikationskern für die universelle Laufzeitumgebung (JuRTE = Jungheinrich Run Time Environment), sowie einige Simulationsmodule, u.a. die Simulation eines CANopen Knotens basierend auf der technischen Dokumentation des Knotens (EDS). Die JuRTE kommt zum einen in allen Prüfständen mit einem Echtzeit-PXI-System von National Instruments zum Einsatz, zum anderen ist sie auch Kern der PC-Software (JuTEE = Jungheinrich Test Execution Engine), welche u.a. noch um eine XSLT-basierende Kommunikationsschnittstelle zum TestBench Client erweitert wurde.

Die technischen Schnittstellen (Digitaler Output, Analog Output, Analog Input, CANopen, FPGA, ...) können über LabVIEW-Standardbefehle angesprochen werden, so dass darauf aufbauend komplexe Makros in imbus TestBench erstellt werden konnten, ohne erneut LabVIEW-Code schreiben zu müssen.

Erstmals wurde diese Testtechnologie bei der Entwicklung eines Steuergerätes für Gabelstapler mit Verbrennungsmotor eingesetzt. Dabei wurden Projektkosten über den Verzicht auf Prototypenfahrzeuge und Absaugeinrichtungen gespart. Da die Softwaretests nun ohne laufenden Dieselmotor stattfinden konnten, wurde damit auch ein Beitrag zum Umweltschutz geleistet.

```

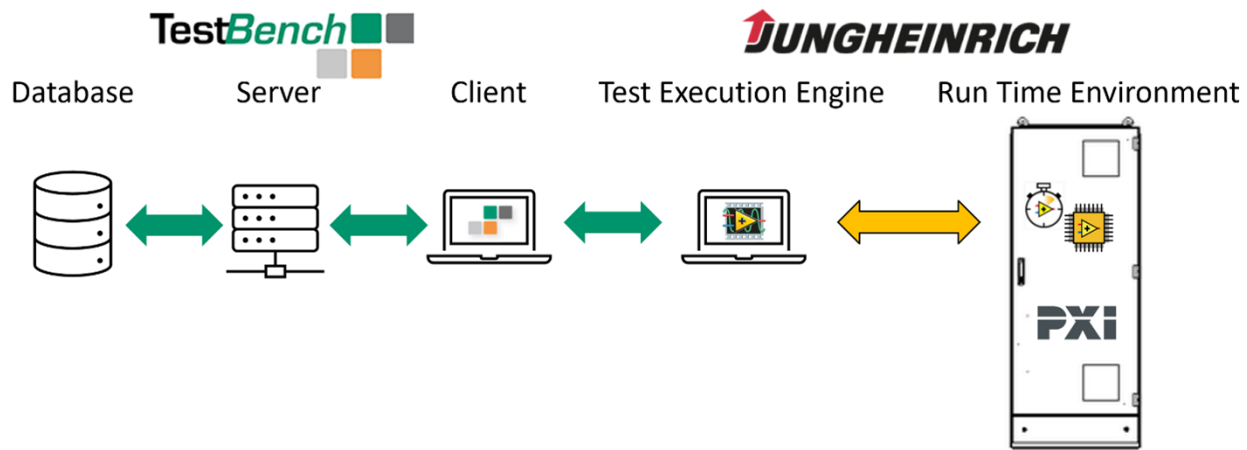
source_index = 0x10
target_index = 0x10
target.value = query(source_index)

int(f"Validating: {source_index} <-> {index}")

```

1101 1001 1001 1011

1101 1001 1001 1011



Über Agile Entwicklung und DevOps

Jungheinrich ist heute in der Lage neben Steuergeräten für Fahrzeuge auch Leistungsumrichter auch Elektronik für Batterien und Ladegeräte in Hardware in the Loop-Prüfständen zu testen. Da zum Test der Sicherheitsfunktionen diverse Betriebszustände angefahren werden müssen, werden zusätzlich etliche Anforderungen an Betriebsfunktionen mitgetestet. Durch die gezielte Variation von Parametern in imbus TestBench lassen sich darüber hinaus viele weitere Anforderungen überprüfen. Diese Option nutzt Jungheinrich, um in den agilen Entwicklungen Testaufgaben vom Systemtest am Fahrzeug in die Integrationstestebene vorzuverlegen (Shift-Left). Dafür wurden die bislang ausschließlich im Systemtest eingesetzten Ingenieure als Reviewer der Testspezifikation in die agilen Erstellungsprozesse einbezogen. So konnte das große fachliche Knowhow nicht nur transferiert, sondern auch dokumentiert werden.

