2.4 Virtual Fort Knox: Sichere IT-Infrastruktur für die deutsche Wirtschaft

[Johannes Diemer | Hewlett-Packard]

2.4.1 Industrie 4.0: Vom Konzept zur Infrastruktur

Wie reagiert der weltweit sehr erfolgreiche deutsche Maschinen- und Anlagenbau auf die in den Kapiteln 2.1 und 2.2 beschriebenen Herausforderungen der Dynamisierung von Produktlebenszyklen und die Individualisierung von Produkten? Wie meistert er den im Kapitel 2.3 beschriebenen Wandel der Produktions- und Geschäftsparadigmen hin zu kooperativen Produktions- und Wertschöpfungsverbünden (horizontalen Wertschöpfungsnetzwerken)?
Hierfür wird eine offene, föderative und zugleich hochsichere ITK-Infrastruktur notwendig sein, die solche horizontalen Wertschöpfungsnetzwerke ermöglicht. Das Fraunhofer Institut für Produktionstechnik und Automatisierung (IPA) und HP haben in der gemeinsamen, vom Land Baden-Württemberg geförderten Forschungsinitiative Virtual Fort Knox (VFK) ein Referenzmodell einer solchen Plattform für produzierende Unternehmen konzipiert. Ein besonderes Anliegen der Initiative ist die Einbeziehung kleiner und mittelständischer Unternehmen des Maschinen- und Anlagenbaus, damit diese durch Kooperation ihre Effizienz steigern können und dadurch im globalen Wettbewerb ihre weltweit führende Rolle weiter ausbauen können.
Virtual Fort Knox lässt sich aus zweierlei Blickwinkeln beschreiben:

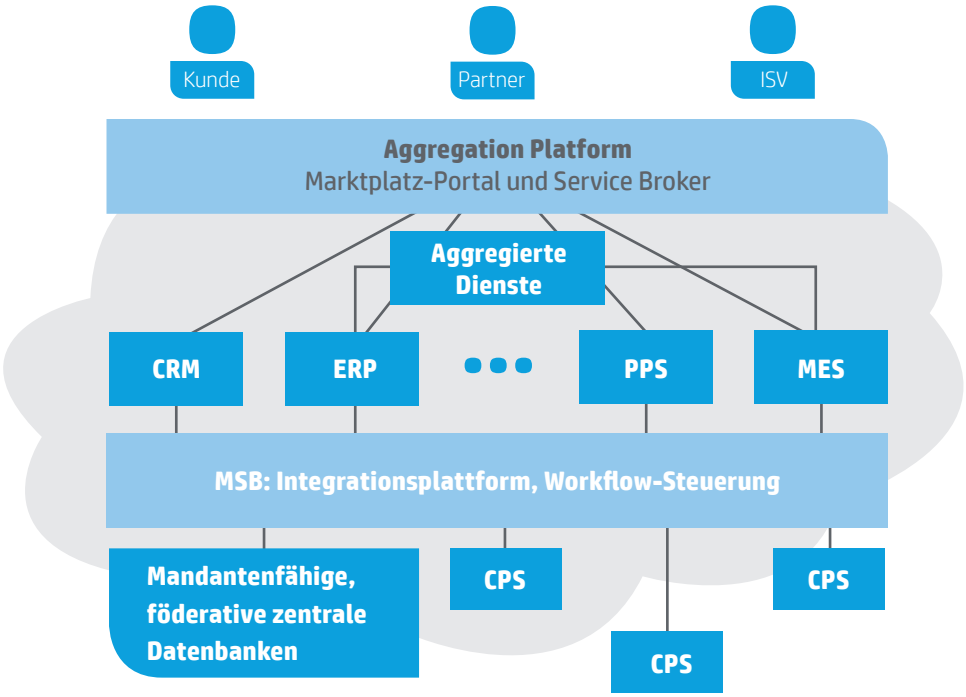
- Einerseits **inhaltlich-technisch.** Hier geht es um die technischen Aspekte der IT-Infrastruktur einschließlich der Integration der sogenannten „Cyber-Physical Systems“ (CPS) sowie um die notwendigen Konzepte, Lösungen für die Sicherheit (Schutz des Wissens und IP) und Verlässlichkeit. Die Umsetzung der Initiative zielt darauf ab, im Sinne von Industrie 4.0 mit der Plattform die folgenden drei Merkmale zu realisieren: (1) Horizontale Integration über Wertschöpfungsnetzwerke, (2) digitale Durchgängigkeit des **Engineerings** über die gesamte Wertschöpfungskette sowie (3) vertikale Integration und vernetzte Produktionssysteme.[1] Schließlich stellt sich die Frage des geeigneten Betreiber-Modells bzw. der Organisationsform des/der Betreiber(s) und der entsprechenden Geschäftsmodelle. Im Rahmen dieser Initiative wurde ein „Proof of Concept“ (PoC) vorgelegt.

