

Cyber-Sicherheit in vernetzten Lieferketten

Jonas Kallisch, Marvin Voss, Maxim Runge, Christoph Wunck, Karl-Heinz Niemann

Suggested citation:

Kallisch, Jonas, Marvin Voss, Maxim Runge, Christoph Wunck, and Karl-Heinz Niemann. 2025. "Cyber-Sicherheit in vernetzten Lieferketten." *Giesserei - Die Zeitschrift für Technik, Innovation und Management* 112 (4): 28–32. <https://doi.org/10.25968/opus-3594>.

Abstract

Mit zunehmender Komplexität der Lieferketten durch Globalisierung und Entwicklung der Technologie steigt auch die Notwendigkeit des Austausches von Informationen zwischen kooperierenden, aber unabhängigen Unternehmen. Dabei stehen sie vor der Herausforderung, eine Balance zwischen der erforderlichen Transparenz zur übergreifenden Optimierung der Lieferkette und dem Schutz sensibler Daten aus ihren Produktionssystemen zu finden. Angesichts zunehmender Bedrohungen durch Cyberkriminalität, von gezielten Angriffen auf Produktionssysteme bis hin zum Datendiebstahl geistigen Eigentums, ist der Schutz digitaler Infrastrukturen für Unternehmen unverzichtbar. Im Rahmen des Teilprojekts „IT-Infrastruktur und IT-Sicherheit“ hat das Zukunftslabor Produktion den Prototyp einer Unterstützungsplattform für einen unternehmensübergreifenden Datenaustausch unter Bewahrung von Datensouveränität entwickelt und zusammen mit Praxispartnern evaluiert. Ihre Funktionsweise wird in diesem Beitrag erläutert, der den vierten und letzten einer Serie bildet, in der die Projektpartner jeweils ihre Teilergebnisse vorstellen.

