R1.1: IoT-Szenarien im Projekt

Abgleich Wissensstand im Projekt

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Version 1.1, Datum: 25.02.2017

Autoren:

Frank-Walter Jäkel (Ed)	– Fraunhofer IPK
Theo Margraf	– AUDI AG
Stefan Stoelzle	– AUDI AG
Paul Hopton	– Relayr
Yuliya Brynzak	– Relayr
Michael Wagner	– Fraunhofer FOKUS
Rutten, Stefan	– DEKRA
Andre Wardaschka	– DEKRA

Inhalt

1. Einleitung

Das Projekt „Ein Testlab und Testware für Internet der Dinge-Lösungen und –Geräte“ des BMWi kurz IoT-T hat als Ziel Firmen bei der Erstellung von IoT basierten Lösungen und Produkten in den Bereichen Qualitätssicherung und Zertifizierung zu unterstützen. Hierzu sind die Erstellung einer IoT Testware und die Etablierung mindestens eines IoT-Testlab geplant. Die IoT-Testware wird beim automatisierten testen von IoT relevanten Technologien wie z.B. Protokollen helfen und u.a. im IoT-Testlab zum Einsatz kommen. Dabei wird das IoT-Testlab Technologien wie CoAP und MQTT adressieren und gleichzeitig auf Standards wie z.B. TTCN3 aufsetzen. Das IoT-Testlab wird als praktisches Angebot für Firmen durch die DEKRA etabliert werden. Es soll Firmen ermöglichen auf IoT Testexpertise zugreifen zu können und Anwendungen zertifizieren zu lassen. Langfristig soll Firmen ermöglicht werden qualitative, sichere und interoperable IoT Lösungen zu erstellen.

Der vorliegende Report beinhaltet erste Ergebnisse bzgl. der Analyse von IoT-Lösungen und Szenarien. Insbesondere werden die Anwendungsszenarien und mögliche Demonstratoren der Anwender Audi und RELAYR beschrieben. Die spezifischen Anforderungen an IoT-Testware und IoT-TestLabs sind nicht Bestandteil dieses Reports. Die priorisierten Anforderungen werden im weiterführenden Report (R1.2) beschrieben. Ein weiterer Report mit den identifizierten Begriffen (R1.3) wird ebenfalls Anfang März 2017 verfügbar sein. Beteiligt an der Erstellung des Reports waren alle Partner des Projektes: Relayr, Audi, DEKRA, Fraunhofer FOKUS und Fraunhofer IPK.

1.1. Anwendungsszenarien

Die Anwendungsszenarien dienen zur Schärfung der Anforderungen an die IoT Testware und das IoT TestLab als auch für die spätere Entwicklung von realistischen Testfällen. Die Anwendungsszenarien beziehen sich auf konkrete Arbeiten der beteiligten Anwender (Relayr und Audi). Sie repräsentieren keine IoT Testplattform aber die Umgebungen in denen die IoT Testmethoden und IoT Testware im Projekt beispielhaft überprüft werden können. Sie bilden damit auch Referenzanwendungen für IoT-Testware und IoT TestLab. Die Anwendungspartner repräsentieren dabei zwei unterschiedliche Anwendergruppen:

- Endanwender von IoT Lösungen (Audi),
- Entwickler und Anbieter von IoT Lösungen (Relayr).

Die unterschiedlichen Sichten dieser beiden Gruppen spiegeln sich auch in den Anwendungsszenarien wider. Audi sieht den Fokus auf der Nutzung von IoT in der Fertigung und die damit verbundene Absicherung der Prozesse. Relayr sieht im Wesentlichen die Absicherung ihrer Produkte und Leistungen im Vordergrund.

Workshops bei den Industriepartnern Audi und Relayr ermöglichten einen intensiven Austausch zwischen den Projektpartnern und einen Abgleich des Wissenstandes im Projekt. Besonders die Positionierung der Anwendungsszenarien konnte Projektbezogen besprochen werden. Um die betroffenen Prozesse sowie mögliche Potentiale zu identifizieren wurden erprobte Methoden aus der Unternehmensmodellierung und dem Anforderungsmanagement [1, 2, 3, 4] eingesetzt.

Audi fokussiert auf die Absicherung des Informationsmanagements in der Fertigung (siehe Kapitel 2). Relayr fokussiert auf ihre Produkt und Serviceentwicklung zur Einbindung von vernetzten Geräten und Sensoren in ihre Cloud (siehe Kapitel 3).

Entsprechend der unterschiedlichen Ausrichtung der Szenarien von Relayr und Audi sind auch die Betrachtungsbereiche in ihrer Granularität unterschiedlich. Audi betrachtet den Entwicklungsprozess von der Planung bis zur Ausführung, aber mit dem Fokus auf das Informationsmanagement in der Shopfloor IT und deren Services bezogen auf IoT Komponenten. Ziel ist hier neben der besseren Absicherung auch eine Standardisierung, um den Einführungsprozess neuer Verfahren und Technologien zu beschleunigen und den Austausch von Prozessabläufen und Anlagen zu vereinfachen.

Relayr betrachtet die Anbindung von Hardwarekomponenten in die Relayr Cloud. Relevant sind dabei die Entwicklung von entsprechenden Adaptoren, die Datenaufbereitung und das Monitoring. Ziel ist hier eine frühzeitige Absicherung der Entwicklung der Adaptoren und der Datenqualität bei der Verbindung mit der Cloud. Ein wesentlicher Punkt sind dabei Sicherheitsfragen.

Generell ergänzen sich beide Szenarien sehr gut, da sie unterschiedliche Abstraktionsebenen bezüglich IoT betrachten. Wir haben Maschinen und Sensoren bei Relayr, welche in der Web-Infrastruktur bekannt gemacht werden und wir haben Services/Funktionen, welche virtuell oder von Maschinen bereitgestellt werden müssen um den Shopfloor IT Gedanken bei Audi zu realisieren.

Eine gemeinsame Fragestellung in beiden Szenarien sind Sicherheits- und Interoperabilitätsaspekte insbesondere in Bezug auf Cyberangriffe und Vernetzung.

1.2. Anforderungsmanagement

Im Verlauf von Workshops und Telefonkonferenzen wurden erste Ideen zu Anforderungen formuliert. Diese werden in ein Anforderungssystem überführt und im weiteren Verlauf des Projektes ergänzt und bzgl. Wichtigkeit und Machbarkeit priorisiert. Die Beschreibung der Anforderungen orientiert sich an VOLERE [5, 6] und wurde durch einen Prozessbezug ergänzt. Basis ist eine Analyse der Prozesse in den Szenarien und die daraus abgeleiteten Anforderungen, welche durch Anforderungen aus bekannten IoT Ansätzen ergänzt werden.

Ein System zur Unterstützung des Anforderungsmanagement wurde vom IPK zur Verfügung gestellt und über die Server von FOKUS für alle Partner bereitgestellt. Hierüber können die Anforderungen verteilt aufgenommen, verwaltet und priorisiert werden.

Der Bericht zu den Anforderungen (R1.2) wird nach Plan Anfang März bereitgestellt.

1.3. Betrachtungsbereich und Abgrenzung

Die Analyse des Betrachtungsbereiches hat die Anwenderszenarien sowie damit in Beziehung stehende Standards und IoT Lösungen umfasst. Als Referenzarchitektur wurde das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) [7, 8] identifiziert. Im Weiteren wurden die Szenarien auf diese Referenzarchitektur bezogen. Im Laufe der Diskussion wurde die umfangreiche Bandbreite von RAMI4.0 auf den für das Projekt relevanten IoT Umfang eingegrenzt (siehe Abbildung 1). Aus RAMI4.0 werden insbesondere die Begriffsdefinitionen im Projekt verwendet. Hierzu wurde eine Anwendung im Internet bereitgestellt um Begriffe im Projekt zu definieren und zu diskutieren. Anfang März wird hierzu ein Glossar (R1.3) als Report verfügbar sein.

Die Diskussion der Anwenderszenarien bezüglich Testbedarfe hat den Betrachtungsumfang weiter eingegrenzt insbesondere auf Tests zu IT Sicherheit und Interoperabilität. Sowohl Audi als auch Relayr haben hier einen Schwerpunkt gelegt. Audi sieht diesen in den bereitgestellten Services und Relayr in den Schnittstellen zur Cloud.