- Andererseits stand die Frage, welche Rolle **Vertrauen und Akzeptanz** beim Aufbau einer solchen Plattform spielen, von Anfang an im Zentrum des Forschungsprojektes. Warum soll ich die Plattform Virtual Fort Knox nutzen? Werden mein Wissen und IP im Rahmen der Kooperation ausreichend geschützt? Ist die Kooperation für mich rentabel, bringt sie zusätzlichen Umsatz, Gewinn oder reduziert sie wesentlich meine Kosten? Dies sind die typischen Fragen, die durch die Initiative beantwortet werden müssen.

Kapitel 2.4.2 beschreibt die technischen Kernelemente in gebotener Kürze. Kapitel 2.4.3 geht auf die Aspekte Akzeptanz und Vertrauen ein. Kapitel 2.4.4 behandelt die Frage des Geschäftsmodells für eine digitale Industrieplattform.

2.4.2 Technische Kernelemente

Zweck der VFK-Plattform ist die Unterstützung der unternehmensübergreifenden Kooperation durch die intelligente Vernetzung aller Ressourcen in den Unternehmen und über die Unternehmensgrenzen hinaus. Informationen bzw. Daten werden in unterschiedlichen Unternehmen und Unternehmensbereichen erfasst und auf der VFK-Plattform zusammengeführt. Zu den technischen und physischen Datenquellen zählen unter anderem intelligente Lager, Werkzeuge und Material, mobile Ressourcen, Maschinen und Anlagen, Mitarbeiter, intelligente Robotersysteme bis hin zu ganzen Fabriken. Jedes intelligente, mit Sensoren oder Aktoren ausgerüstete System, auch Cyber-Physical System genannt, unterstützt zukünftig neben der Informationsverarbeitung die Kommunikation zwischen den Ressourcen untereinander.
Entscheidend dabei ist der föderative Charakter der Plattform, die den Schutz von Wissen und geistigem Eigentum (Intellectual Property – IP) sicherstellt. Föderativ bedeutet in diesem Kontext, dass die VFK-Plattform, Dienste und Anwendungen von unterschiedlichen Teilnehmern gemeinsam für kooperative Aktivitäten genutzt werden, wobei aber für jeden der Teilnehmer die eigene Komponente beziehungsweise der eigene Kontext gesichert bleibt. Es werden nur die Daten und Informationen zwischen den Teilnehmern ausgetauscht, die für das gemeinsame Agieren notwendig sind.