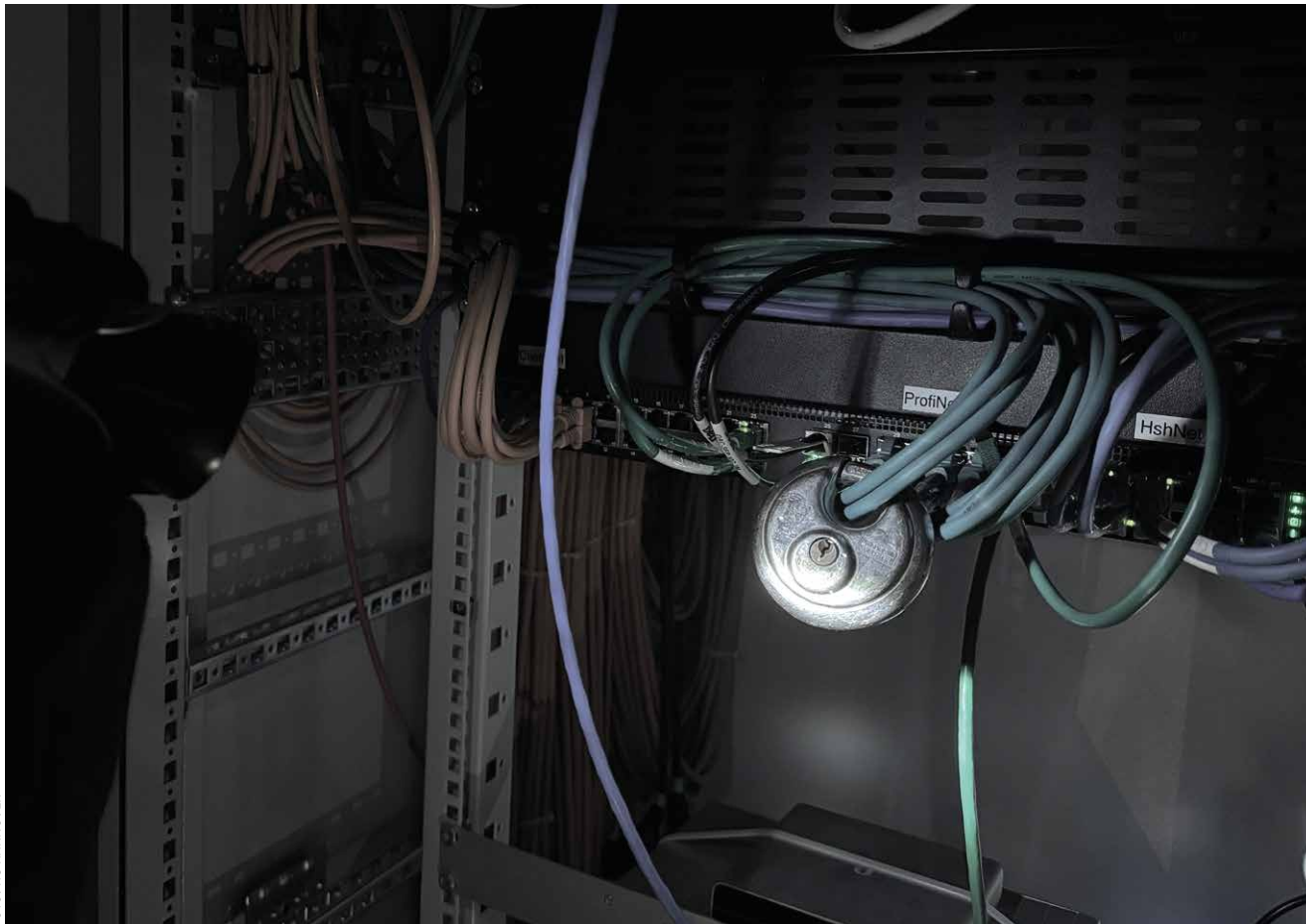


FOTO: HS HANNOVER

Digitalisierung im Brownfield

Cyber-Sicherheit in vernetzten Lieferketten, Teil 4 von 4

Föderiertes Netzwerk unter Verschluss.

VON JONAS KALLISCH, MARVIN VOSS, MAXIM RUNGE, CHRISTOPH WUNCK, KARL-HEINZ NIEMANN

Das Personal einer Gießerei verfügt über ein umfangreiches Wissen und wertvolle Erfahrungen im Umgang mit den eingesetzten Maschinen und Werkzeugen. Diese Kenntnisse sind essenziell für den Erfolg des Unternehmens. Mit einem „scharfen Blick“ oder anhand charakteristischer Geräusche der Maschine erkennt das erfahrene Personal zuverlässig den Zustand der Anlagen und des Produktionssystems. Aber auch dieses Personal bewegt sich nur in einem kleinen Teil der Produktionskette und überblickt nur seinen eigenen Aufgabenbereich. Für eine effizientere und zuverlässigere Pro-

duktion ist man auch auf Informationen aus vor- und nachgelagerten Prozessstufen angewiesen. Technisch unzureichend gestaltete Datenplattformen stellen dabei nicht nur ein Sicherheitsrisiko dar, sondern können auch das Vertrauen zwischen Partnern in der Lieferkette negativ beeinflussen. Die Entwicklung einer sicheren und gleichzeitig nutzerfreundlichen Infrastruktur ist daher eine zentrale Herausforderung.

Gefahren und Mehrwerte vernetzter Lieferketten

Unternehmensübergreifender Datenaustausch stellt eine technische sowie organisatorische Herausforderung dar. Einerseits muss dabei die Architektur der di-

versen Produktions- und IT-Systeme berücksichtigt werden, die in der Regel über lange Zeiträume gewachsen sind und unterschiedliche Technologien einsetzen. Andererseits müssen auch die verschiedenen informationsbezogenen Anforderungen der jeweiligen Unternehmen und Personen im unternehmensübergreifenden Fertigungssystem berücksichtigt werden.

Technisch gesehen existieren verschiedene Möglichkeiten zum Austausch von Daten zwischen unabhängigen Akteuren. Die bestehenden Ansätze eines Datenökosystems oder eines Datentreuhänders bieten jedoch keine Möglichkeit, sensible Daten aus den Produktionssystemen zu schützen. Der Grund dafür ist, dass die Modelle dieser Ökosysteme die

