(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
23. März 2017 (23.03.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/045789 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04W 4/00* (2009.01)
H04W 12/10 (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2016/064785

(22) Internationales Anmeldedatum:
27. Juni 2016 (27.06.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2015 217 855.2
17. September 2015 (17.09.2015) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FISCHER, Kai**; Heinrich-Marschner-Straße 74, 85598 Baldham (DE). **HEINTEL, Markus**; Prälat-Wellenhofer-Str. 31, 81377 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

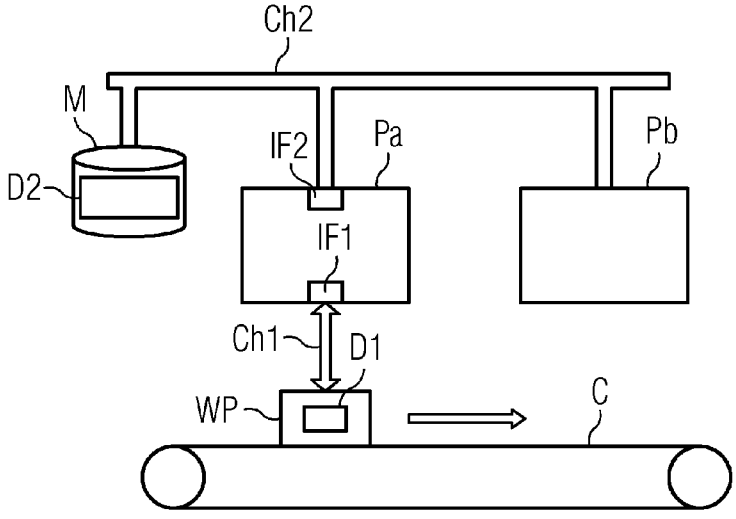
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

WO 2017/045789 A1

(54) Title: EXAMINING A CONSISTENCY BETWEEN REFERENCE DATA OF A PRODUCTION OBJECT AND DATA OF A DIGITAL TWIN OF THE PRODUCTION OBJECT

(54) Bezeichnung : PRÜFUNG EINER KONSISTENZ ZWISCHEN REFERENZDATEN EINES FERTIGUNGSOBJEKTES UND DATEN EINES DIGITALEN ZWILLINGS DES FERTIGUNGSOBJEKTES

FIG 1



(57) Abstract: The invention relates to a method, to an associated computer program product, to a production unit, and to an arrangement for examining a consistency between reference data of a production object and data of a digital twin of the production object, wherein two separate communication channels are used.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren, ein zugehörigen Computerprogrammprodukt, eine Fertigungseinheit sowie eine Anordnung zur Prüfung einer Konsistenz zwischen Referenzdaten eines Fertigungsobjektes und Daten eines digitalen Zwillings des Fertigungsobjektes, wobei zwei getrennte Kommunikationskanäle genutzt werden.

Beschreibung

Prüfung einer Konsistenz zwischen Referenzdaten eines Fertigungsobjektes und Daten eines digitalen Zwillings des Fertigungsobjektes

Die Erfindung betrifft ein Verfahren, ein zugehörigen Computerprogrammprodukt, eine Fertigungseinheit sowie eine Anordnung zur Prüfung einer Konsistenz zwischen Referenzdaten eines Fertigungsobjektes und Daten eines digitalen Zwillings des Fertigungsobjektes, wobei zwei getrennte Kommunikationskanäle genutzt werden.

In modernen Automatisierungsanlagen werden zur Steuerung von Fertigungsprozessen oder einzelnen Produktionsschritten IT-Systeme eingesetzt. Diese IT-Systeme kontrollieren den Fertigungsprozess basierend auf einem digitalen Abbild der Fertigungsanlage oder einem digitalen Abbild eines zu produzierenden Werkstücks. Das digitale Abbild wird auch digitaler Zwilling oder Digital Twin genannt. Der digitale Zwilling des Werkstücks wird während der Fertigung mit dem Zustand des Werkstücks synchronisiert. Der Einsatz von IT-Systemen in der Industrieautomatisierung erfordert angepasste Maßnahmen zur Gewährleistung der IT-Sicherheit. IT-Systeme mit deren zugrundeliegendem Kommunikationsnetzwerk sind oftmals leichter angreifbar. Insbesondere ist die Konsistenz zwischen physischer Welt und virtueller Repräsentation in Form des digitalen Zwillings entscheidend für einen sicheren Produktionsablauf. Daher sollen Manipulationen an einem Werkstück oder an seinem digitalen Zwilling erkennbar sein.