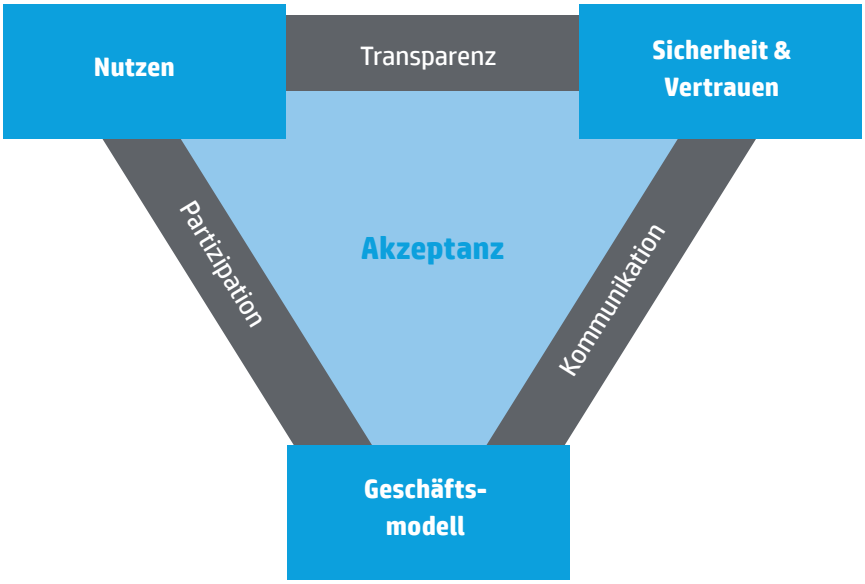
Grafik 13: VFK-Referenzarchitektur

Der Zugang erfolgt über eine Aggregation-Plattform. Sie dient als Markplatz und ist als Broker für das Aufsetzen und die Verwaltung (einschließlich der Abrechnung) von aggregierten Diensten, die mehrere Dienste in Workflows zusammenfassen, zuständig. Die Mitarbeiter in produzierenden Unternehmen (Kunden) nutzen über die Aggregations-

Plattform anforderungsgerechte Software-Lösungen und Dienste bei der Ausführung ihrer Tätigkeiten. Anbieter von Software und Diensten (ISVs und Partner) bieten über sie ihre Leistungen an.
Die Offenheit der Plattform wird in der Referenzarchitektur durch die Konzeption eines systemoffenen Kommunikationssystems realisiert. Dabei handelt es sich um einen Manufacturing Service Bus (MSB) mit Schnittstellen zur Vernetzung der föderativen Plattform mit Diensten für betriebswirtschaftliche Verwaltungs- und Planungssysteme (CRM, ERP) und Produktionsplanungssysteme (PPS, MES). Über den MSB werden auch die Datenschnittstellen der Cyber-Physical-Systems (CPS) sowie mandantenfähige, föderative Datenbanken angebunden.

2.4.3 Vertrauen und Akzeptanz: Das Vertrauensmodell des VFK

Subjektive Wahrnehmungen als Kernelement einer technischen Plattform
Die zukünftigen Kooperationspartner werden hohe Ansprüche an die Sicherheit der Plattform stellen, da diese Teile ihres geistigen Eigentums in Form von Daten und Informationen in den Verantwortungsbereich des VFK übertragen werden. Das können beispielsweise Informationen über Geschäftsprozesse oder Daten über das technische Know-How des Kunden sein (unter anderem in Form von Konstruktionsdaten von Maschinen). Des weiteren stellt die Bereitschaft, Kooperationen mit bislang unbekannten Partnern einzugehen, eine weitere Komplexitätsstufe dar, die Aufbau und Aufrechterhaltung von Vertrauen verlangt.[2]
Vertrauen ist ein vielfältiger Begriff, der aus unterschiedlichen Perspektiven definiert werden kann. Aus der Sicht des BSI „[...] basiert Vertrauen auf der Einschätzung, ob ein Anbieter alle Risiken ausreichend, angemessen und nachhaltig abgedeckt hat, sowohl diejenigen aus dem Bereich der Informationssicherheit als auch jene aus Bereichen wie Datenschutz, Technik und Recht".[3] Nach Schweer gründet sich Vertrauen in eine Organisation auf der **Wahrnehmung** von Transparenz, Partizipationsmöglichkeiten, Kooperationsbereitschaft, Orientierung an ethischen und moralischen Prinzipien, langfristiger Glaubwürdigkeit und Gerechtigkeit für alle Mitglieder der Organisation.[4] Es geht also um die subjektive Wahrnehmung der Personen, deren Vertrauen man gewinnen will, und nicht um eine objektive Sicherheit, die gewährleistet wird. Dies wurde auch in Expertengesprächen bestätigt, die im Rahmen des Projekts geführt wurden. Vertrauen ist für die Gesprächspartner kein statischer Wert, sondern sollte sich aus der Interaktion der kooperierenden Partner auf persönlicher Ebene entwickeln. Deshalb lässt sich Vertrauen in die Plattform nicht direkt durch deren funktionelle und sicherheitstechnische Spezifikation erreichen. Notwendig ist eben die menschliche Interaktion in Form von Kommunikation, Kooperation sowie Koordination.
Im Rahmen des Projekts wurde ein Vertrauenskonzept entwickelt, das Akzeptanz als Ergebnis von planbaren Maßnahmen und Prozessen erzeugt, die den Aufbau sowie die Aufrechterhaltung von Vertrauen fördern.



