Zentrum für digitale Innovationen Niedersachsen

# Detaillierte Ergebnisse – Teilprojekt

## IT-Infrastruktur und Sicherheit

## ZIEL DER DATENPLATTFORM UND NUTZUNGSSZENARIO

**FORSCHUNGSINTERESSE:**

- Wie können Produktionsdaten standort- und unternehmensübergreifend ausgetauscht werden?
- Welches Nutzungsszenario ist realistisch und kann als Grundlage der Forschung dienen?

**VORGEHEN**:

- Die Wissenschaftler*innen entwickelten eine IT-Architektur für eine Datenplattform.
- Die Wissenschaftler*innen bestimmten ein Szenario, welches sie für die Anwendung der Datenplattform zugrunde legen.

**ERGEBNISSE/ERKENNTNISSE:**

- Die Datenplattform ermöglicht eine verteilte Dateninfrastruktur, ohne direkte Verknüpfung der Datenquellen. Das bedeutet, dass die Unternehmen ihre Daten für Analysen bereitstellen, ohne dass Dritte die Daten einsehen können. Details werden im Weiteren vorgestellt.
- Das Nutzungsszenario beinhaltet die gemeinschaftliche Analyse von Daten aus dem Werkzeugbau und der Fertigung im Druckguss. Hierbei geht es darum herauszufinden, weshalb manche Bauteile nicht der gewünschten Qualität entsprechen. Auf Basis der Daten soll eine Prognose erstellt werden, ob die mangelhafte Qualität aufgrund eines Werkzeugfehlers entstanden ist, oder ob andere Ursachen verantwortlich sind. Mithilfe der Datenplattform wollen die Wissenschaftler*innen auch ermitteln, wie wahrscheinlich es ist, dass das Gießwerkzeug während des Gießprozesses ausfällt.

## ZIELGRUPPEN DER DATENPLATTFORM UND ANFORDERUNGSANALYSE

**FORSCHUNGSINTERESSE**:

- Welche Stakeholder haben Interesse an der Datenplattform?
- Welche Anforderungen stellen diese Stakeholder an die Plattform?
- Welche Kriterien hinsichtlich Nutzung, Datenschutz und IT-Sicherheit muss die Plattform erfüllen?

**VORGEHEN**:

- Zunächst erstellten die Wissenschaftler*innen Profile (sogenannte Personae) Rollen innerhalb der Produktionskette (z.B. Qualitätssicherung, Maschinenführung, IT-Administration).
- Auf Basis der Personae fassten die Wissenschaftler*innen die Bedürfnisse in User Stories zusammen und leiteten daraus ab, welche Eigenschaften die zu entwerfende IT-Infrastruktur aus Sicht der jeweiligen Person aufweisen muss (z. B. „Als IT-Administrator*in in der Produktion möchte ich, dass die Verfügbarkeit der Daten im Produktionsbereich stets gewährleistet ist, um die Produktion aufrecht zu erhalten.“).
- Daraufhin definierten die Wissenschaftler*innen Geschäftsanforderungen, Nutzungsanforderungen, Betreiberanforderungen, Schutzziele und IT-Sicherheitsanforderungen für die Datenplattform.
- Des Weiteren identifizierten sie vier Anwendungsfälle, in denen die Datenplattform zum Einsatz kommen kann. Dazu zählen die Kommunikation im Produktionsbereich, die Übertragung der Daten in interne Verwaltungsabteilungen, die Speicherung der Daten in unternehmenseigenen Clouds und die Übermittlung der Daten in firmenexterne „Shared-Clouds“.
- Schließlich formulierten die Wissenschaftler*innen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nichtabstreitbarkeit) und Anforderungen aus Perspektive der IT-Sicherheit (Identifizierung und Authentifizierung, Nutzungskontrolle, Systemintegrität, Vertraulichkeit der Daten, Eingeschränkter Datenfluss, Rechtzeitige Reaktion auf Ereignisse, Verfügbarkeit der Ressourcen).

**ERGEBNISSE/ERKENNTNISSE:**

- Die Wissenschaftler*innen definierten die Zielgruppen und deren Ansprüche an die Plattform.
- Zudem legten sie Anforderungen hinsichtlich Nutzung, Datenschutz und IT-Sicherheit fest.
- Indem sie vier Anwendungsfälle der Plattform identifizierten, wurden die Einsatzmöglichkeiten deutlich.
- Außerdem steht fest, welche Schutzziele und Anforderungen die Plattform aus Sicht der IT-Sicherheit erfüllen muss.