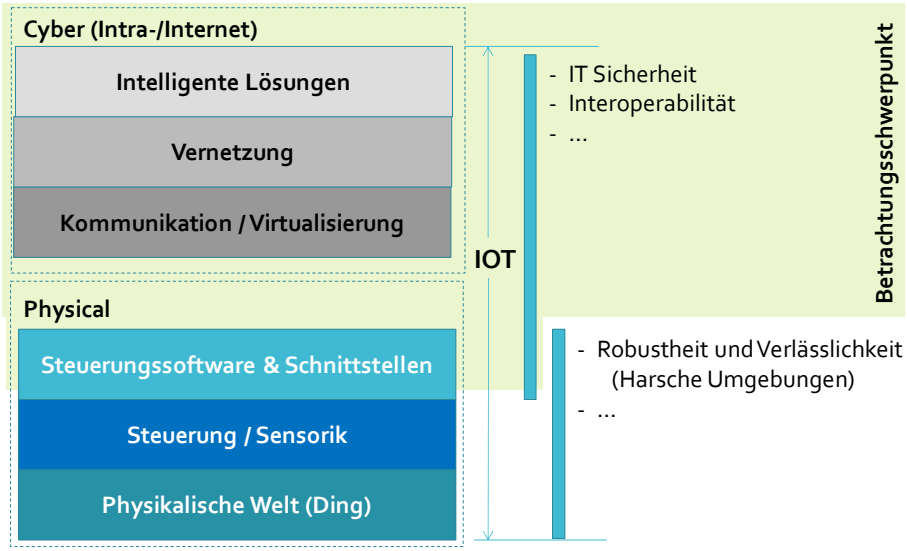

Abbildung 1: Prinzip-Skizze zum IoT Bereich aus der Diskussion im Projekt

2. Audi Szenario: Informationsmanagement in der Shopfloor IT

Zurzeit werden Strukturen und Arbeitsfolgen aus der Produktstruktur und der Ressourcenstruktur abgeleitet. Die Shopfloor IT findet hier keine Berücksichtigung. Zukünftig sollten vordefinierte Services Verwendung finden, welche bereits alle Schnittstellen in standardisierter Form beinhalten. Dabei sind die IoT Komponenten ausgehend von Protokollen und entsprechender Semantiken bis zu den Anlagenservices und Hardwarekomponenten abzusichern.

Das Szenario nutzt die aktuellen Aktivitäten zum Aufbau einer modularen Shopfloor IT bei Audi sowie einen entsprechenden Demonstrator am Fraunhofer IPK. Die von Audi beschriebenen Bedarfe basieren auf der heutigen und zukünftig geplanten Shopfloor IT Realisierung.

Der bereitgestellte Demonstrator ermöglicht den Zugriff auf die modulare Shopfloor IT ohne direkt in die Fertigung von Audi einzugreifen. Was unter Sicherheitsgesichtspunkten nicht möglich wäre. Die IoT-Testware kann daher für Testzwecke direkt in den Demonstrator eingebaut werden. Damit dient der Demonstrator als Modell für die Nutzung der IoT-Testware im industriellen Umfeld. Der Demonstrator entspricht im Wesentlichen der bei Audi in der Entwicklung befindlichen modularen Shopfloor IT. Hierdurch wird sichergestellt, dass IoT-Testware und Methodik direkt in die industrielle Praxis bei Audi überführt und genutzt werden können.

2.1. Ziele des Audi Szenarios

Das Szenario zum Informationsmanagement in der Shopfloor IT verfolgt folgende Zielsetzungen:

- Absicherung der Einbindung von Services/Funktionen z.B. neue Anlagen in das Informationsmanagement.
- Hersteller- und lösungsneutrales Informationsmanagement (Sicherstellung von interoperablen Lösungen).
- Absicherung der IT Infrastruktur entsprechend dem Stand der Forschung gegen Cyber-Angriffe.

- Absicherung von Auswirkungen der Wechselwirkung von Frequenzen z.B. Mobilfunk und RFID Signale (Harsche Umgebung).

2.2. Kurzbeschreibung

Die Shopfloor IT umfasst alle Informationsprozesse und IT Lösungen, die mittelbare Tätigkeiten am Produkt steuern, absichern und erfassen. Die Shopfloor IT unterstützt somit die unmittelbare Ausführung auf Werker und Anlagenebene. Sie beinhaltet Bereitstellen, Erfassen, Verteilen und Visualisieren von Informationen zum Produkt, den Prozessen und den Ressourcen (Betriebsmittel, Anlagen, Menschen) [9].
Die modulare Shopfloor-IT stellt eines der wesentlichen Innovationen zur Beherrschung der Komplexität bei der Audi AG dar. Sie verbindet das Anlagenengineering, die Entwicklung von IT-Fachkonzepten, sowie das Prozessengineering mit Hilfe von wenigen Modulen miteinander. Zum Erfolg der modularen Shopfloor-IT führen vielschichtige IoT-Lösungen, deren Robustheit, Funktionalität, Vernetzbarkeit, Sicherheit und Erweiterbarkeit essentiell für das modulare Konzept sind. Nur mit Hilfe einer innovativen Absicherung dieser Aspekte ist eine breite Einführung des modularen Konzeptes möglich. Der Einsatz dieser Testlösungen ist auch im Rahmen der Harmonisierung der anderen Marken des Volkswagen Konzerns angedacht. Damit soll die Anzahl und die Auswirkung von Störungen trotz erhöhter Komplexität gesenkt werden.

Das Konzept umfasst von den Ausführungsbestimmungen bis zur Ausführungsrückmeldung folgende Funktionen (DIN 62264):

- Spezifikationsmanagement,
- Ausführungsmanagement,
- Datenerfassung,
- Verfolgung.

Die Shopfloor IT kann zwischen der Feldebene und einzelnen MES Funktionen eingeordnet werden und beinhaltet SCADA, SPS sowie die Signalverarbeitung.

2.2.1. Herausforderung

Der Ansatz für die Entwicklung und Wartung der Shopfloor IT in Bezug auf das Informationsmanagement ist derzeit meist sequentiell. Die Architektur und Infrastruktur wird nach der endgültigen Definition der Anlagen entwickelt. Dieser letzte Schritt verbindet die eingebettete IT der Maschinen mit der Shopfloor IT. Hierdurch besteht eine enge Abhängigkeit zwischen der Maschine und dem entsprechenden Informationsmanagements. Auf der anderen Seite veränderte sich die Konfiguration der Maschinen schneller und dies erfordert Flexibilität auch im Hinblick auf das Informationsmanagement. Die Anzahl der Produktvarianten sowie der Produktänderungen nimmt zu und wird komplexer. Dies führt zu einer steigenden Zahl an Fertigungsfunktionen für die Überwachung, Steuerung und Verwaltung der Maschinen. Dies erhöht die Komplexität und Ressourcenkosten für die IT-Planung. Darüber hinaus führen die hohe Anzahl von Funktionen und Geräten zu einem erhöhten Risiko von Ausfällen.

Gleichzeitig steigt der Bedarf an schnellen Veränderungen der Fertigung, was die Online-Anpassung der Informationsprozesse während der Fertigungsausführung erfordert. Um die Produktion fortzusetzen, müssen neue Herstellungskonfigurationen während des Herstellungsprozess integriert

werden. Im Fall von Ausfällen müssen alternative Maschinen leicht in Kraft gesetzt werden. Dies ist derzeit sehr schwierig und mit der aktuellen Shopfloor IT Technologie nicht immer zu realisieren.

Generell wird der vollständige Fertigungsplan, bestehend aus Geschäfts-und Informationsprozess für eine Fertigungseinheit (z.B. Fahrzeugmontageabschnitt) oder eine Fertigungsinsel (z.B. Roboterzelle im Karosseriebau) geplant. Dieser Fertigungsplan besteht aus Standardfunktionen und Informationsobjekten vom Typ Produkt, Prozess und Ressource welche in Fachmodulen organisiert sind.

