

PRESSEMITTEILUNG

16. Februar 2021 || Seite 1 | 4

Maschinendaten vor Manipulationen schützen

Fernwartung mit Fingerabdruck: Datensicherheit für Maschinen und Produktionsanlagen

Die Digitalisierung von Maschinen und Produktionsanlagen ermöglicht Fernwartungen – ein großer Vorteil sowohl für Maschinen- und Anlagenbauer als auch für kleine und mittlere Unternehmen (KMU), die Maschinen und Anlagen betreiben. Gibt es Störungen in der Produktion, musste das Wartungspersonal bisher in die Fabriken der KMU fahren, um vor Ort Testmessungen vorzunehmen. Dafür fehlen aber oft die geeigneten Mitarbeiterinnen und Mitarbeiter. Die Maschinen- und Anlagenbauer sind dann auf den Außendienst von Wartungsfirmen angewiesen – und die KMU müssen warten. Deutlich schneller geht es, wenn sie Maschinendaten auf digitalem Wege direkt an die Maschinen- und Anlagenbauer schicken. Bisher profitieren aber noch deutlich zu wenige Unternehmen von diesen technischen Möglichkeiten, denn sie zweifeln an der Datensicherheit. Deswegen haben Forscherinnen und Forscher des Fraunhofer-Instituts für Werkzeugmaschinen und Umformtechnik IWU dafür eine fälschungssichere Art der Datenspeicherung und -weitergabe entwickelt: Maschinenmessdaten erhalten einen Fingerabdruck, der sich nicht manipulieren lässt.

Die zunehmende Digitalisierung von Maschinen und Produktionsanlagen macht diese nicht nur effizienter, sondern auch komplexer. KMU haben beispielsweise oft weder das Personal noch das Know-how, um die Wartung der modernen Produktionsanlagen, die sie betreiben, selbst auszuführen. Maschinen- und Anlagenbauer bieten diesen Service an, stehen aber beim Personal vor demselben Problem. Die naheliegende Lösung: Fernwartungen. Zwar liegen die notwendigen Messdaten für eine Fernwartung bei den KMU vor, doch um die Datenintegrität zu gewährleisten und – gewollte oder ungewollte – Datenmanipulationen auszuschließen, arbeiten immer noch viele Wartungsdienstleister vor Ort in den Fabriken. Die KMU müssen warten und in dieser Zeit ihre Produktion einschränken.

Kontakt Pressestelle

Dr. Christian Schäfer-Hock | Fraunhofer-Institut für Werkzeugmaschinen und Umformtechnik IWU | Telefon +49 (0)371 5397-1454 | Reichenhainer Straße 88 | 09126 Chemnitz | www.iwu.fraunhofer.de | presse@iwu.fraunhofer.de

Daten für Audits: Manipulation ausgeschlossen

16. Februar 2021 || Seite 2 | 4

Bisher fehlte eine praktikable Lösung, Messdaten zu verschlüsseln und Dritten dennoch für die Audits zur Verfügung zu stellen. Wissenschaftlerinnen und Wissenschaftler des Fraunhofer IWU haben daher im Rahmen des Forschungsprojektes »AUDIo« (Auditlösung für Machine-Learning-basierte, datengetriebene Dienstleistungen) eine IT-Architektur aufgebaut, um Fernwartungen und andere Services im Produktionsumfeld fälschungssicher anbieten zu können. Dabei werden die Prozess- oder Produktdaten verschlüsselt und auf Netzwerkknoten (Datenspeicher) abgelegt. Wer die Daten dann nutzen will, kann mit einer entsprechenden Zugriffsberechtigung über ein Portal auf sie zugreifen. Ein hinterlegter Datei-Fingerabdruck schützt dabei vor unentdeckter Manipulation. Auf diese Weise werden die Daten für Audits sicher nutzbar.

Kalibrierungen selbst anstoßen – Wartungszyklen flexibel planen

In dem Projekt »AUDIo« kümmern sich die Fraunhofer-Forschenden unter anderem speziell um die Kalibrierung von Werkzeugmaschinen ohne aufwändige Vorbereitungen wie Termin- und Reiseplanungen seitens der Maschinen- und Anlagenbauer oder Wartungsdienstleister: Mit dem weit verbreiteten Kreisformtest (»Double Ball Bar«) können KMU als Maschinenbetreiber die notwendigen Parameter zur Ermittlung der Positioniergenauigkeit erfassen und selbst prüfen. Das neue IT-System erlaubt ihnen sogar, einen Teil der notwendigen Kalibrierungen eigenständig vorzunehmen.