## ÜBERLEGUNGEN ZUR IT-SICHERHEIT UND ZU RECHTLICHEN ANFORDERUNGEN

**FORSCHUNGSINTERESSE**:

Wie kann die Datenplattform vor unberechtigten Zugriffen geschützt werden?

**VORGEHEN**:

- Die Wissenschaftler*innen prüften gängige Datenplattformen hinsichtlich der IT-Sicherheitsaspekte, die sie als essenziell identifiziert hatten (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nichtabstreitbarkeit).
- Zudem entwickelten sie abhängig vom Anwendungsfall entsprechende IT-Sicherheitskonzepte. Beispielsweise muss bei sensiblen Datensätzen die Vertraulichkeit gewahrt werden, um Firmengeheimnisse zu schützen, während bei weniger sensiblen Datensätzen die Verfügbarkeit priorisiert werden könnte, um den Betrieb zu gewährleisten.
- Des Weiteren entwickelten die Wissenschaftler*innen ein Konzept, wie die Erkenntnisse zur IT-Sicherheit in die Workflows der Datenplattform integriert werden können. Zu den Workflows zählt z. B. die Daten der Druckgießmaschinen zu gewinnen und in die Plattform einzuspeisen, verschiedene Kommunikationsprotokolle der unterschiedlichen Anlagen zu kombinieren oder Sicherheitszertifikate auszutauschen.

- Darüber hinaus analysierten die Wissenschaftler*innen, welche juristischen Fragestellung in Bezug auf die Datensicherheit innerhalb der Produktion relevant sind. In einem Konzeptpapier stellten die Wissenschaftler*innen die Datenflüsse und die beteiligten Akteure dar. Dieses leiteten sie an einen juristischen Praxispartner weiter.

**ERGEBNISSE/ERKENNTNISSE:**

- Die Überprüfung gängiger Datenplattform ergab, dass keine der geprüften Plattformen alle erforderlichen Sicherheitsaspekte abdeckt.
- Die Auswahl und Entwicklung der IT-Sicherheitskonzepte wurden an die spezifischen Anforderungen der Anwendungsfälle angepasst.
- Es liegt ein Konzept vor, um die Sicherheitsanforderungen in die Workflows der Datenplattform zu integrieren.
- Zu den relevanten juristischen Fragestellungen zählen Dateneigentum, Datenschutz und vertragliche Situation der Beteiligten (Kund*innen, Werkzeugbau, Gießerei).
- Der juristische Praxispartner leitete aus dem Konzeptpapier rechtliche Anforderungen ab, z. B. welche Verträge geschlossen werden müssen.

## IT-SICHERHEIT GEMÄß GELTENDER INDUSTRIENORM

**FORSCHUNGSINTERESSE**:
Wie kann die IT-Sicherheit der Datenplattform umgesetzt werden?

**VORGEHEN**:

- Die Wissenschaftler*innen orientierten sich an der Industrienorm IEC62443-3-3, die die technischen Anforderungen an die Sicherheit von Systemen beschreibt. Sie überprüften, welche Anforderungen die Datenplattform gemäß der IEC62443-3-3-Norm erfüllen muss und definierten entsprechende Maßnahmen zur Umsetzung.
- Zudem führten sie eine Risikoanalyse durch, um zu testen, ob das Minimal-Viable-Produkt (MVP) den allgemeinen IT-Sicherheitskriterien entspricht, insbesondere im Hinblick auf unberechtigten Zugriff und Vertraulichkeit der Daten.

**ERGEBNISSE/ERKENNTNISSE:**

- Die Analyse der Industrienorm ergab, dass die Plattform etwa 50 sicherheitsrelevante Anforderungen erfüllen muss, darunter Identifizierung, Authentifizierung, Vertraulichkeit und Reaktionsfähigkeit auf Ereignisse.
- Durch die Risikoanalyse nach VDI/VDE 2182 - Blatt 1 konnten die Wissenschaftler*innen Schwachstellen erkennen und beheben.
- Die Nutzung von Thread Modeling Tools ergänzte die Risiko- Bedrohungsanalyse über den Entwicklungszeitraum kontinuierlich.