Anhand eines vollständigen Fertigungsplans ist die vertikale Integration abzusichern (Abbildung 2). Vertikale Integration meint die Interoperabilität der Funktionen der Shopfloor IT über einen Modulbaukasten mit generischen Businessservices, welche in USDL beschrieben sind. Beispiele hierfür sind: Identifizieren, Anlagenrückmeldungen verarbeiten, Auslagern, Einfördern oder Abdichten. Diese werden auf die Informations- und Geschäftsprozessebene über Services zur Steuerung der Produktionsressourcen (z.B. SPS Schrittkette, ROS, C5G Control Program, Cloud-Services) abgebildet. Produktionsobjekte sind dabei alle am Produktionsprozess beteiligten Ressourcen und Produkte.

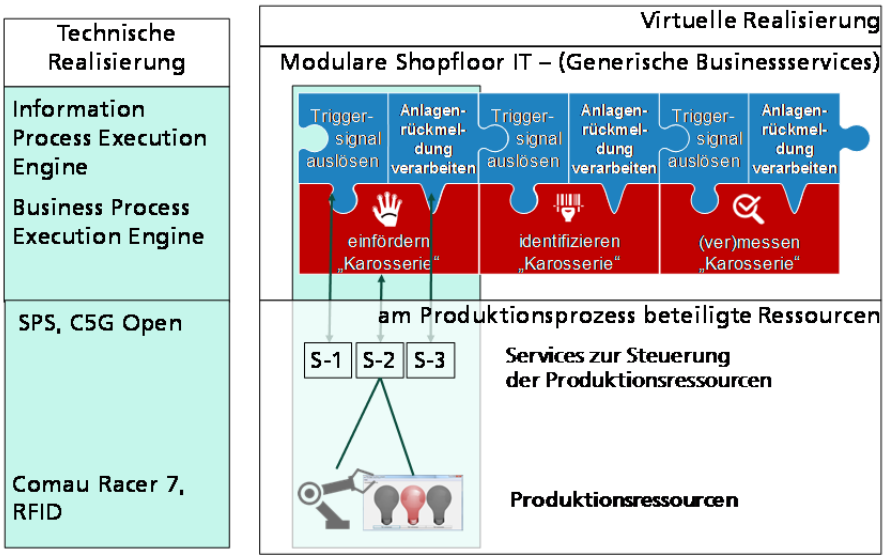

Abbildung 2: Konzept modulare Shopfloor - IoT Scope von Audi

Die möglichen Bedarfe Richtung IoT Tests sind in den folgenden beiden Szenarien zusammengefasst:

Szenario 1: Absicherung der Services/Funktionen:

Ausgehend von dem Konzept in Abbildung 2 werden Tests zu Services und Funktionen mit folgendem Fokus angestrebt:

- Tests in wieweit die Services zur Steuerung der Produktionsressourcen und der Businessservices einer vorgebenden Semantik (z.B. VDMA …) entsprechen.
- Vollständigkeit der angebotenen Services zur Steuerung der Produktionsressourcen bezogen auf die Anforderungen der Businessservices
- Test gegen Überbestimmtheit der angebotenen Services
- Test von nichtfunktionalen Anforderungen z.B. Verfügbarkeit, Reaktionszeit und Sicherheit
- Testen des Fertigungsplans (z.B. Belegungszeit von Fertigungsinseln, Taktzeiten von Linien, …)

- Test auf Cyber Sicherheit

Der Test des Fertigungsplans entspricht dem Test von vernetzten Services.

Szenario 2: (Tests für den realen Betrieb inklusive der harschen Umgebung)

Das Szenario 2 untersucht insbesondere die Verbindung zwischen Softwareservices und Hardwarekomponenten.

- Test, ob die Services zur Steuerung der Produktionsressourcen korrekt zu beteiligten Produkten und Ressourcen zugeordnet sind
- Test der Integration von Hard- und Softwareservices
  - Lasttests
  - Reaktionszeiten
  - Ausfälle
  - Robustheit bzgl. Komponentenausfall
- Test auf Cyber Sicherheit
- Harsche Umgebung (z.B. Überlagerung von Frequenzen, Temperatur, Druck → technische und chemische Belastungen)

Beide Szenarien bilden die Basis für die Identifikation von Prüfanforderungen.

2.2.2. Akteure / Rollen

Die Rollen geben einen Überblick die organisatorische Einbettung des Szenarios und die zu berücksichtigenden Interessengruppen. Sie sind hier zu den Hauptaktivitäten zugeordnet, welche in Kapitel 2.4 im Prozess illustriert sind:

- Planen

  Planen beinhaltet auch die digitale Absicherung von Planungsstadien sowie die Auslegung der Shopfloor IT und ist damit bereits relevant bzgl. der Tests von Services zu IoT Komponenten.
- Umsetzen

  Bei der Umsetzung sind getestete und ggf. zertifizierte Services und IoT Komponenten zu betrachten.
- Betreiben

  Beim Betrieb spielen Robustheiten bzgl. Änderungen und IT Sicherheit eine wichtige Rolle sowie Lernaspekt bzgl. neuer und unerwarteter Verhaltensweisen des Systems.

Die Rollen entsprechend der Hauptaktivitäten sind:

- Planen
  - Fertigungsprozessplaner
  - Informationsprozessplaner
  - Technologie- und Anwendungsplaner
- Umsetzen
  - Technologie- und Anwendungslieferant
- Betreiben
  - Prozessbetreiber

- Technologie- und Anwendungsbetreiber
- Übergeordnete Rollen
  - Standardisierer (Konzernarbeitskreis Shopfloor IT)

2.3. Die Test-Story

Die Test-Story beinhaltet den industrienahen Entwicklungsprozess bis hin zur serienreifen Inbetriebnahme. Die Tests beziehen sich auf IoT Protokolle und Services/Funktionen in der Produkt-, Prozess-, Ressourcen- und Informationsprozessentstehung.

2.3.1. Audi Ansatz

Im realen Prozess werden dazu in Team Center/Connect alle Ressourcen- und Produktdaten aus CATIA oder ähnlichen Systemen geladen, um den Prozess, wie auch den Informationsprozess, direkt und in 3D in Connect aufbauen zu können. Hierzu helfen Bibliotheken der jeweiligen Ressourcen und Produkte, die direkt Prozessbausteine hinterlegt haben, womit der Prozess geplant wird.

Ist die Planung in Connect abgeschlossen erfolgt die Überführung des Gesamtmodells in „Process Simulate“. Hier können alle Funktionen, Informationsobjekte sowie ihre gesamten Verknüpfungen als zusammenhängender Fertigungsprozess, digital abgesichert werden. Von hier aus kann über OPC UA Kommunikation (als OPC UA Client fungierend) der Gesamtprozess automatisch generisch beschrieben werden und ist damit ausführbar.

Die Ausführung erfolgt dann wiederum über einen OPC UA Server. Hier können aber ebenso lediglich einzelne Feldgeräte angeschlossen sein. Außerdem wird hier, direkt an der ausführenden Steuerung, die Absicherung des nicht-funktionalen Ablaufes durchgeführt. Dieses entspricht der virtuellen Inbetriebnahme. Die Prozessinformationen laufen wie zuvor über die OPC UA Kommunikation zurück an sämtliche zugreifenden OPC UA Clients, wie „Process Simulate“ (Hardware in the Loop) und einem überwachenden System/Leitstand. Die zugehörige Hardware für die gesamte Kommunikation ist ein Produktions-Service-Bus.

2.3.2. Story für Demonstrator

Zur Veranschaulichung der Einbindung der IoT Methodik, IoT-Testware und potentialer Zertifikate kann folgender Anwendungsfall genutzt werden:

Eine neue Anlage soll in die Shopfloor IT integriert werden. Es handelt sich um einen 6 achsigen Industrieroboter von der Firma Comau vom Typ Razer 7 mit folgenden technischen Randbedingungen:

- Steuerung ist eine C5G von Comau.
- Die Steuerung hat eine offene PDL2 Schnittstelle.
- Die auszuführenden Skripte werden über TCP/IP an die Steuerung geschickt.
- Die Schnittstelle kann über Internet und ETHERNET realisiert werden.