»Die Ergebnisse des AUDIo-Projekts ermöglichen Maschinenbetreibern jetzt einen Rollenwechsel vom passiv geprägten Auftraggeber oder ›Consumer‹ hin zum ›Prosumer‹«, sagt Dipl.-Medieninformatiker Gordon Lemme, Wissenschaftler im Wissenschaftsbereich »Produktionssysteme und Fabrikautomatisierung« am Fraunhofer IWU. »Das heißt, er wird quasi zu einem Verbraucher, der gleichzeitig Produzent ist, indem er die Kalibrierung zum gewünschten Zeitpunkt selbst anstoßen und notwendige Daten selber aufnehmen kann. Das funktioniert also ›eventbasiert‹, ohne die bislang üblichen Wartezeiten mit stillstehenden Maschinen und auch ohne Reisekosten für Servicepersonal. Wartungszyklen können so kurzfristig und weitestgehend unabhängig geplant werden.«

Hash-Funktion als Fingerabdruck

Nach Erhebung der Messdaten einer Maschine mittels »Double Ball Bar«-System wird von dem Datensatz vollautomatisch ein einzigartiger Datei-Fingerabdruck generiert. Diese sogenannte Hash-Funktion zeichnet sich dadurch aus, dass sie leicht errechnet werden kann, ihre Umkehr aber ausgeschlossen ist. Dies bedeutet, dass eine Berechnung des Datei-Fingerabdrucks auf Grundlage des Dateiinhaltes schnell und leicht realisiert werden kann, wohingegen es praktisch unmöglich ist, den Inhalt auf Basis des Hash-Wertes zu ermitteln. Die Daten sind fälschungssicher.

Anschließend kann der Maschinenbetreiber die Datei verschlüsselt auf einer bereitgestellten Dienstleistungsplattform ablegen – bei einem Clouddienstleister oder auf einem eigenen Server. Dem Maschinenbauer oder einem Dienstleister kann er dann über eine Kalibrierungs-Applikation (App) entsprechende Zugriffsrechte für die Datenanalyse oder eine Fernwartung einräumen.

Datensicherung nach dem Distributed-Ledger-Prinzip

Über die Dienstleistungsplattform wird der Datei-Fingerabdruck parallel auf der Hardware aller Teilnehmer des Netzwerks (Gateway) in Form einer identischen Kopie abgelegt und mit vorherigen Fingerabdrücken anderer Dateien über einen Algorithmus verkettet. Das ist das Distributed-Ledger-Prinzip: »Dadurch entsteht ein verteiltes System mit beliebig vielen Teilnehmenden, also zum Beispiel Maschinenbetreibern, Dienstleistern und Maschinenherstellern. Auf diese Weise lässt sich die Integrität der Daten bei diesen datengetriebenen Dienstleistungen sehr leicht kontrollieren. Denn bei jedem Gateway kommen die miteinander verketteten Datei-Fingerabdrücke quasi zur Deckung. Hierdurch wird die nachträgliche Manipulation eines einzelnen Fingerabdrucks nahezu unmöglich, denn durch die zahlreichen, identischen Kopien auf den vielen anderen Gateways kommt es bei einer Veränderung an nur einem Gateway zu keiner Übereinstimmung der Netzwerkteilnehmenden. Eine Manipulation würde sofort auffallen« erklärt Gordon Lemme.

Das System verhindert so auch, dass eine Schwachstelle, ein sog. »Single-Point-of-Failure« entsteht. Mithilfe der Originaldateien kann der für alle Netzwerkteilnehmenden einsehbare Datei-Fingerabdruck jederzeit neu erzeugt werden, wohingegen fehlerhafte Daten einen erkennbar falschen Fingerabdruck erzeugen.

Zum Projekt »AUDlo«

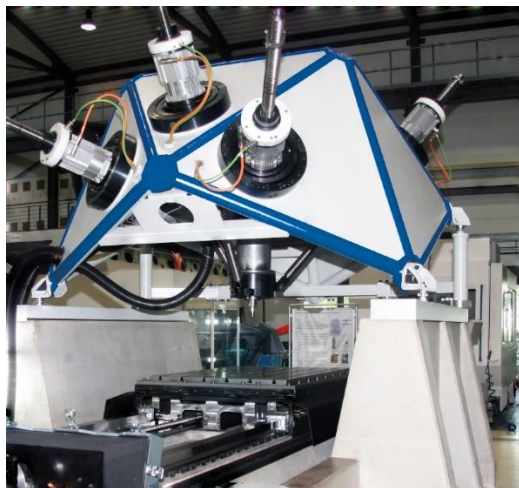
16. Februar 2021 || Seite 4 | 4

Das Forschungsprojekt »AUDlo« wird aufgrund eines Beschlusses des Deutschen Bundestages finanziert durch das BMWi-Programm »Smarte Datenwirtschaft«, Reg.-Nr. 01MD19005. Projektpartner sind die Technische Universität Dresden, die Software AG (Darmstadt) und die METROM Mechatronische Maschinen GmbH.

Bilder:



(1) Logo des Forschungsprojektes »AUDlo – Auditlösung für Machine-Learning-basierte, datengetriebene Dienstleistungen« © Fraunhofer IWU



(2) Mobile Arbeitsmaschine, an der eine Kalibrierung mit manipulationssicheren Daten vorgenommen wird © Fraunhofer IWU

Bilder in hoher Auflösung downloaden: <https://s.fhg.de/UB2>