## BEDENKEN AUS UNTERNEHMERISCHER SICHT ENTGEGENWIRKEN

**FORSCHUNGSINTERESSE**:

- Welche Bedenken haben Unternehmen bezüglich Datensicherheit und Eigentum?
- Wie können diese Bedenken überwunden werden, um von den Vorteilen des Datenaustausches zu profitieren?

**VORGEHEN**:

- Die Wissenschaftler*innen führten Gespräche mit Praxispartnern hinsichtlich ihrer Bedenken, Unternehmensdaten über eine Datenplattform zu teilen.
- Im Rahmen einer Literaturrecherche untersuchten die Wissenschaftler*innen des Zukunftslabors Produktion eine Vielzahl von Studien im Hinblick auf Konzepte, die eine unternehmensübergreifende Datennutzung entlang der Lieferkette ermöglichen.

**ERGEBNISSE/ERKENNTNISSE:**

- Aus den Gesprächen mit den Praxispartnern wurde deutlich, dass sie Sorge vor einer Veränderung der Machtverhältnisse innerhalb der jeweiligen Lieferkette, vor Datendiebstahl und vor dem Verlust geistigen Eigentums an Wettbewerber*innen haben. Außerdem fehlt zum Teil das Fachwissen innerhalb der Betriebe, die Produktionsdaten auszuwerten und Optimierungsmaßnahmen abzuleiten.
- Die Literaturrecherche ergab, dass die bisher existierenden Konzepte und Architekturen nicht alle Anforderungen der KMU erfüllen. Zu diesen Anforderungen gehört vor allem, dass die Datensicherheit gegenüber Dritten und die Dateneigentumsinteressen gegenüber anderen Teilnehmern der Lieferkette ausreichend geschützt sind.
- Aus der Prüfung bisheriger Konzepte ging hervor, dass sie den Bedürfnissen der Unternehmen nicht ausreichend gerecht werden. Daher definierten die Wissenschaftler*innen für sich den Anspruch, den Prototyp der Datenplattform so zu gestalten, dass er die Anforderungen erfüllt.

## (TECHNISCHE) HERAUSFORDERUNGEN DES DATENAUSTAUSCHES

**FORSCHUNGSINTERESSE:**
Wie können Datenbestände aus unterschiedlichen Datenquellen ausgetauscht werden?

**VORGEHEN**:

- Die Wissenschaftler*innen stellten fest, dass die Unternehmen der Lieferkette unterschiedliche Anwendungssysteme mit unterschiedlichen Datenmodellen nutzen, die miteinander kommunizieren sollen. Dazu zählen Enterprise Resource Planning Systeme (ERP) - Planungssysteme von der Auftragserteilung über den Produktionsauftrag bis hin zur Rechnungserstellung - sowie Manufacturing Execution Systeme (MES) - Systeme zur Feinplanung der Fertigung, z. B. der Produktionslinie und der Maschinenbelegung. Die unterschiedlichen Datenmodelle erschweren den Datenaustausch über die Plattform.
- Daher entwickelten die Wissenschaftler*innen ein Konzept, das den Datenaustusch ermöglicht. Basierend auf diesem Konzept entwickelten die Wissenschaftler*innen einen Prototyp für den unternehmensübergreifenden Informationsaustausch. Um den Prototyp zu testen, verknüpften die Wissenschaftler*innen Daten von Verbundpartnern und assoziierten Partnern.
- Zudem programmierten die Wissenschaftler*innen eine Webapplication zur Verknüpfung der Datenbestände und entwickelten eine Unterstützungssoftware zur Integration von Datenbeständen.
- Darüber hinaus entwickelten die Wissenschaftler*innen Benutzeroberflächen für die Plattform und einfache Elemente wie ein Nutzerlogin oder das Backend für die Datenbank. In der Benutzeroberfläche werden auch die Beziehungen der Unternehmen entlang der Lieferkette visualisiert.