Es ist allgemein bekannt, eine eindeutige Referenz auf einem Werkstück oder einem Werkstückträger anzubringen, beispielsweise mittels eines passiven Markers wie eines Barcodes oder NFC-Chips. Diese Referenz kann von einer Fertigungsanlage ausgelesen werden und ermöglicht eine eindeutige Zuordnung des Werkstücks bzw. die Zuordnung zu seinem digitalen Zwilling. Es ist überdies bekannt, dass ein Werkstück selbst über

IT-Fähigkeiten verfügt und einer Fertigungsanlage aktiv eine Referenz senden kann. Mit diesen Verfahren wird ungesichert eine Referenz des Werkstücks an eine bearbeitende Maschine übermittelt. Sobald ein Auslesen beispielsweise eines RFID-Chips möglich ist, kann eine ungesicherte Übertragung durchgeführt werden, auch durch nicht zu diesem Zweck vorgesehene Lesegeräte, die beispielsweise manipuliert sind. Zudem könnte ein Werkstück einen manipulierten Referenzwert übertragen.

Das Vorsehen kryptographischer Verfahren zum Schutz des Referenzwertes erfordert einen aufwändigen Key Management Prozess, bei welchem gegebenenfalls durch jedes Werkstück einzeln Schlüsselmaterial ausgestellt und verwaltet werden muss. Bei einer Vielzahl von Werkstücken innerhalb einer Fertigungsanlage ist dieser Prozess komplex und verwaltungsintensiv.

Daher ist es Aufgabe der vorliegenden Erfindung, ein Verfahren, ein Computerprogrammprodukt hierfür, ein Fertigungsobjekt sowie eine Anordnung bereitzustellen, welche auf einfache Weise die Sicherheit bei der Verarbeitung von Daten eines digitalen Zwillings eines Fertigungsobjektes erhöhen.

Diese Aufgabe wird durch die Gegenstände der unabhängigen Ansprüche gelöst. Vorteilhafte Ausgestaltungen sind in den abhängigen Ansprüchen angegeben.

Die Erfindung betrifft ein Verfahren zur Prüfung einer Konsistenz zwischen Referenzdaten eines Fertigungsobjektes und Daten eines digitalen Zwillings des Fertigungsobjektes, wobei die Referenzdaten über einen ersten Kommunikationskanal und die Daten des digitalen Zwillings über einen zweiten Kommunikationskanal übertragen werden, und wobei eine erste Übertragung über den ersten Kommunikationskanal an eine physische Verfügbarkeit des Fertigungsobjektes innerhalb einer Fertigungsanlage gekoppelt ist und eine zweite Übertragung über den zweiten Kommunikationskanal an einen Zugriff auf ein Kommunikationsnetzwerk der Fertigungsanlage gekoppelt ist.

Unter einem Fertigungsobjekt wird beispielsweise ein Werkstück oder Werkstückträger verstanden, beispielsweise ein Werkstück, welches in einem Fertigungsprozess bearbeitet wird. Es kann sich um einen Herstellungsschritt innerhalb eines Veredelungsprozesses handeln oder um einen Zusammenbau mehrerer Werkstücke zu einem Produkt.

Die Referenzdaten des Fertigungsobjektes enthalten zumindest eine Information, die die Identifikation des Fertigungsobjektes ermöglicht. Beispielsweise ist eine Nummerierung der Fertigungsobjekte innerhalb einer Fertigungsanlage vorgesehen, welche jedes Werkstück oder jedes Objekt zur Bearbeitung eines Werkstückes eindeutig identifiziert. Die Referenzdaten können dafür einen Referenzwert enthalten, der speziell zu Zwecken der Identifizierung vorgesehen ist.