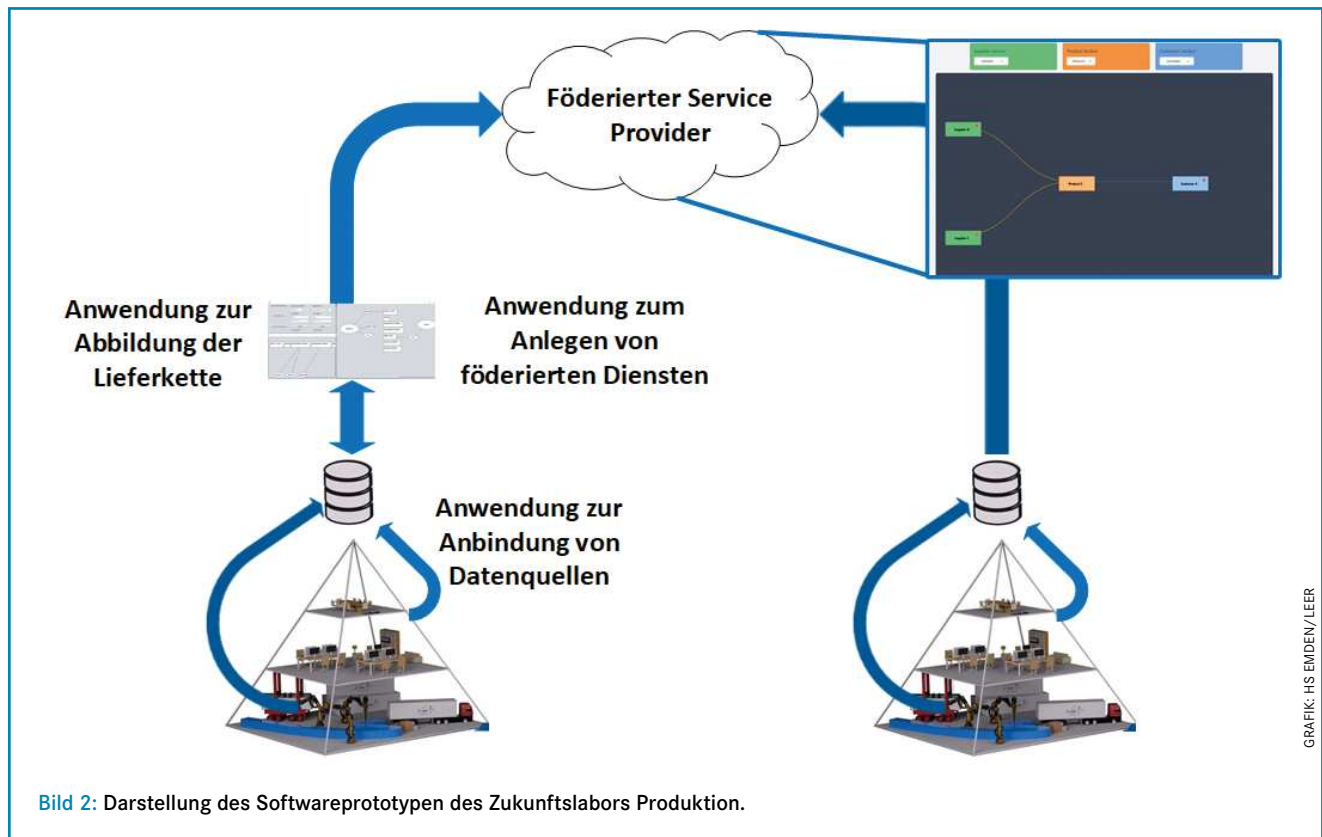


Bild 2: Darstellung des Softwareprototypen des Zukunftslabors Produktion.

GRAFIK: HS EMDEN/LEER

Vertikales föderiertes Lernen kann hingegen eingesetzt werden, um die Ursachen von Produktionsausfällen zu identifizieren. In diesem Fall ermöglichen Modellvergleiche die Erweiterung der Datenbasis durch die Einbeziehung der Datenmodelle von Zulieferern. Durch die Kombination können Optimierungen erzielt werden, die die Wettbewerbsfähigkeit der gesamten Lieferkette steigern.