Im Jahr 2020 wurden mehrere hundert Integrations-tests, die mittlerweile eine reine Laufzeit von ca. 18 Stunden haben, über Jenkins in die DevOps-Tool-Chain eingebunden. Durch Jenkins Pipelines wird der zu prüfende Binärcode und die Testautomatisierung für Nightly-Tests auf die Testrechner geholt. Vor dem Start der Tests wird die zu testende Elektronik im Prüfstand automatisch mit dem letzten Build geflasht. Die Tests

werden anschließend über Nacht auf mehreren Prüfständen parallel durchgeführt. Zum Daily-Stand-Up am nächsten Morgen können die automatisch erzeugten Berichte im Team bereits ausgewertet und diskutiert werden.

imbus unterstützte das Softwaretestteam mit drei nach ISTQB® Standard zertifizierten Mitarbeitern. In einem Zeitraum von nur zwei Jahren wurden ca. 4.000 automatisierte Testfälle geschrieben, die alle Anforderungen abdecken.

Das Resultat

Jungheinrich gelang es, die Entwicklungsvorhaben für seine vollständige Fahrzeug-Flotte erfolgreich auf die höheren Prozessanforderungen der IEC DIN EN 13849 umzustellen. Die anfänglich befürchteten hohen Mehraufwände konnten vermieden werden:

- durch die Einführung intelligenter Prozesse und den konsequenten Einsatz von Testautomatisierung;
- durch den Einsatz der imbus TestBench als leistungsfähiges Testmanagementtool;
- durch besser strukturierte und nachvollziehbare Dokumentation;
- durch die verbesserte Möglichkeit, neue Mitarbeiter

```
source_index = 0x10  
target_index = 0x10  
target.value = query(source_index)  
  
int(f"Validating: {source_index} <-> {index}")
```

1101 1001 1001 1011

1101 1001 1001 1011
1101 1001 1001 1011

1101 1001 1001 1011

schnell und effizient einzuarbeiten und in die vorhandenen Prozesse einzubinden.

Während der agilen Transition der Entwicklung in den letzten Jahren erwies sich die zu diesem Zeitpunkt bereits etablierte und ausgereifte Testautomatisierungsinfrastruktur als Zugpferd und konnte hier ihr volles Potential entfalten.

Jungheinrich musste seit mehr als 10 Jahren keinen Produktrückruf, keine Fahrzeugstilllegungen oder Software-Patches wegen eines Softwarefehlers in den identifizierten Sicherheitsfunktionen veranlassen.

imbus unterstützte diesen Erfolg in den letzten 10 Jahren flexibel mit 2-5 Ingenieuren: zunächst mit Beratung und der Einführung der imbus TestBench, später mit manuellen Tests an Gabelstaplern, Batterien und Ladegeräten, sowie bei der Programmierung der Jungheinrich Testumgebung. Von 2013 bis heute wurden 9 imbus Mitarbeiter beim Test von Sicherheitsfunktionen an einzelnen Fahrzeugen und aktuell bei der vollständigen Automatisierung aller Integrationstests der neuesten Fahrzeuggeneration eingesetzt. Ihr Einsatz erfolgte flexibel und stets orientiert an den Bedürfnissen und Herausforderungen von Jungheinrich.



Kontakt

imbus AG
Kleinseebacher Str. 9
91096 Möhrendorf
DEUTSCHLAND

Tel. +49 9131 7518-0
info@imbus.de
www.imbus.de