Auf dem digitalen Zwilling des Fertigungsobjektes ist beispielsweise der Fertigungsplan hinterlegt, nach welchem der Fertigungsprozess durchgeführt werden soll. Beispielsweise sind Statusinformationen zum Status des Fertigungsobjektes in aktueller Form auf dem Werkstück hinterlegt. Der digitale Zwilling spiegelt die momentan bestehende physische Anordnung in einer Fertigungsanlage oder einen Status einer Fertigungsanlage, beispielsweise eines Cyber Physical Production Systems, kurz CPPS. Dies ermöglicht eine Synchronisation und bidirektionale Wechselwirklung oder Absprache mit der digitalen Welt in einem PLM- oder Engineering System. Der digitale Zwilling enthält beispielsweise Informationen über die Kapazitäten oder Umgebungsbedingungen, Produktionsschritte oder Aufgaben innerhalb des Cyber Physical Production Systems. Beispielsweise wird ein Speicherinhalt nach jedem Fertigungsschritt aktualisiert, um den Status anzupassen.

Es sind zwei Kommunikationskanäle, ein erster Kommunikationskanal und ein zweiter Kommunikationskanal vorgesehen. Der erste Kommunikationskanal ist an eine physische Verfügbarkeit des Fertigungsobjektes innerhalb einer Fertigungsanlage ge-

koppelt. Beispielsweise ist der erste Kommunikationskanal nur aktiv oder nur nutzbar, falls sich das Fertigungsobjekt in einer bestimmten räumlichen Umgebung innerhalb der Fertigungsanlage aufhält. Somit beruht der erste Kommunikationskanal auf einer physischen Nähe des realen Werkstücks zu einem Wirkungsbereich des Kommunikationspartners. Dabei kann es sich beispielsweise um eine Fertigungseinheit handeln.

Der zweite Kommunikationskanal ist an einen Zugriff auf ein Kommunikationsnetzwerk der Fertigungsanlage gekoppelt. Beispielsweise kann der zweite Kommunikationskanal nur genutzt werden, falls eine Nutzung oder ein Zugang oder ein Zugriff auf ein IT-System der Fertigungsanlage möglich ist. Insbesondere ist ein solcher zweiter Kommunikationskanal über das Kommunikationsnetzwerk der Fertigungsanlage für eine Fertigungsanlage während eines Produktionsprozesses dauerhaft aktiviert und nutzbar. Beispielsweise kann eine Fertigungseinheit mit anderen Fertigungseinheiten der Fertigungsanlage permanent Daten austauschen. Es kann überdies der Zugriff auf das Kommunikationsnetzwerk an eine Authentisierung der Fertigungsanlage gekoppelt sein, so dass nur autorisierte Anfragen Zugriff erhalten. Die Sicherheit beruht also auf Absicherung des Kommunikationsnetzwerkes, beispielsweise durch kryptographische Schlüssel oder Zertifikate. Der erste Kommunikationskanal ist hingegen beispielsweise nur in vorgegebenen Zeitspannen nutzbar, in welchem sich das Werkstück oder das Fertigungsobjekt beispielsweise nahe genug oder mit einer passenden Ausrichtung in der Nähe einer Fertigungseinheit befindet. Hier wird also die Sicherheit durch die physische Verfügbarkeit des Werkstücks hergestellt.

Auf vorteilhafte Weise werden Daten, die das Fertigungsobjekt betreffen, somit über zwei unabhängige Wege in der Anlage verteilt. Dadurch, dass das Werkstück selbst Informationen tragen kann, kann eine Fertigungsmaschine Daten des physischen Werkstücks direkt auslesen und überdies Daten des digitalen Zwillings des Werkstücks über den zweiten Kommunikationskanal beispielsweise aus einem IT-Kommunikationsnetz aus-

lesen. Die Verwendung zweier unabhängiger Kommunikationskanäle erhöht die Sicherheit der Daten des digitalen Zwillings, da ein Angreifer für einen erfolgreichen Angriff auf einen Fertigungsschritt zwei unabhängige Kommunikationskanäle gleichzeitig erfolgreich kompromittieren oder manipulieren muss. Beide Kommunikationskanäle sind vorteilhafterweise in einem digitalen Automatisierungssystem ohne notwendige Nachrüstung vorgesehen. Eine IT-Kommunikationsinfrastruktur, wie beispielsweise Profibus oder Industrial Ethernet, kann neben den üblichen Einsatzwecken auch zu Zwecken der Übertragung der Daten des digitalen Zwillings genutzt werden. Der physische Transport des Fertigungsobjektes bewirkt vorteilhafterweise automatisch, dass sich das Fertigungsobjekt gemäß dem Produktionsplan für bestimmte Zeiten in einem Wirkungsbereich einer Fertigungseinheit aufhält. Ein Kommunikationsweg, der auf physischer Nähe beruht, wie beispielsweise optische Kommunikationsverfahren oder Nahfeldkommunikationsverfahren, sind zum Auslesen von Referenzwerten vorgesehen.