Im Rahmen des Zukunftslabors Produktion wurden vor allem Verfahren des vertikalen föderierten Lernens eingesetzt, bei denen verschiedene Datenmerkmale desselben Herstellungsprozesses analysiert wurden. So konnten Zusammenhänge zwischen Maschinenparametern, Qualitätskontrolldaten und Produktionsprozessen sicher aufgedeckt werden, ohne sensible Daten preiszugeben. Um die Verfahren anwenden zu können, wurde zunächst ein technischer Prototyp einer dezentralen Datenplattform entwickelt, die aus einer Container-basierten Architektur mit drei Ebenen besteht. Diese Schichten erfüllen folgende Funktionen:

- > Die Datenintegrations-Schicht fasst verschiedene Datenquellen wie Produktions- und Sensordaten aus der Fertigung eines Unternehmens zusammen und bereitet sie für Analysen vor. Sie benutzt einen Message-Broker (Kafka-Connect), der einen einheitlichen Datenstrom bereitstellt und die Verbindung zu den di-

versetzten Quellen von Produktionsmaschinen ermöglicht.

- > Die Datenmanagement-Schicht organisiert und strukturiert Daten. Sie ist die Grundlage für Analyseverfahren. Diese Schicht besteht aus einer Edge-Datenplattform, die vom jeweiligen Unternehmen verwaltet wird, und einem Workflow-Connector. Dieser stellt die Beziehungen zwischen den Teilnehmern einer Lieferkette dar und ermöglicht so eine unternehmensübergreifende Analyse. Für die Edge-Datenplattform wurde das NoSQL-Datenbankmanagementsystem Hadoop gewählt, um eine möglichst breite Anbindbarkeit aufgrund der unterschiedlichsten Datentypen zu ermöglichen. Es bietet eine gute Grundlage für Analysemodelle und ein bewährtes Ökosystem.

- > In der Analytik-Schicht kommt das föderierte Lernen zum Einsatz. Die Schicht besteht aus einer Definitionsebene auf dem Server, in der die Analysebedürfnisse und Strategien zur Datenanalyse festgelegt werden, und einer Client-Ebene, die die Analysemodelle auf Basis von Datenanalysen vor Ort bereitstellt. Zur Umsetzung wurde das Framework-Tool „Flower“ genutzt, das sich leicht integrieren lässt und bei vielen anderen Projekten auch eingesetzt wird. Das Framework-Tool befindet sich zum Zeitpunkt dieser Veröffentlichung jedoch noch in der kontinuierlichen Weiterentwicklung und ist bisher noch nicht als Produkt uneingeschränkt nutzbar.

Zusammengefasst bietet der in Bild 2 dargestellte Prototyp eine Lösung für die Herausforderungen des unternehmensübergreifenden Datenaustauschs. Dies konnte in mehreren Datenanalysen und Fallstudien nachgewiesen werden. Die entwickelten Softwarekomponenten können bei den Autoren bezogen werden.

Lieferkettenintegration und Ergebnisse der Testanwendung

Um das entwickelte Konzept zu evaluieren, wurden Sensordaten eines Anwendungspartners aus der Gießereibranche in den Prototypen aufgenommen. Diese wurden zunächst mit Unterstützung der TU Braunschweig und des Forschungszentrums L3S in Hannover analysiert und anschließend für die Analyse im Rahmen des föderierten Lernens aufgeteilt und mithilfe des Prototyps analysiert.

Die Ergebnisse zeigten den Mehrwert des föderierten Lernens in verschiedenen Analysemodellen. Die Genauigkeitsabweichung zwischen dem vertikal basierten Prognosemodell und dem zentralen, vollständig aggregierten Datenanalyseverfahren betrug etwa 15 %. Trotz dieses deutlichen Unterschieds war es für das Modell möglich, charakteristische Prozessfehler wie Kaltlauf und Blasenbildung bei einem Aluminium-Druckgießprozess eindeutig vorherzusagen. Je nach Sensitivität der zu analysierenden Daten empfiehlt es sich zu prüfen, ob für den Fall

nicht doch eine gezielte und kontrollierte Weitergabe von Rohdaten zur Verbesserung der Ergebnisse sinnvoll ist, um nicht höhere Genauigkeitsabweichungen als 15 % in Kauf zu nehmen. Dabei ist sicherzustellen, dass die Datenhoheit gewahrt bleibt und geeignete Sicherheitsmaßnahmen zum Schutz sensibler Informationen getroffen werden.