**ERGEBNISSE/ERKENNTNISSE:**

- Das Konzept sieht wie folgt aus: Zunächst müssen die Unternehmen die Austauschschnittstelle definieren, d. h. die Daten für den Austausch aufbereiten. Daraufhin können sich über die Datenplattform miteinander verbinden. Auf der Plattform ist ein Modell

der Lieferkette hinterlegt, wodurch die Beziehungen zwischen den Unternehmen abgebildet werden (Wer liefert was wann an wen?). Dadurch werden vor- und nachgelagerte Prozesse sichtbar. Die Unternehmen müssen keine sensiblen Daten wie z. B. Maschinendaten austauschen, sondern bereits bekannte Daten oder aus Rohdaten abgeleitete Informationen (z. B. Seriennummern oder Ergebnisse der Qualitätsanalyse). Die Serien- oder Chargennummern der ausgetauschten Waren werden verwendet, um die Datenelemente der Unternehmen zu verbinden. Sie dienen als Identifikatoren, um die Produkte innerhalb des unternehmensübergreifenden Workflows zu finden und zu verknüpfen.

- Die Unterstützungssoftware hilft dabei, die Datenpunkte innerhalb eines Unternehmens zu identifizieren und sie in eine Datenbank zu überführen, die zwischen der eigentlichen Datenquelle und der Datenplattform des Zukunftslabors Produktion geschaltet ist. Die Software unterstützt die Unternehmen also dabei, die eigenen Datenbestände aus den einzelnen Silos zusammenzuführen.
- Die Webapplication verknüpft die Datenquellen aller beteiligten Unternehmen entlang der Lieferkette. Über die Webapplication werden die realen Beziehungen der Unternehmen abgebildet, sodass die Verknüpfung der Beteiligten sichtbar wird. Damit werden die Unternehmen in die Lage versetzt, die Lieferkettenabhängigkeiten (Zulieferer/Kunde) mit den intern gelagerten Datenbeständen zu koppeln.

## DATENAUSWERTUNG MITTELS FEDERATED LEARNING

**FORSCHUNGSINTERESSE:**
Wie können die Daten unternehmensübergreifend ausgetauscht werden, sodass das geistige Eigentum der Unternehmen geschützt wird?

**VORGEHEN**:

- Die Wissenschaftler*innen entwickelten eine Connector-Funktion, die als zentrale Schnittstelle fungiert, über die Datenplattformen und externe Dienste wie Sicherheitszertifikate oder User-Logins aggregiert werden. Die Daten selbst werden nicht auf der Plattform gespeichert, sondern verbleiben auf den Servern der Unternehmen und sind über den Connector analysierbar.
- Um die Daten zu analysieren, entschieden sich die Wissenschaftler*innen für das Federated Learning. Dabei handelt es sich um eine Technik des Maschinellen Lernens, bei der nur Modelle und Parameter ausgetauscht werden, nicht die Daten selbst.
- Gemeinsam mit einer Rechtsanwaltkanzlei evaluierten die Wissenschaftler*innen den technischen Schutz der Daten und diskutierten Optionen, die Datensouveränität weiter zu verbessern.

**ERGEBNISSE/ERKENNTNISSE:**

- Das entwickelte Architekturmodell ermöglicht eine Datenanalyse, ohne dass sensible Daten offengelegt werden müssen und die Privatsphäre verletzt wird. Es schützt also die Datensouveränität der Unternehmen technisch, indem die Daten dezentral bleiben und nur Modelle aggregiert werden. Voraussetzung ist auch hier, dass die entsprechenden Sicherheits- und Datenschutzvorkehrungen eingestellt werden.
- Eine Option, die Datensouveränität aus rechtlicher Sicht noch weiter zu stärken, besteh darin, die Plattform durch einen unabhängigen Dritten bereitstellen zu lassen. Der Vorteil besteht darin, dass eine unabhängige Partei keinen Nutzen aus dem Missbrauch der Plattform ziehen würde und somit das Risiko einer Manipulation oder Ausnutzung von möglichen, aktuell noch unbekannten Schwachstellen reduziert wird.

## MINIMAL-VIABLE-PRODUKT (MVP)

**FORSCHUNGSINTERESSE**:
Sind die Funktionalität und Nutzbarkeit der Datenplattform anwendungsorientiert gestaltet?

**VORGEHEN**:
Die Wissenschaftler*innen erstellten sie ein Minimal-Viable-Produkt (MVP), eine funktionsfähige Testversion der Datenplattform zur Evaluation der Erfüllung der IT Security-Anforderungen. Das MVP diente zur Erprobung der Sicherheitsfeatures, zur Durchführung von Performance-Analysen und sicherheitskritischen Tests wie Penetrationstest.