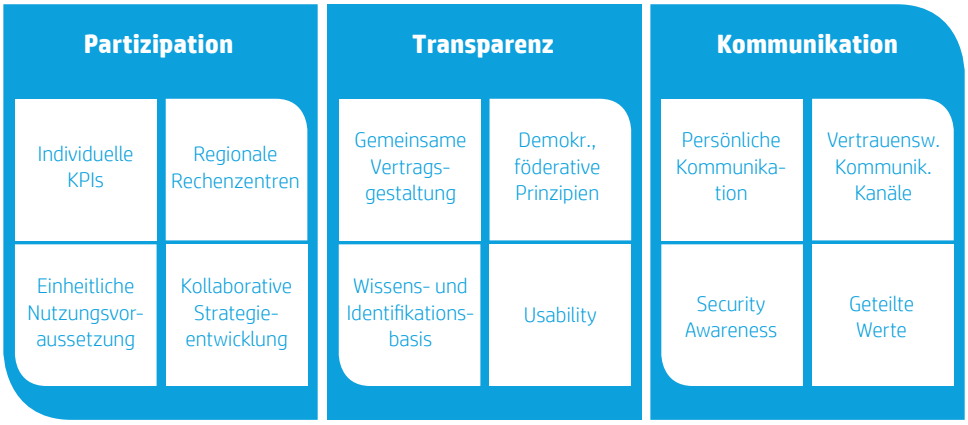
Grafik 14: Akzeptanz als Kernelement des Virtual Fort Knox

Akzeptanz wird im Kontext des VFK als der Zustand angesehen, der einen Anwender motiviert, sich dem Konsortium anzuschließen. Das ist genau dann der Fall, wenn er Vertrauen in das Plattformkonsortium hat, er sich einen Nutzen aus den Plattformfunktionen verspricht und wirtschaftlichen Erfolg erwartet. Das Vertrauensmodell des VFK geht davon aus, dass sich Akzeptanz nur indirekt über die drei Komponenten Geschäftsmodell, Nutzen sowie Sicherheit und Vertrauen beeinflussen lässt. Dazu stehen Mittel der Transparenz- und Kommunikationsgestaltung sowie die Möglichkeit zur Partizipation zur Verfügung.[5]

Die Partizipation ist dabei der entscheidende Gedanke. Sie wird durch Mitwirkungsrechte und -pflichten über die Leistungserbringung der VFK-Plattform erreicht. Die beteiligten Partner und Kunden werden in die Entwicklung und der Regelung des Betriebs der Plattform einbezogen und erhalten somit eine Identifikationsmöglichkeit, die über eine Kunde-Dienstleister-Beziehung hinausgeht. Die Einbeziehung soll eine effiziente Abdeckung und Abstimmung der unterschiedlichen Anforderungen durch Kunden, Software- und Dienste-Anbieter ermöglichen. Formal wird dies in Regeln für das föderative Kooperationsmodell und in der Gesellschaftsform des VFK verankert.

Dabei ist der Grad der Mitwirkung auf ein sinnvolles und angemessenes Maß zu beschränken. Es ist angedacht, in Abhängigkeit des Engagements der Partner hier verschiedene Klassen der Mitwirkung zu realisieren. Beteiligte Partner können direkt Gesellschafter werden oder aber Anteile an der Gesellschaft erwerben. So entscheiden sie durch ihr Investment in die Gesellschaft über den Grad ihrer Mitwirkung sowie ihrer Beteiligung an Gewinnen der VFK-Plattform. Angestrebt wird eine Beteiligung insbesondere der Maschinen- und Anlagenbauer, um den besonderen Anforderungen dieses Leitmarktes gerecht zu werden.