Die Konnektivität, Robustheit und Sicherheit der Verbindung muss gewährleistet werden.

Es wird geprüft, ob der Roboter die erforderlichen Protokolle und Services unterstützt. Falls dieses nicht der Fall ist werden die Services für den Roboter erstellt um ihn in die modulare Shopfloor IT einbinden zu können. Entsprechend der Vorgaben der modularen Shopfloor IT werden die Services/Funktionen geschrieben. Diese Services müssen vollständig und semantisch korrekt für die

entsprechende Anlage realisiert werden. Serviceanfragen, welche nicht realisiert werden können, müssen entsprechende Fehlercodes liefern. Im nächsten Schritt werden die Services/Funktionen veröffentlicht. Die veröffentlichte Schnittstelle bildet den Adapter bzgl. der Einbindung in die Shopfloor IT.

Die Adapter können in unterschiedliche Architekturen (OPC-UA, CoAP, DDS) eingebunden werden. Im konkreten Beispiel gehen wir von OPC-UA aus. Als Kommunikationsprotokoll wird TCP/IP verwendet. In der konkreten Umsetzung ist geplant die Adapter als Clients zentral in einem Server anzumelden. Alternativ kann eine CoAP Umsetzung erfolgen. Neben der Interoperabilität der Services ist auf Latenzzeiten und IT Sicherheit zu achten.

Abschließend können Shopfloor IT Workflows unter Einbindung der neuen Anlage ausgeführt werden. Dabei müssen Ansprechbarkeit, Verfügbarkeit der Anlage und Fehlerfälle identifizierbar sein.

2.3.3. Potentielle Tests

Die potentialen Tests betreffen die Verfügbarkeit der benötigten Services (Konformität, Interoperabilität), die Schnittstellenformate und Kommunikationsprotokolle, sowie den Betrieb in harschen Umgebungen. Dabei liegt der Fokus auf der technischen Absicherung der Services, da Tests und Zertifikate für die verwendeten Hardwarekomponenten in vielen Fällen bereits verfügbar sind und für den spezifischen Fall angezogen werden können. Damit ist beispielsweise der Test bzgl. Auswirkungen der Wechselwirkung von Frequenzen wünschenswert aber nicht zwingend im Projekt erforderlich.

Hingegen sind die Tests der Kommunikationsarchitektur OPC-UA wie auch der Protokolle erforderlich um Antwortzeiten und Betrieb der Shopfloor IT sicher zu stellen.

Ausgangssituation:

- Ein Fertigungsprozessplaner verkettet die Funktionen, die jeweils ein Produktionsabschnitt repräsentiert, zu einer sinnhaltigen Prozesskette.
- Ein Informationsprozessplaner komplettiert diese Funktionen mit Hilfe von Informationsobjekten und bringt damit alles in einen Zusammenhang. Dies geschieht indem er die, für die Funktion nötige und verantwortete, Information mit den jeweiligen Funktionen so verbindet, dass jede Funktion ordnungsgerecht mit Informationen gespeist wird.
- Funktionale und nicht-funktionale Randparameter werden in der Funktion festgeschrieben.

Testbedarf:

- Diese entstandene Gesamtstruktur aus Funktionen und Informationsobjekten, die miteinander verknüpft sind, muss nun auf Richtigkeit und Sinnhaftigkeit getestet werden.
- Die verwendeten Funktionen stehen in einem realistischen Zusammenhang, im Sinne von Reihenfolge (Test der logischen Verknüpfung der Funktionen).
- Die Funktionen müssen so mit Informationsobjekten gespeist werden, dass die Funktion ordnungsgemäß (funktionsgemäß) und wie in den Randparametern vorgegeben ausgeführt werden kann (Test der Vollständigkeit der Informationszufuhr der Funktionen).

Diese Testbedarfe werden im Zuge der Anforderungsdefinition (R1.2) konsolidiert und detailliert.

2.4. Prozesse mit Randbedingungen und Einflussfaktoren

Der Prozess in dem das Audi IoT Szenario eingebettet ist, beginnt mit dem Bedarf Umbau/ Neubau der Fertigungsprozesse. Nach der Planung der Produkte, Prozesse und Ressourcen wird ein Fertigungsplan verabschiedet und die Umsetzung geplant. Nachdem der Fertigungsplan umgesetzt wurde, erfolgt der Betrieb mit ggf. Anpassungen an Planung und Infrastruktur. Das Informationsmanagement ist zurzeit noch relativ spät involviert und soll über die modulare Shopfloor IT auch in frühere Planungsphasen stärker berücksichtigt und abgesichert werden (Abbildung 3). Hierzu gehören dann auch Tests und Zertifikate für die verwendeten IoT Elemente.

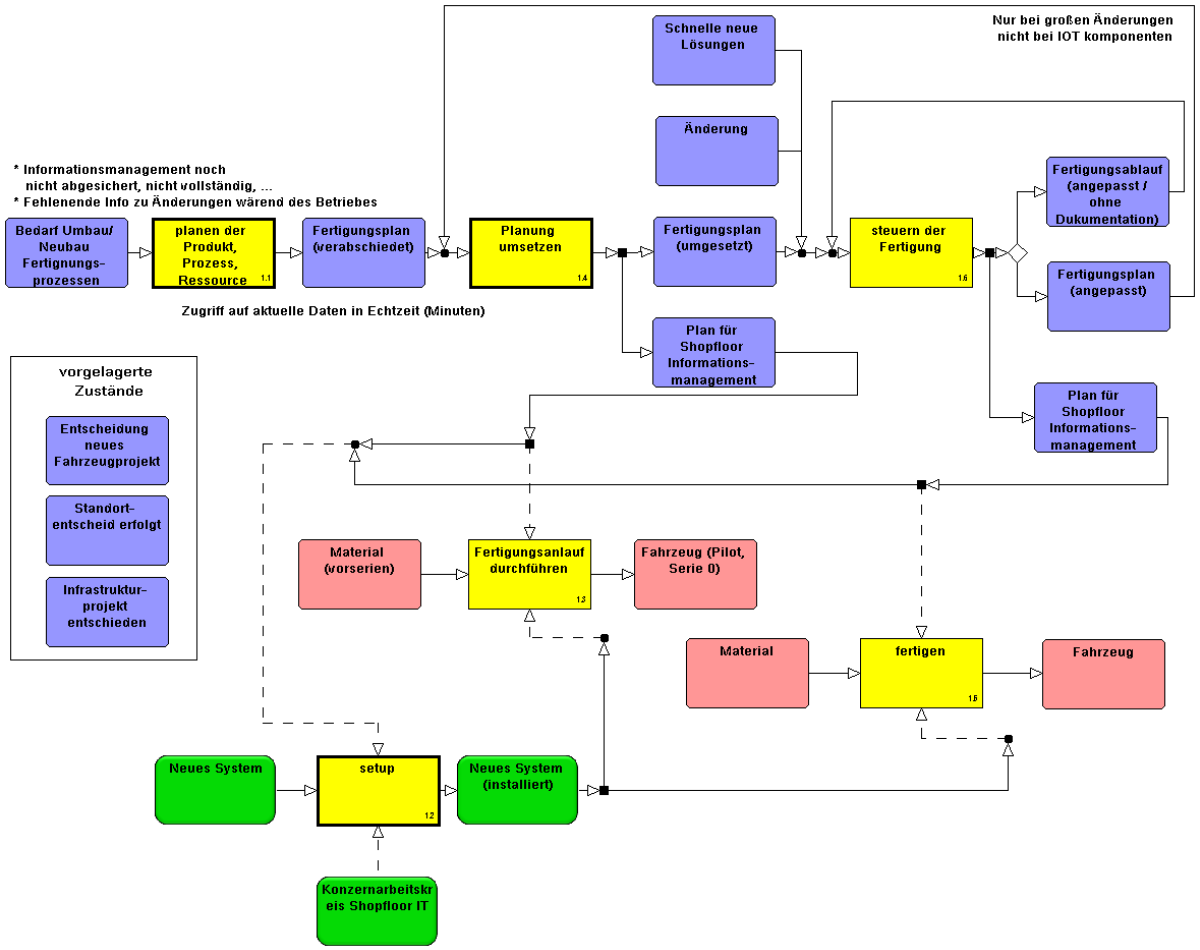

Abbildung 3: Ist Prozess mit Soll Anteilen

Der Prozess ist stark aus Sicht der Produktion und der Nutzung von IoT in den Planungs- und Umsetzungsprozessen der Produktion dargestellt. Die IoT Elemente selber sind hier nicht sichtbar, da sie an den Details der einzelnen Prozesse beteiligt sind. Details sind in Abbildung 2 dargestellt, wobei die Schritte „einfördern“, „identifiziere“ und „vermessen“ sowohl in der Planung virtuell abgesichert werden als auch im realen Prozess von der Shopfloor IT gesteuert werden müssen.