Der Prototyp wurde im Rahmen des Verbundprojekts an Daten der Technischen Universität Braunschweig, der Universität Hannover und der Leuphana Universität Lüneburg überprüft. Die Ergebnisse dieser Kontrollstudien dienen zur Überprüfung und es wurde getestet, wie einfach das Konzept in Datenökosysteme einbindbar ist. Die Ergebnisse der Fallstudien wurden in vier wissenschaftlichen Arbeiten veröffentlicht. Außerdem sind sie in Artikeln auf der Website des Zentrums für digitale Innovationen Niedersachsen (ZDIN) zusammengefasst.

Sicherheitsaspekt als Rückgrat der Plattform

Das föderierte Lernen ist eine Schlüsseltechnologie zur Wahrung der Datensouveränität und zum Schutz der Vertraulichkeit sensibler Informationen. Diese technische Methode allein kann jedoch nicht alle relevanten Schutzziele abdecken. Um diese Lücken zu schließen, wurden im Teilprojekt IT-Sicherheit Lösungen entwickelt, die das technische Konzept des unternehmensübergreifenden föderierten Lernens in dieser Hinsicht sinnvoll ergänzen.

Sicherheitsnormen

Um die Sicherheit der entwickelten Datenplattform ganzheitlich zu erreichen, wurde die Norm IEC 62443 3-3 für Sicherheitsanforderungen technischer Systeme für eine grundlegende Datenplattformarchitektur umgesetzt und getestet. Das erweiterte Sicherheitskonzept der entwickelten Datenplattform basiert auf einer umfassenden Bedrohungsanalyse nach VDI/VDE 2182 - Blatt 1. Durch die Anwendung dieser Richtlinie werden potenzielle Risiken systematisch aufgedeckt und Schwachstellen in allen Komponenten der Datenplattform identifiziert und bewertet. Die Analyse schafft eine klare Grundlage für die gezielte Auswahl geeigneter Schutzmaßnahmen. Der Prozess beginnt dabei mit der Erfassung aller Komponenten und Assets, gefolgt von der Analyse möglicher Bedrohungsszenarien, der Zuordnung zu Schutzzielen, der Risikobewertung, der Auswahl und Umsetzung geeigneter Maßnahmen sowie der

Tabelle 1: Vereinfachter Ausschnitt der durchgeführten Risikoanalyse nach VDI/VDE 2182-Blatt 1

Bedrohung	Schutzziel(e)	Risikoeinschätzung	Maßnahmen
Systemausfall durch (D)DoS	Verfügbarkeit	Mittel	(D)DoS-Schutzdienste wie Cloudflare oder Lastverteilung einsetzen
Verlust der Datenhoheit durch Lokalisierung externer VPN-Server	Integrität, Vertraulichkeit	Mittel bis hoch	Anpassung der Systemarchitektur durch Umverteilung der Kommunikationswege zwischen den Containern
Eindringen in das System durch Angreifer / Man-in-the-Middle	Verfügbarkeit, Integrität, Authentizität	Niedrig	VPN bietet bereits Schutz; Zusätzliche Überwachung (IDS) prüft Netzwerkaktivitäten auf Anomalien, zusätzliche Komponentenauthentifizierung
SQL-Injection	Verfügbarkeit, Integrität, Vertraulichkeit	Mittel	Eingabevalidierung, Einschränkung der Datenbankrechte auf ein Minimum, regelmäßige Updates
Root-Manipulationen	Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität	Mittel bis hoch	Nur eingeschränkte Benutzerrechte verwenden

abschließenden Validierung (Bild 3). Dabei wird der gesamte Lebenszyklus der Anlage berücksichtigt und der Prozess iterativ wiederholt.

Die Richtlinie ist speziell auf die Anforderungen von Produktionssystemen ausgerichtet und enthält neben der Vorgehensbeschreibung auch Vorgaben in Bezug auf die Dokumentation. Der praxisnahe Ansatz der Richtlinie hat sich für die dynamische Umsetzung in unserem Forschungsprojekt als sehr hilfreich erwiesen. Dies war besonders wertvoll, da die technischen Mittel im Unterprojekt IT-Infrastruktur aufgrund des sich ändernden Forschungsstandes häufig angepasst werden mussten. Ein beispielhafter Auszug typischer Risiken und entsprechender Gegenmaßnahmen für dieses Szenario zeigt Tabelle 1 mit verschiedenen Bedrohungsszenarien wie (D)DOS-Angriffe, SQL-Injections und Root-Manipulationen. Als Gegenmaßnahmen werden beispielhaft konfigurierte Benutzereinschränkungen, Eingabevalidierung, Anpassungen der Systemarchitektur und VPN-basierte Sicherheitsprotokolle vorgeschlagen. Besonders kritisch sind Risiken hinsichtlich