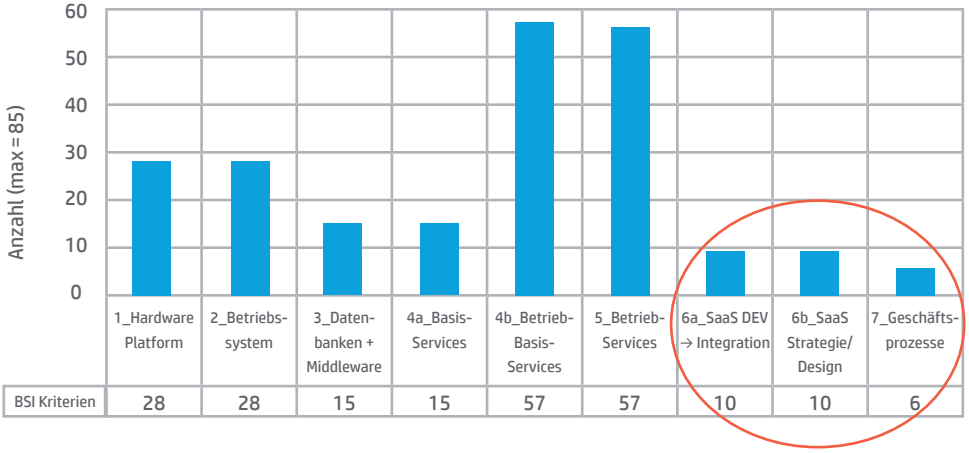
Sozio-emotionale Vertrauensstrategien



Grafik 15: Integrationsmodell zur Schaffung von Akzeptanz im VFK

Technische Umsetzung

Grundsätzlich bietet sich bei der technischen Umsetzung zunächst eine Orientierung an den BSI-Standards der 100er Reihe an. Darin wird der Aufbau eines Informationssicherheitsmanagements nach dem BSI-Standard „100-2 IT-Grundschutz und Vorgehensweise" vorgeschlagen. Das Umsetzen dieser Maßnahmen bietet eine sehr gute Möglichkeit, ein grundlegendes Informationssicherheitsniveau zu erreichen.
Im Rahmen des Projekts wurde jedoch festgestellt, dass die Maßnahmen nach IT-Grundschutz nicht vollständig geeignet sind, um die besonderen Anforderungen für eine unternehmensübergreifende Zusammenarbeit auf der VFK-Plattform abzubilden. Die aktuellste Version des BSI-Standards aus dem Jahre 2008 geht auf die besonderen Anforderungen des Cloud-Computing ein, fokussiert sich dabei aber auf die Ebenen bis zu SaaS und macht zu den noch relativ jungen Geschäftsprozessen in Wertschöpfungsnetzwerken keine konkreten Aussagen. Auch das Cloud-Computing-Eckpunktepapier des BSI ist nicht detailliert genug, um daraus eine konkrete, die Geschäftsprozesse einschließende Sicherheitsarchitektur für eine Community Cloud abzuleiten.[6]

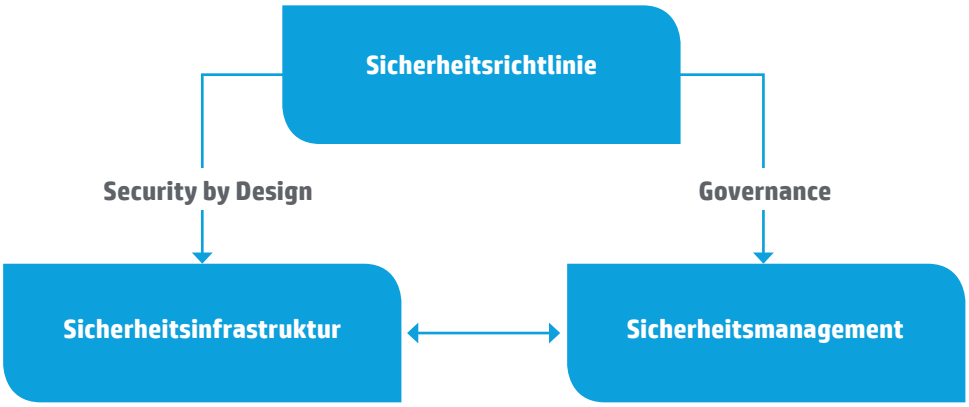


Grafik 16: Verteilung BSI-Kriterien auf Cloud-Referenzarchitektur gemäß Eckpunktepapier (Quelle: interne HP-Studie)

Klar ist: Die bisher weit verbreitete Reduzierung der Sicherheit auf die Darstellung der technischen Leistungsfähigkeit von IKT-Schutzmechanismen reicht nicht aus, um Vertrauen zu schaffen. Die Komplexität dieser Schutzmechanismen ist oft für den Anwender nicht mehr nachvollziehbar und behindert sogar eher die Akzeptanz neuer IKT-Leistungsmodelle. Daraus ergibt sich, dass ein über die Sicherheitsarchitektur hinausreichendes Vertrauensbildungskonzept erforderlich ist, um der Sorge um Daten- und Kontrollverlust zu begegnen.[7]