2.5. Nutzen

Der erwartete Nutzen der Projektergebnisse für das Audi-Szenario liegt in der Verfügbarkeit von IoT Testware für die unterschiedlichen Bereiche der Shopfloor IT und von Zertifikaten zur Sicherstellung der Konformität von Kommunikationsarchitekturen und Protokollen. Abbildung 4 illustriert die angestrebte Nutzung der IoT-Testware und IoT-Testlab, wobei IoT-Testware Komponenten im Testlab Verwendung finden, aber auch für weitere Tests verfügbar sind. Hierdurch kann Audi von bereits zertifizierten Services und IoT Komponenten profitieren aber auch weitere Audi spezifischere Tests durchführen. Zertifikate können beispielsweise Konformität von Protokollen und zu IT Sicherheitsanforderungen abdecken. Tests im Zusammenhang mit den Servicebeschreibungen der Maschinen und dem Aufbau der Shopfloor Module in der Shopfloor IT sind dann stärker Audi intern, wobei Eigenschaften, welche vom Anlagenlieferant bereitgestellt werden müssen, auch branchenspezifisch sein können. Hierzu gehören spezielle Schnittstellenspezifikationen oder auch OPC-UA Services.

Die IoT-Testware ergänzt die bestehenden Tests bei Audi zu Interoperabilitäts- und Sicherheitsfragen bei der Inbetriebnahme von Anlagen. Hierdurch können entsprechende Risiken und Aufwände reduziert werden.

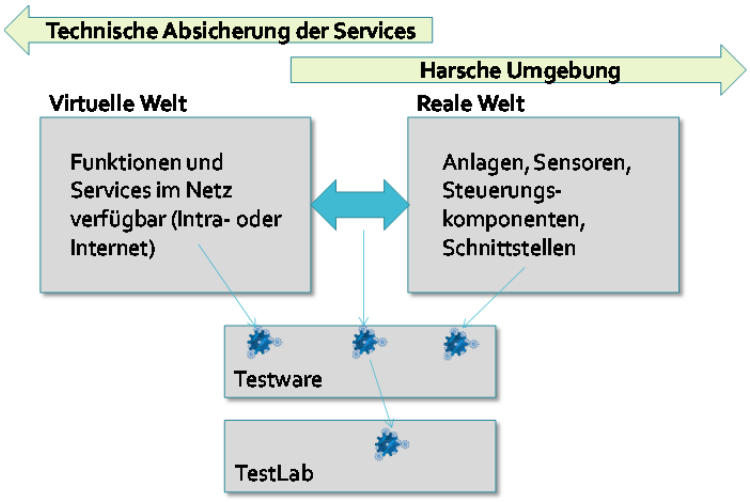

Abbildung 4: Geplante Nutzung von IoT-Testware und IoT-Testlab im Audi-Szenario

2.6. Protokolle, Standards

Neben Standardprotokollen wie TCP/IP wird von der Nutzung von OPC-UA im Audi-Szenario ausgegangen. Für die Servicebeschreibung wird zurzeit USDL und WSDL eingesetzt. Eine spätere Nutzung oder Einbindung von REST ist ebenfalls angedacht. Hinzu kommen anlagenspezifische Schnittstellen.

2.7. Schritte zur Umsetzung des Audi Demonstrators

2.7.1. Geplanter Anwendungsdemonstrator und Testdemonstrator

Der Demonstrator dient zur Darstellung der möglichen industriellen Nutzung der IoT Testmethoden, der IoT-Testware und der Ergebnisse der IoT-Testlabs (z.B. Sicherheitszertifikate für IoT

Komponenten). Der Demonstrator dient als Referenz für industrielle Anwendungen, ist aber nicht direkter Bestandteil des IoT-Testlab. Der Aufbau des Demonstrators folgt den Konzepten und Anforderungen der modularen Shopfloor IT bei Audi, welche eine modellbasierte Konfiguration der Shopfloor IT über vordefinierte Module erlaubt. Die verfügbaren Bestandteile sind in Abbildung 5 dargestellt.

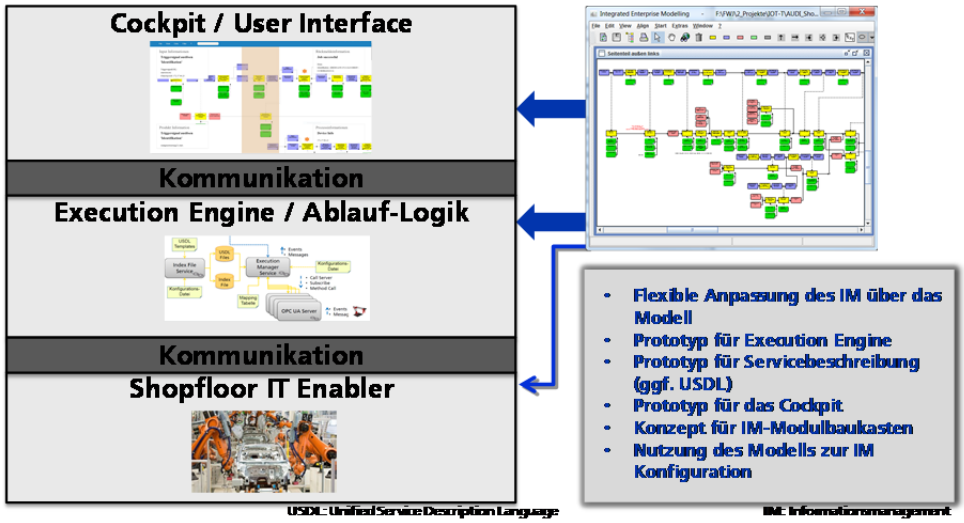

Abbildung 5: Ausgangskonzept für den Anwendungsdemonstrator Shopfloor IT

Um eine Umgebung für das schnelle und einfache Erproben der IoT-Testmethoden und IoT-Testware, bezogen auf die modulare Shopfloor IT bereitzustellen, wird am IPK ein entsprechender Demonstrator realisiert (siehe Abbildung 6).

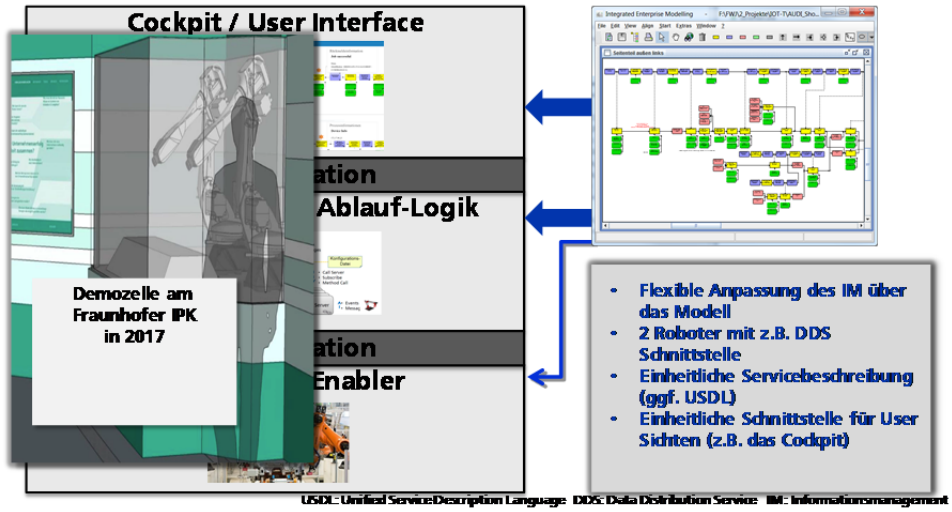

Abbildung 6: Anwendungsdemonstrator modulare Shopfloor IT

Die Idee ist die Evaluierung der IoT-Testware beispielsweise zur Nutzung für Konformitätstests von Funktionen und Services, welche von den Anlagen (Robotern) zur Verfügung gestellt werden

möglichst unter der Verwendung von zertifizierten Standardprotokollen. Der Demonstrator wird die Darstellung in der Test-Story Kapitel 2.3 veranschaulichen und greifbar machen.