der Integrität und Vertraulichkeit von Diensten. Diese konnten im Projekt durch Zugriffsbeschränkungen und Anpassungen der Systemarchitektur minimiert werden. Die Tabelle stellt einen wesentlichen Aspekt der Sicherheitsstrategie bei der Entwicklung der Datenplattform dar, um Systemausfälle und Datenverlust von vornherein zu vermeiden.

Ergänzend zu dieser strukturierten Bewertung wurde die IEC 62443-3-3 Norm angewendet, um eine standardisierte Anforderungsanalyse für IT- und OT-Sicherheitsmaßnahmen in Bezug auf technische Systeme durchzuführen. Damit wird sichergestellt, dass sowohl branchenspezifische als auch regulatorische Anforderungen erfüllt werden.

Datenarchitektur

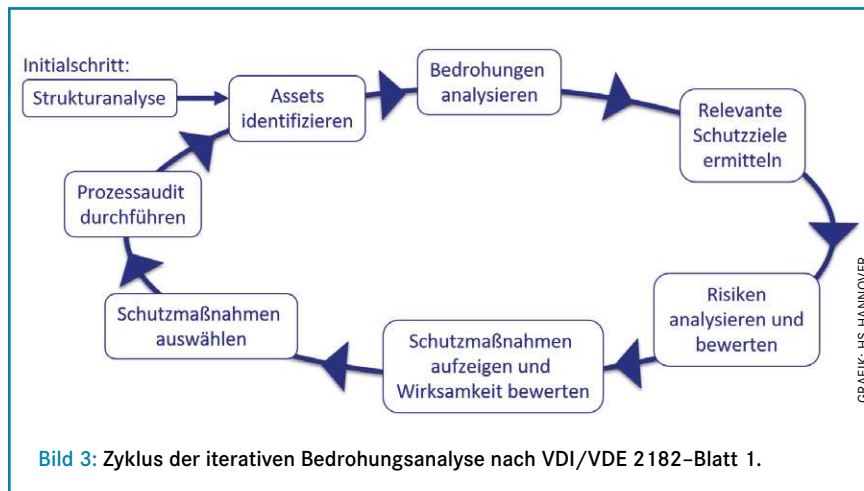
Auch die weiter vorne beschriebene Architektur (s. Bild 2) leistet einen Beitrag zur Stärkung der Sicherheit. Der Supply-Chain-Connector, der als einziger autorisierter Kommunikationspunkt fungiert, überträgt die intransparenten Lernmodelle ausschließlich über VPN und somit verschlüsselt, um mögliche Rückschlüsse

Stampfschablonen • Einschmelzzyylinder



A. Fengler
Hermann Uhlmann
Maschinen- und
Waagenbau GmbH
Hasseröder Straße 6

38855 Wernigerode
Tel. 03943 / 632201
Fax. 03943 / 905685
www.fengler-uhlmann.de



scheidender Wettbewerbsfaktor. Die entwickelte Datenplattform demonstriert, wie die Digitalisierung in der Gießereibranche praxisnah und nachhaltig umgesetzt werden kann. Dies ist ein entscheidender Faktor für den Übergang zu einer vernetzten, zukunftsfähigen Produktionsweise, bei der insbesondere Effizienz und Vertrauen eine entscheidende Rolle spielen.

www.zdin.de/zukunftslabore/produktion
www.hs-emden-leer.de/prof-dr-christoph-wunck
<https://hs-h.de/isa>

Jonas Kallisch, Prof. Dr.-Ing. Christoph Wunck, Abteilung Elektrotechnik und Informatik, Fachbereich für Technik, Hochschule Emden/Leer; Marvin Voß, Maxim Runge, Prof. Dr. Karl-Heinz Niemann, Institut für Sensorik und Automation, Hochschule Hannover.