- Das Architekturdesign befasst sich mit der Konzeption der Sicherheitsarchitektur und der darauf aufbauenden Sicherheitsmanagementprozesse. Dabei steht vor allem die Erfüllung der klassischen Informationsschutzziele Vertraulichkeit, Verfügbarkeit und Integrität von Daten und Kommunikationsinfrastrukturen im Vordergrund.
- Die Definition der Vertrauensprozesse hat dagegen die Schaffung von Akzeptanz für das VFK auf der Ebene sozio-emotionaler Einflussfaktoren zum Ziel. Diese umfasst Konzepte zur Förderung kollaborativer Arbeitsprozesse, die Definition von Kommunikationsstrukturen sowie von Partizipationsmöglichkeiten durch die Plattformpartner.

Die Sicherheitsarchitektur des Virtual Fort Knox implementiert Konzepte zur ganzheitlichen Betrachtung von technischer Sicherheit zum Management der VFK-Sicherheit. Eine Sicherheitsrichtlinie dient als zentrales Instrument zur Steuerung der Informationssicherheit. Aus der Sicherheitsrichtlinie leitet sich, unter Berücksichtigung des Security-by-Design-Ansatzes, zum einen die Sicherheitsinfrastruktur ab und zum anderen, unter Einbeziehung der Aspekte der Governance, das Sicherheitsmanagement der Plattform. Dabei beeinflussen sich die Sicherheitsinfrastruktur und das Sicherheitsmanagement gegenseitig. Die konkrete Implementierung der Infrastruktur hängt von den Anforderungen ab, die sich aus der Definition der Sicherheitsrichtlinie und des Sicherheitsmanagements ergeben.



Grafik 17: VFK-Sicherheitsarchitekturmodell

Die Sicherheitsrichtlinie des Virtual Fort Knox umfasst ein Sicherheitsschichtenmodell mit den dazugehörigen Bewertungskriterien und Schutzzielen sowie die Definition von organisatorischen Rollen und Verantwortlichkeiten in der Sicherheitsorganisation. Sie dient dazu, die Anforderungen des Nutzerkreises an ein risikogerechtes Sicherheitskonzept abzubilden. Sie beinhaltet Aussagen zu den Zielen, Strategien, Verantwortungsbereichen und

Entscheidungskriterien für die Informationssicherheitsmaßnahmen des Virtual Fort Knox. Die Sicherheitsrichtlinie ist ebenso als langfristige Strategie zu sehen, die die Art und Weise beschreibt, wie Sicherheit in der Plattform Community des Virtual Fort Knox verstanden wird. Sie muss so gestaltet werden, dass sie sich dynamisch an sich ändernde Bedrohungslagen und Anforderungen an den Schutzbedarf von Informationen anpassen lässt. Es sollte stets das Ziel sein, Angriffsflächen von vornherein zu minimieren oder gar nicht erst zu bieten. Dabei gilt es in regelmäßigen Zyklen zu evaluieren, ob die Informationssicherheitsrichtlinie den Schutzbedarfsanforderungen gerecht wird.
Der Anbieter der VFK-Plattform implementiert vollständig die Sicherheitsrichtlinie für die Kollaboration. Kunden sowie Dienstleister bzw. Anwendungsanbieter entscheiden selbst über die Adaption dieser Richtlinie oder die eigenständige Schaffung eines zu dieser Richtlinie kongruenten Sicherheitsansatzes. Die Nachprüfbarkeit der Compliance wird über transparente Sicherheitsstandards (teilweise auch marktüblich: ISO 2700x, BSI 100- x) gewährleistet.

2.4.4 Wer bezahlt's? Geschäftsmodelle für eine digitale Industrie-Infrastruktur

Industrie 4.0 im Allgemeinen und VFK im Speziellen basieren auf dem Gedanken einer gemeinsamen digitalen Plattform, die Leistungen für die teilnehmenden Unternehmen bereitstellt, die diese selber so nicht erbringen könnten. Entscheidend für die Umsetzung einer solchen Plattform ist die Frage, welche Geschäftsmodelle damit verbunden sind: Wer bezahlt welche Leistung?