3. Relayr Szenario: Beurteilung von Gateways

Das Szenario fokussiert auf der Beurteilung der Eignung von Gateways und Hubs für den IoT-Einsatz.

3.1. Ziele

- Schnelle und kostengünstige Einschätzung von Gateway-Hardware- und Software-Lösungen.
- Beurteilung, ob die Gateway-Lösungen den Anforderungen entsprechen.
- Erkennung von Funktions- und Konfigurationsabweichungen auf verschiedenen Gateway-Plattformen.
- Bereitstellung der Ergebnisse in Form von Daten, die zur Bestätigung der Eignung einer Gateway-Lösung für einen bestimmten Verwendungszweck dienen können.

3.2. Zusammenfassung

Lösungen für den Anschluss von Endgeräten an das Internet werden immer gebräuchlicher. Für Lösungen aus Hardware, Betriebssystem und Anwendungspaketen, wie etwa Relayr Vertex, gibt es zahlreiche Einsatzszenarien. Die Interoperabilität der einzelnen Komponenten einer Gateway-Lösung ist allerdings nicht garantiert. Zuverlässigkeit, Sicherheit, Interoperabilität und umfassende Funktionsfähigkeit müssen überprüft werden.

Als aktueller Stand der Technik gelten zahlreiche manuelle Prozesse, die für jede neue Lösung bzw. jedes Upgrade einer bestehenden Lösung neu überdacht werden müssen. Eine solche Vorgehensweise ist kostspielig und fehleranfällig. Die IoT-Testware würde eine Umgebung liefern, in der die grundlegenden Funktionen des Gateways kosteneffizient und zuverlässig getestet werden könnten.

Dabei liegt der unmittelbare Schwerpunkt auf Industrie-Gateway-Lösungen. Die gleichen Prüfstandards können aber auch bei Cosumer-IoT-Hubs Anwendung finden, die sich typischerweise in Smart-Home-Lösungen finden.

Ergebnis eines solchen Tests wäre die Bestätigung, dass sich eine konkrete Lösung für ein konkretes Szenario eignet.

3.3. Beteiligte und deren Aufgaben

An der Entscheidung zur Prüfung einer Gateway-Lösung sind unter Umständen verschiedene Parteien beteiligt.

Beteiligte:

- Gateway-Anbieter bzw. dessen Partner
- Betriebssystem-Anbieter bzw. dessen Partner
- Software-Anbieter
- Prüftechniker/-ingenieure
- Kunden (Geschäftseinheiten bzw. Einkauf/Beschaffung)

- Softwareentwickler
- Systemarchitekt (bzw. Systemintegrator)
- Verkäufer/Vertriebsmitarbeiter

Mögliche Aufgaben:

- Einrichtung eines Testlabors (erfolgt einmalig)
    - Bestellung von Testhardware
    - Bereitstellung der Testausrüstung
    - Erweiterungsmöglichkeiten für Testlabor vorsehen
- Analyse der Spezifikationen des Hardware-Anbieters
- Analyse der Anforderungen der Software
- Bestellung der Gateway-Hardware gemäß den Spezifikationen
- Test der Kompatibilität der Hardware mit der Software
    - Anschluss und Konfiguration der Hardware
    - Entwicklung von Software für die Hardware
    - Ausführung der Skripte
    - Realisierung der Szenarien
    - Korrektur der Testabläufe anhand der Beobachtungen
- Erstellung eines Test- bzw. Prüfberichts

3.4. Testszenarien

Eine Reihe von Herstellern bietet bereits IoT-Gateway-Lösungen an, die ausschließlich für den industriellen Einsatz vorgesehen sind. Dazu gehören bekannte Gateways namhafter IT-Anbieter:

- Gateway Dell Edge 5000
- Router der Baureihe Cisco IR
- Baureihe Advantec ARK
- HP Edgeline IoT Systems

Zu den Anbietern aus der traditionellen Industriesteuerung gehören:

- B&R Automation PC910
- Plattform National Instruments CompactRIO
- Router InSYS MRO
- Baureihen TTTech nerve MFN sowie RFN

Die Gateway-Hersteller haben angegeben, dass diese Gateways ausdrücklich für das IoT entwickelt wurden. Allerdings unterscheiden sich Spezifikationen und Funktionsumfang dieser Gateways erheblich voneinander. Da weder formale Kriterien vorliegen noch ein Zertifizierungsprozess besteht, kommt es zu Problemen wenn Industriekunden eine Produktionslinie um IoT-Funktionen erweitern wollen. In den folgenden Unterkapiteln werden die ermittelten Anwendungsfälle dargestellt.

3.4.1. Fertigungsunternehmen mit bereits bestehender angeschlossener IoT-Infrastruktur

Zahlreiche Hersteller möchten ihre bestehenden Lösungen um IoT-Lösungen erweitern und auf diese Weise Prozessoptimierungen, Echtzeit-Überwachung oder vorbeugende Wartung realisieren.

3.4.1.1. Beurteilung der Eignung einer bestehenden Gateway-Lösung

Ein Hersteller hat möglicherweise bereits beträchtliche Investitionen getätigt und seine technische Infrastruktur um entsprechende IT-Ausrüstung ergänzt. Er möchte nun überprüfen, ob er seine bestehende IoT-Infrastruktur nutzen kann, um IoT-Lösungen funktional wie ein Gateway betreiben zu können.

3.4.1.2. Beurteilung der Eignung eines Upgrades der Gateway-Hardware

Für bestehende IT-Lösungen ist ein Upgrade vorgesehen. Eventuell als Teil eines Standardverfahrens, aufgrund von Ausfällen oder ganz einfach im Rahmen neuer Geschäftsmodelle. Hier soll eine Gateway-Lösung mit neuer Hardware eingesetzt und eine geeignete Lösung gefunden werden.

3.4.1.3. Beurteilung der Eignung eines Upgrades der Gateway-Software

Vereinzelt besteht eventuell bereits eine vollständige IoT-Infrastruktur, die aber auf den neuesten Stand gebracht werden soll. Dabei können sich Software- und Hardware-Lösungen unabhängig voneinander entwickeln. Bevor über ein Upgrade nachgedacht wird, könnte das Technik-Team die Eignung der Lösung noch einmal bestätigen.

3.4.2. Fertigungsunternehmen (Produzent) erwägt den Einsatz neuer IoT-Infrastruktur

Die Spezifizierung von IoT-Infrastruktur für eine neue Anlage ist unter Umständen einfacher.

3.4.2.1. Beurteilung der von einem Anbieter vorgeschlagenen Gateway-Lösung

Anbieter von Steuerungsausrüstung bieten teilweise bereits Gateway-Lösungen an. Der Kunde möchte eventuell ein konkretes Angebot prüfen, das ihm unterbreitet wurde. Eine vorliegende Zertifizierung wäre für ihn ein guter Anhaltspunkt für die Entscheidung.

3.4.2.2. Beurteilung der Angebote zur Lieferung neuer Hardware über Ausschreibung

Der Kunde sucht aktiv eine neue Gateway-Lösung. Um mehrere Angebote vergleichen zu können, hat er eine Ausschreibung vorgenommen, an der sich verschiedene Anbieter beteiligen können. Eine Zertifizierung wäre Bestandteil dieser Ausschreibung.

3.4.2.3. Beurteilung eines Gateways, das von einem Geschäftspartner bereitgestellt wird

Auch ein Geschäftspartner kann ein Gateway anbieten und die Nutzung eines Gateways vorschlagen oder strebt ein IoT-Joint-Venture an. Dann erwirbt der Kunde eine Gateway-Lösung nicht direkt, sondern investiert in den Funktionsumfang einer Gateway-Lösung.