**ERGEBNISSE/ERKENNTNISSE:**

- Auf Grundlage des Feedbacks nahmen die Wissenschaftler*innen Anpassungen an der Plattform vor.
- Ursprünglich verwendeten sie das Jade-Framework für die Verknüpfung der Analyse-Dienste. Die Tests zeigten, dass das Jade-Framework nicht mehr den aktuellen IT-Sicherheitsstandards entspricht. Deshalb wechselten die Wissenschaftler*innen auf das modernere Spring Boot Framework, das auf Microservices basiert. Das sind kleine, unabhängige Dienste, die über Schnittstellen miteinander kommunizieren. Durch den Wechsel zu Spring Boot und die Nutzung von Microservices konnte die Entwicklungszeit verkürzt, die Skalierbarkeit verbessert und die Markteinführungszeit neuer Funktionen reduziert werden. Für das finale MVP wurden letztendlich Container-basierte Services aus verschiedenen Software-Komponenten ausgewählt, um alle Funktionalitäten sicher und effizient zu realisieren.

## RISIKEN DURCH MENSCH UND TECHNIK

**FORSCHUNGSINTERESSE**:
Welche Risiken können hinsichtlich der Faktoren Mensch und Technik bei der Nutzung der Datenplattform entstehen?

**VORGEHEN**:

- Die Wissenschaftler*innen identifizierten Risiken, die durch Mensch und Technik entstehen können.
- Aus den Risiken leiteten sie Handlungsempfehlungen für Unternehmen ab.

**ERGEBNISSE/ERKENNTNISSE:**

- Zu den menschlich verursachten Risiken zählt, dass Mitarbeiter*innen Informationen an Unbefugte weitergeben und Daten falsch interpretieren, fälschen oder missbrauchen. Zudem können sich Hacker Zugang zum System verschaffen und mit falschen Anfragen Informationen über die Unternehmen gewinnen. Zu den technisch bedingten Risiken zählt, dass die Datenbanken miteinander verbunden und Datenströme zusammengeführt werden müssen. Das kann zu Datendiebstahl, Datenlecks, fehlerhaften Daten und fehlerhaften Schlussfolgerungen führen.
- Unternehmen müssen sich der Risiken bewusst sein und entsprechende Maßnahmen ableiten. Dazu zählt, die Cybersicherheit zu verbessern, die Produktionsumgebung abzusichern und Zugriffsrechte für Mitarbeiter*innen festzulegen. Zudem sollte der Shopfloor – also der Maschinenpark – vom restlichen Firmennetz getrennt werden. Die Daten dieser Anlagen sollten zur Sicherheit nur über ein sicheres Verbindungsgerät in die Datenplattform eingebracht werden.

# DEMONSTRATORS ZUR DARSTELLUNG DER LIEFERKETTE

**FORSCHUNGSINTERESSE**:
Wie kann die Vernetzung der Produktion anschaulich dargestellt werden?

**VORGEHEN**:

- Die Wissenschaftler*innen arbeiten an einem Demonstrator, der die Vernetzung der Lieferkette abbildet.
- Auf einer transportierbaren Holzplatte wird eine Miniaturfabrik dargestellt, die eine CNC-Fräse enthält. Über eine Eisenbahn wird ein Holzstück in die Fabrik geliefert, das dort graviert wird. Die Eisenbahn erfasst dabei Daten zur Auslastung und Geschwindigkeit. Ein Scanner digitalisiert die Kontaktinformationen einer haptischen Visitenkarte, die in eine virtuelle Visitenkarte umgewandelt und auf einen Chip im Holzstück übertragen wird. Diese Daten können anschließend über ein Lesegerät ausgelesen werden, ähnlich wie bei einer Bankkarte.

**ERGEBNISSE/ERKENNTNISSE:**

- Der Demonstrator stellt verschiedene Prozessschritte dar, wie z. B. Transport, Verarbeitung und Datenerfassung. Er veranschaulicht auf einfache Weise eine Lieferkette, an der mehrere Unternehmen beteiligt sind.
- Der Demonstrator kann kontinuierlich erweitert werden, um weitere Forschungsergebnisse zu veranschaulichen
- Der Demonstrator kann auf Messen und Veranstaltungen eingesetzt werden, um Interessent*innen einen anschaulichen Einblick in die Forschung zu geben.