Vor diesem Hintergrund entwickelte Henning ein Geschäftsmodell, das dem besonderen Gedanken der Kooperation durch die Einführung einer verbindenden Vision Rechnung trägt.[8] Im Rahmen der Nutzung der Plattform wird zwischen unterschiedlichen Rollen differenziert, die verschiedene Interessen und Strategien bei der Nutzung der Plattform verfolgen:

- **IT- und Basisdienste-Lieferant:** Stellt für die Plattform technische Services zur Verfügung (zum Beispiel Data-Center, Infrastructure), kann die Lieferung einzelner Leistungen oder den Betrieb der gesamten Plattform umfassen.
- **Plattformbetreiber:** Stellt die Plattform bereit und ermöglicht den Dienst- und Anwendungsanbietern, über die Plattform ihre Leistungen dem Kunden zur Verfügung zu stellen.
- **Dienste- und Softwareanbieter:** Bieten dem Kunden Dienste und Software an sowie aggregierte Dienste, die mehrere Dienste zu einem zusammenfassen.
- **Kunde:** Der Kunde ist ein Unternehmen, das auf der Plattform angebotene Dienste nutzt und dafür sorgt, dass die Anwender und eventuell Maschinen Zugriff auf die Dienste der Plattform bekommen.

Das Geschäftsmodellframework untergliedert sich in die folgenden Kategorien: Partner, Wertschöpfung, Angebot, Kundenbeziehung, Nutzenbeschreibung, Kanäle, Kultur und

Werte, Vision, Zielkunden sowie Kosten und Erlöse. Diese einzelnen Kategorien stehen rollenübergreifend in Beziehung zueinander und beeinflussen in ihrer Gesamtheit Kosten und Erlöse der Kunden, Dienste- und Softwareanbieter, des Plattformbetreibers und der IT- und Basisdienste-Lieferanten. Das folgende Szenario soll die Komplexität verdeutlichen: Ein Möbelhersteller will mithilfe der VFK-Plattform den Dienst eines Produktions-Planungs-Systems des Softwareanbieters A zu Steuerung und Optimierung seiner Produktionslinie einsetzen. Gleichzeitig nutzt er die Software des Anbieters B, um die Auslastung und Effizienz seiner Produktionslinie zu messen. Dank der Plattform können nun die Dienste der beiden Anbieter A und B als gemeinsame Leistung zusammengefasst werden. Nehmen wir an, Anbieter C möchte diesen neuen Dienst anbieten. Das Interesse des Möbelherstellers im Sinne eines optimalen Nutzens ist die direkte Bindung der Kosten für den aggregierten Dienst an die Stückzahl der produzierten Möbel. Er wird also pro Stück einen festen Betrag zahlen. Der Anbieter C akzeptiert das Modell, zahlt selber aber an die Softwareanbieter A und B für die Nutzung der Software (as a Service). Der Plattformbetreiber berechnet A und B die Nutzung von Rechnerkapazitäten und die Bereitstellung der Sicherheitsinfrastruktur, deren Preis zum Beispiel über die Anzahl der angeforderten Verbindungen zur Plattform ermittelt wird.

Anhand der Preisgestaltung auf den unterschiedlichen Ebenen der Beteiligten wird deutlich, dass die einzelnen Geschäftsmodelle abgestimmt werden müssen. Sobald Kosten und Erlöse aufeinander abgestimmt werden, beeinflussen sich Angebot, Wertschöpfung und Nutzen in den unterschiedlen Modellen gegenseitig. Aspekte wie Kultur und Werte sollten für alle möglichst ähnlich formuliert werden. Gerade hier hilft die Formulierung der gemeinsamen Vision.

Mit einem ebenfalls von Henning entwickelten Bewertungsmodell lassen sich nun Geschäftsmodellvarianten analysieren, um die Stärken und Schwächen sowie die Chancen und Risiken jeder Variante zu bestimmen. Das Bewertungsmodell ist eine Kombination der PEST(LE)-Analyse, der SWOT-Analyse, der Szenario-Technik, der Balanced Score Card und den Verfahren der Wirtschaftlichkeitsberechnung, dem ROI, dem Zukunftserfolgswert und der Amortisationsdauer. Die Entscheidung für oder gegen die Umsetzung einer Geschäftsmodellvariante wird durch die Kooperation und deren Beteiligte getroffen. Dabei dient das Bewertungsmodell als Entscheidungsunterstützung.
Die im vorherigen Abschnitt beschriebenen Kernelemente des VFK zur Erreichung der Akzeptanz greifen auch bei der Erstellung und Bewertung der Geschäftsmodelle. Transparenz und Kommunikation sind im Erstellungsprozess notwendig; über das Geschäftsmodell wird der Nutzen definiert. Letztlich führt das Vertrauen in das gemeinsam entwickelte Geschäftsmodell zur Akzeptanz.