3.4.3. Gateway-Hersteller

Hersteller von Gateway- und Controller-Lösungen würden erheblich in Forschung und Entwicklung investieren, wenn sie auf einen quantifizierbaren Zertifizierungsprozess zurückgreifen könnten, dem ihre Lösung zu entsprechen hat. Auf dem Markt wären zertifizierte Lösungen gegenüber nicht zertifizierten Lösungen im Vorteil.

3.4.3.1. Entwicklung eines neuen Gateway-Produkts

Ein klar vorgegebener Zertifizierungsprozess würde Herstellern, die die Einführung neuer IoT-Gateway-Modelle beabsichtigen, Leitlinien an die Hand geben. Mit einer Zertifizierung würden feste Kriterien vorgegeben, auf die Verbraucher zurückgreifen könnten, um informierte Entscheidungen zu treffen. Darüber hinaus würden transparente Benchmarks festgelegt, die zur Entwicklung eines geeigneten Produkts dienen können.

3.4.3.2. Beurteilung eines bestehenden Produkts

Auf dem Markt werden, wie bereits erwähnt, schon zahlreiche spezialisierte IoT-Gateways angeboten. Da der IoT-Markt noch jung ist, ist es für Gateway-Hersteller schwierig, den Kunden vor wichtigen Investitionsentscheidungen entsprechende Zusicherungen zu geben. Mit einer Zertifizierung würden feste Kriterien vorgegeben, auf die Verbraucher zurückgreifen könnten, um informierte Entscheidungen zu treffen.

3.5. Potenzielle Testschritte

Aller Voraussicht nach sind zur Realisierung der Projektziele folgende Schritte notwendig, um im Rahmen der Tests ein umfassendes Bild zu bekommen.

IoT-Testlab

- Grundlegende Kompatibilitätstests auf der Grundlage von Datenblättern und Spezifikationen
- Test der Erreichbarkeit der physischen Ports: IO-Link, CAN-Bus, USB
- Test der Netzwerkzuverlässigkeit mit TestWare: WLAN, Ethernet, Bluetooth, UMTS

IoT-Testware

- Einfache und zuverlässige Anwendungsbereitstellung (Software-Installation)

- Einfache und zuverlässige Aktualisierung (Sicherheitspatches, Fehlerkorrekturen, neue Versionen)
- Test der Wiederherstellbarkeit bei Neustarts oder Fehlfunktionen (Watchdog-Prozess)
- Test der Rechenlast
- Test der Interoperabilität verschiedener Protokolle
- Test der Sicherheit