Kontakt:

karl-heinz.niemann@hs-hannover.de,
 jonas.kallisch@hs-emden-leer.de

Gefördert durch:



Koordiniert von:



Das Forschungsvorhaben Zukunftslabor Produktion mit dem Förderkennzeichen ZN3489 wird vom Niedersächsischen Ministerium für Wissenschaft und Kultur sowie von der Volkswagenstiftung gefördert und vom Zentrum für Digitale Innovationen Niedersachsen koordiniert. Die Autoren bedanken sich bei den genannten Institutionen für die Unterstützung.

aus der Produktionstechnik nach außen zu verhindern. Auch die eindeutige Nachvollziehbarkeit aller Nutzer, Komponenten und Datenströme minimiert die Angriffsfläche weiter. Die genaue Trennung zwischen der Kommunikation, also dem Austausch von Daten zwischen den Systemen und der Verarbeitung dieser Daten, bieten einen verbesserten Schutz sensibler Informationen. Selbst im Falle eines Eindringens in die Kommunikationswege bleiben die Bereiche, in denen die Daten tatsächlich verarbeitet werden, geschützt.

An allen Schnittstellen der Datenplattform werden Firewalls eingesetzt, um das System vor potenziellen Sicherheitsvorfällen zu schützen. Ein Anomalie-Erkennungssystem sowie ein Authentifizierungssystem für die Gesamtheit der Komponenten dienen der zuverlässigen Erkennung und Abwehr von Sicherheitsvorfällen. Ergänzend wird der Schutz durch weitere Maßnahmen wie Zugriffsmanagement, Protokollierung und eine System-Back-up-Strategie verstärkt.

Durch die Kombination aller Maßnahmen konnten die in der Bedrohungsanalyse aufgezeigten Schwachstellen effektiv behoben werden. Durch das abgestimmte Zusammenspiel von technischen und organisatorischen Ansätzen ist die Datenplattform abgesichert, sodass mögliche Angriffswege auf ein vertretbares Maß reduziert wurden.

Daten sichern. Prozesse optimieren. Zukunft gestalten

Die Ergebnisse des Teilprojekts verdeutlichen, dass eine digitale Transformation der Gießereibranche unabdingbar ist. Die zunehmende Vernetzung von Produktionssystemen und die wachsende Bedeutung von Informationen aus der Produktion erfordern einen sicheren und effizienten Umgang. In dem durchgeführten

Forschungsprojekt Zukunftslabor Produktion wurde dargestellt, wie eine Plattform, die auf Datensouveränität basiert, Shop-Floor-Daten in wertvolle Erkenntnisse umwandelt, ohne dass sensible Informationen die Unternehmen verlassen müssen. Der Einsatz von föderiertem Lernen ermöglicht die intransparente Kombination lokaler Unternehmens- zu globalen Analysen. Dadurch werden Potenziale erschlossen, wie die präzise Vorhersage von Prozessparametern, die Reduzierung von Ausschuss und die effizientere Nutzung von Ressourcen innerhalb der Lieferkette. Dies führt zu einem gemeinsamen Mehrwert für alle Beteiligten.

Um die Sicherheit der Plattform zu gewährleisten, wurde ein umfassendes Sicherheitskonzept entwickelt, das auf Standards wie VDI/VDE 2182 Blatt 1 und IEC 62443-3-3 basiert. Diese Maßnahmen dienen nicht nur dem Schutz sensibler Produktionsdaten, sondern fördern auch das Vertrauen zwischen Partnerunternehmen in der Lieferkette. Der Supply-Chain-Connector dient dabei als zentraler Kommunikationspunkt für eine kontrollierte und sichere Zusammenarbeit innerhalb des Konsortiums.

Aus technischer Sicht ermöglicht die Datenplattform den Betreibern von Gießereien, die Vorteile der Digitalisierung direkt in der täglichen Arbeit zu nutzen. Sie erlaubt datengetragene Entscheidungen, wie zum Beispiel die Beantwortung der Frage, ob ein Formwerkzeug ausgetauscht werden muss. Gleichzeitig ermöglichen die Analysen, eine präzisere Steuerung der Prozesse. Das führt zu einer Reduzierung von Ausschuss und einer effizienteren Nutzung von Ressourcen. Die Plattform lässt sich einfach in bestehende Systeme integrieren und ist für Anlagen jeder Art kompatibel.

Die Kombination von Datensouveränität, Sicherheit und Innovation ist ein ent-