2.4.5 Ausblick

Die bisher erreichten Ergebnisse des Forschungsprojekts sind ermutigend, insbesondere da es gelungen ist, exemplarisch die horizontale Integration über Wertschöpfungsnetzwerke zu demonstrieren. Die kurze Dauer der Förderung von sechs Monaten zwang allerdings dazu, sich auf die wesentlichen Aspekte zu konzentrieren und innovativ bisher

verfügbare Technologie und Forschungsergebnisse schnell umzusetzen. Auch die kommerzielle Umsetzung ist angedacht; gemeinsam mit dem IPA und weiteren Partnern wird zurzeit an der Bereitstellung einer kommerziell nutzbaren Plattform gearbeitet. Sie soll dann speziell den mittelständischen Unternehmen den Einstieg in das Thema Industrie 4.0 ermöglichen mit dem Ziel, die Wettbewerbsfähigkeit des deutschen Maschinen- und Anlagenbaus weiter zu stärken. Das Land Baden-Württemberg bezeichnet dieses Projekt zu Recht als Pilotprojekt.

Gerade im Kontext von Industrie 4.0, bei dem es darum geht, die führende Wettbewerbsfähigkeit des Maschinen- und Anlagenbaus zu erhalten, kommt es auf Schnelligkeit an. Der Ansatz der zeitlich beschränkten Förderung mit dann aber entsprechend hohen Fördersummen könnte gerade auf weitere im Umsetzungsbericht Industrie 4.0 geforderten Leuchtturmprojekte angewendet werden.[9] Hier müsste die gängige Förderpolitik der Ministerien in Bund und Ländern überdacht werden, auch im Sinne einer besseren Differenzierung zwischen Forschungs- und Innovationsförderung – ein Thema, das sicher auch die Arbeitsgruppen und der Lenkungsausschuss von Industrie 4.0 aufgreifen sollten. Der BITKOM mit seiner Zuständigkeit für IT könnte wesentlich auf die Förderung von Pilot-Plattformen hinwirken, die mit dem VFK vergleichbar sind.

Die bisher erreichten Ergebnisse lassen sich gut auf andere Marktsegmente transferieren. So ist zum Beispiel eine Nutzung der Methoden des VFK im öffentlichen Sektor denkbar. Das Modell der Öffentlich Privaten Partnerschaften (ÖPP) kann genutzt werden, um VFK-Plattformen zu finanzieren, die dann Kommunen, Ländern und dem Bund Fachverfahren (wie zum Beispiel Kfz-Anmeldung) zur Verfügung zu stellen.

1 Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0.

2 Vgl. R. Ko/P. Jagadpramana / M. Mowbray / S. Pearson/ M. Kirchberg/ Q. Liang/ B. Lee (2011): Trust-Cloud. A Framework for Accountability and Trust in Cloud Computing. Singapur, Bristol. HP Laboratories.

3 Bundesamt für Sicherheit in der Informationstechnik (2012): Eckpunktepapier Sicherheitsempfehlungen für Cloud-Computing-Anbieter. Bonn. S. 24.

4 M. Schweer (2012). Vertrauen als Organisationsprinzip in interorganisationalen Kooperationen. IN: C. Schilcher (Hg.), Vertrauen und Kooperation in der Arbeitswelt. Wiesbaden.

5 Siehe auch M. Rapp (2012). Konzepte zur Vertrauensbildung in föderative IKT-Plattformen für den mittelständischen Maschinen- und Anlagenbau. Master-Thesis. Berlin.

6 Bundesamt für Sicherheit in der Informationstechnik (2012): Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter. Bonn.

7 M. Rapp (2012). Konzepte zur Vertrauensbildung in föderative IKT-Plattformen für den mittelständischen Maschinen- und Anlagenbau. Master-Thesis. Berlin.

8 J. Henning (2012) Kollaboration in der Cloud: Modell zur Bewertung des Einsatzes von Community.

9 Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. (Kapitel 5)