3.6. Prozess mit Grenzfällen und Einflussfaktoren

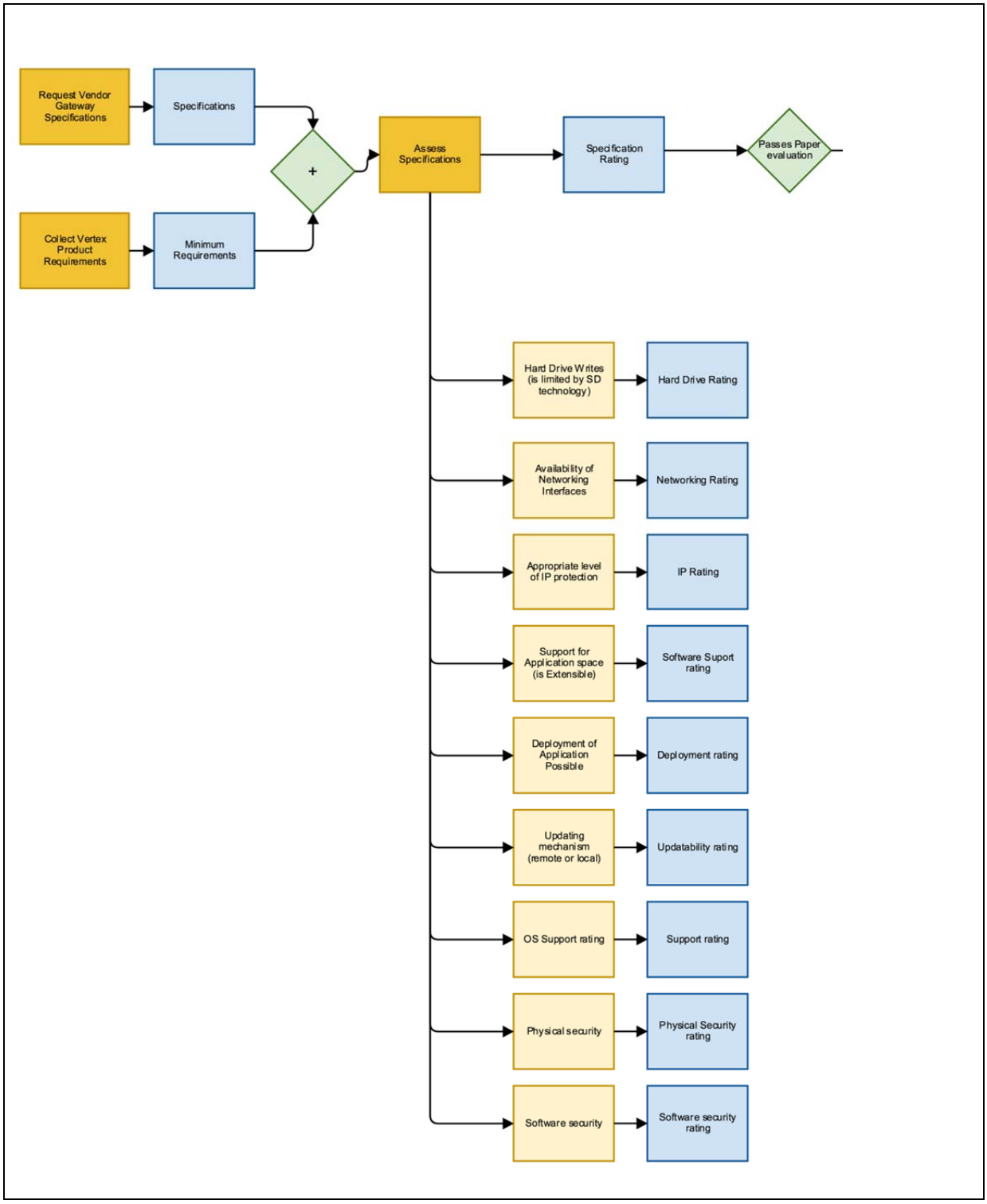

Abbildung 7: Relayr Prozess Teil 1

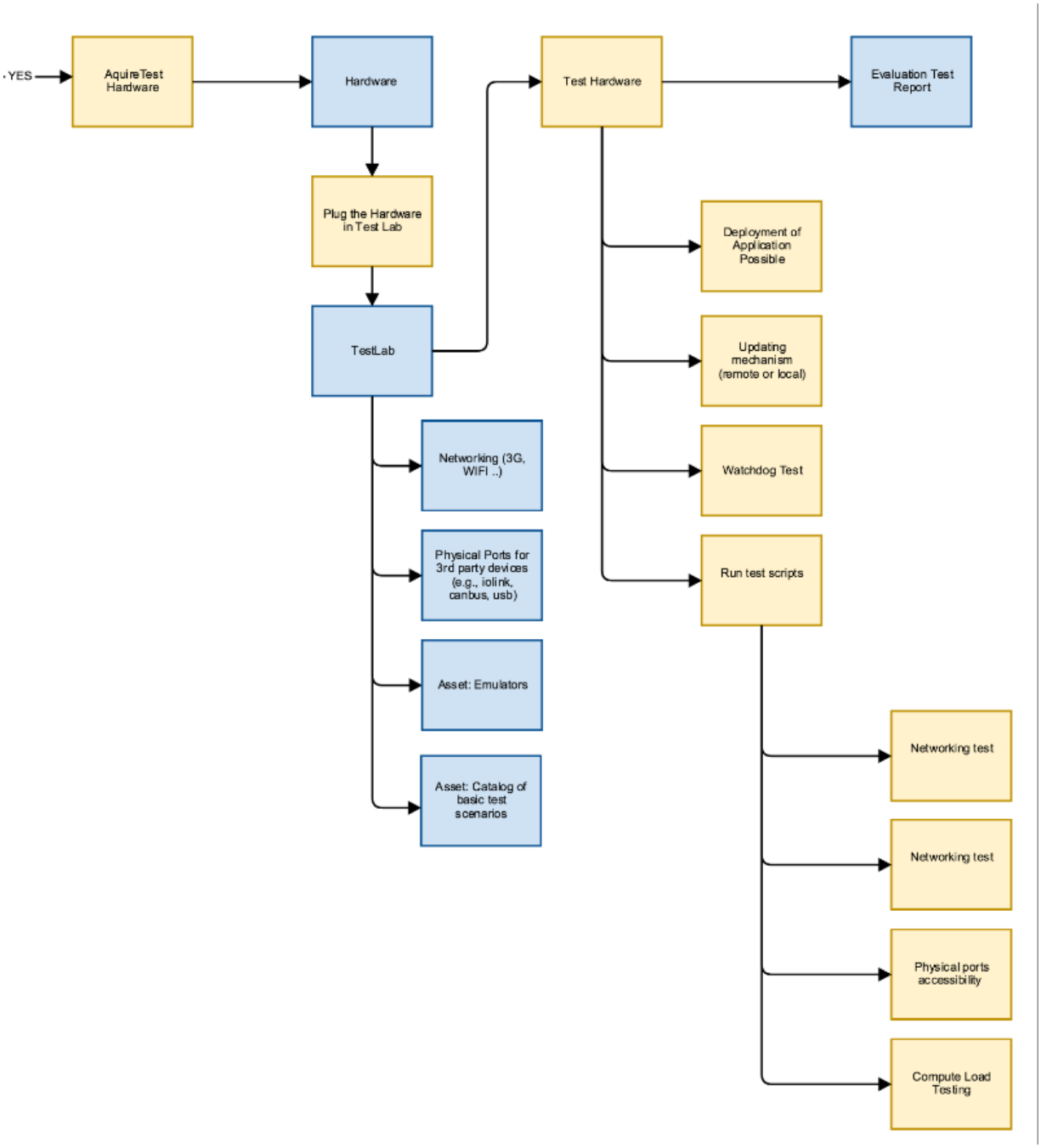

Abbildung 8: Relayr Prozess Teil 2

3.7. Vorteile und Indikatoren

Vorteile:

- Effiziente Analyse von Gateway-Lösungen

- Schrittweiser Prozess zur schnellen Fehlererkennung spart Zeit
- Transparentes datenbasiertes Ergebnis, um vernünftige Entscheidungen zu ermöglichen

Indikatoren:

- Identifikation von Schwächen des getesteten Gatewaysystems, um inkompatible, unvollständige oder fehlerhafte Lösungen zu erkennen.

3.8. Voraussetzungen für die Implementierung

Folgende Testtypen sind für das Szenario relevant:

1. Konnektivitätstests
2. Datenübertragungstests
3. Wartungseignung (Aktualisierung/Update)
4. Sicherheit
5. Haltbarkeit (physikalische Bedingungen)
6. Funktionstest
7. Widerstandsfähigkeit
8. Leistungstest (Minimum)

3.9. Protokolle, Standards und Sicherheitsanforderungen

3.9.1. Protokolle

Eine Gateway-Lösung soll den Übergang von einem Systemtyp zu einem anderen Systemtyp ermöglichen. An dieser Stelle könnten zahlreiche bestehende Industrieprotokolle sowie neu entwickelte IoT-Protokolle geprüft werden. Wir haben die folgenden Protokolle als Maß für Interoperabilität ausgewählt.

Protokoll		URL
MQTT	NA	http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/errata01/os/mqtt-v3.1.1-errata01-os-complete.html
CoAP	RFC 7252	https://tools.ietf.org/html/rfc7252
OPC-UA		https://opcfoundation.org/about/opc-technologies/opc-ua/

3.9.2. Standards

Zahlreiche bereits bestehende Zulassungen eignen sich unter Umständen für die Beurteilung bestimmter Teile einer Lösung (IEC-62443, OWASP usw.). Außerdem müssen Ansätze wie das IEEE P2413 (Standard for an Architectural Framework for the Internet of Things – Standard für ein Architektur-Framework für das Internet der Dinge) berücksichtigt werden.

3.9.3. Sicherheitsfunktionen

IoT-Lösungen sind einer Vielzahl von Bedrohungsvektoren ausgesetzt. Gateways und Hubs spielen eine kritische Rolle bei der Abwehr von Bedrohungen einer IoT-Anlage, die auf Angreifer oder fehlerhafte Ausrüstung zurückgehen. Das TestLab sollte Tests in den entsprechenden Bereichen vornehmen:

- Sicherheit und Qualität des Uplinks
- Betriebssicherheit und Zuverlässigkeit in einem kompromittierten/feindlichen Netzwerk
- Physische Sicherheit eines Gateways oder Hubs
- Softwareintegrität

4. Zusammenfassung und Ausblick

Die Szenarien decken sowohl Anwender (Audi) als auch Provider (Relayr) von IoT Lösungen ab. Damit ist die Grundlage für die gezielte Identifikation von Anforderungen gelegt (R1.2). Während der Diskussion der anwendungsfälle wurde bereits eine Reihe von Begriffen identifiziert, welche in das IoT Test Glossar (R1.3) aufgenommen und definiert werden. Hierfür wurde jeweils eine Webanwendung bereitgestellt, um die kontinuierliche Sammlung von Anforderungen und Begriffen zu unterstützen. Die beschrieben Szenarien beinhalten zudem bereits die Konzepte für Anwendungsdemonstratoren, welche zum einen den Test der IoT-Testware als auch deren späteren Demonstration und Verbreitung unterstützen können.

Unabhängig von den Anwendungspartnern im Projekt hat sich die Relevanz insbesondere zur Absicherung von Sicherheitsaspekten weiter verstärkt. Nachdem erste Zwischenfälle durch schlecht gesicherte Technik mit Internet-Anschluss die Risiken dieser Technologie zeigen. Im November 2016 hat das Heimatschutzministerium der USA "strategische Grundsätze für die Sicherung des Internet of Things“ veröffentlicht [10]. Somit erscheint die im Projekt identifizierte Notwendigkeit von Tests im Rahmen der Cybersicherheit als sehr relevant.

5. Referenzen

1. Bajric, A., Mertins, K., Rabe, M., Jaekel, F.-W.: A Success Story: Manufacturing Execution System Implementation. In the Proceeding of the 6th International Conference on Interoperability for Enterprise Software and Applications (IESA 2010), Springer, Coventry, UK, April 13-15, 2010.
2. Wintrich,W., Gering, P., Meissner, M. Interactive Process Oriented Requirements Management. On the move to meaningful Internet systems. OTM 2015 conferences : Confederated international conferences: CoopIS, ODBASE, and C&TC 2015, Rhodes, Greece, October 26-30, 2015; Proceedings S.303-310.
3. Spur, G., Mertins, K., Jochem, R.: Integrierte Unternehmensmodellierung. Beuth, Berlin (1993).

4. Fraunhofer IPK, www.moogo.de. Letzter Zugriff Februar 2017.
5. http://www.volere.co.uk/. Letzter Zugriff Februar 2017.
6. IEC 62443
7. ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.. Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0). http://www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf. Letzter Zugriff Februar 2017.
8. Struktur der Verwaltungsschale Fortentwicklung des Referenzmodells für die Industrie 4.0-Komponente, April 2016 http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=6
9. Riedel, O.; Margraf, T.; Stölzle, S.; Knothe, T.; Eggers, A.; Wintrich, N.: Modellbasierte modulare Shopfloor IT - Integration in die Werkzeuge der Digitalen Fabrik. Study, Electronic Publication 2014. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3162488.pdf.
10. Orcutt, M.:Lebensgefährliches Internet der Dinge?. Technology Review. Heise 7.12.2016. https://www.heise.de/tr/artikel/Lebensgefaehrliches-Internet-der-Dinge-3562468.html