Die Konsistenzprüfung zwischen Daten des physischen Werkstücks und Daten, die in einem digitalen Zwilling des Werkstücks gespeichert sind, sichert eine Integrität und/oder Authentizität einer der beiden Datensätze, sofern dem anderen vertraut werden kann. Somit sind Manipulationen von Daten des digitalen Abbildes im digitalen Zwilling oder Manipulationen am Werkstück oder Werkstückträger detektierbar. Ist einer der beiden Kommunikationskanäle geschützt bzw. das Werkstück oder der digitale Zwilling des Werkstücks geschützt, so kann die Konsistenzprüfung Auskunft über die Integrität des jeweils anderen Kanals oder Datensatzes geben.

Die Konsistenzprüfung erfolgt zu dem Zweck, im Falle einer Inkonsistenz reagieren zu können. Beispielsweise erfolgt ein Ausgeben eines Prüfergebnisses und nur im Falle einer bestätigten Konsistenz erfolgt daraufhin ein weiterer Schritt, beispielsweise eine Verarbeitung des Fertigungsobjektes durch die Fertigungseinheit. Beispielsweise ist eine Übertragung der Daten des digitalen Zwillings nur möglich in Fällen, in

denen ein Prüfergebnis vorliegt, das die Konsistenz zwischen den Referenzdaten und den Daten des digitalen Zwillings belegt, so dass damit insbesondere auf eine Integrität der Daten des digitalen Zwillings geschlossen werden kann. Es erfolgt auf vorteilhafte Weise eine Kopplung der Daten des digitalen Zwillings mit einem spezifischen physikalischen Werkstück.

Gemäß einer Ausgestaltung beruht der erste Kommunikationskanal auf einer physischen Nähe und ist insbesondere für ein optisches Kommunikationsverfahren oder für ein Nahfeldkommunikationsverfahren ausgerichtet. Somit kommt es zu einer Übertragung der Referenzdaten von einem Fertigungsobjekt über den ersten Kommunikationskanal nur, falls beispielsweise der physische Abstand klein genug ist. Beispielsweise wird ein Nahfeldkommunikationsverfahren wie NFC, kurz für Near-Field-Communication, angewandt, welches für kurze Strecken von wenigen Zentimetern eine Datenübertragung ermöglicht. Somit ist nur in einem begrenzten räumlichen Bereich innerhalb der Fertigungsanlage die erfolgreiche Nutzung des ersten Kommunikationskanales möglich. Eine Datenübertragung von insbesondere manipulierten Referenzdaten eines anderen oder manipulierten Fertigungsobjektes, welches sich nicht in dem festgelegten räumlichen Gebiet innerhalb der Fertigungsanlage, insbesondere in einem Radius um die Fertigungseinheit, befindet, können somit auf vorteilhafte Weise nicht über den ersten Kommunikationskanal übermittelt werden.

Gemäß einer Ausgestaltung beruht der zweite Kommunikationskanal auf einer Kommunikationsinfrastruktur, insbesondere auf einer Profibus- oder Industrial Ethernet-Struktur. Somit können klassische Industriekommunikationsnetzwerke genutzt werden, welche insbesondere eine Kopplung zu einem Büronetzwerk aufweisen können.

Gemäß einer Ausgestaltung wird als Referenzdaten neben einem Referenzwert zusätzlich eine erste Prüfsumme über die Daten des digitalen Zwillings übertragen und es wird eine zweite

Prüfsumme über die über den zweiten Kommunikationskanal übertragenen Daten des digitalen Zwillings gebildet und die zweite Prüfsumme mit der ersten Prüfsumme verglichen und auf Konsistenz hin geprüft. Insbesondere wird als Referenzwert ein Marker, z.B. in Form einer Seriennummer oder einer fertigungsanlageninternen Nummerierung übermittelt. Bei der ersten Prüfsumme über die Daten des digitalen Zwillings handelt es sich beispielsweise um einen Hash-Wert. Es wird eine Hash-Funktion auf die Daten des digitalen Zwillings angewandt und nur die Prüfsumme, aus welcher aufgrund der Eigenschaften von Einwegfunktionen nicht auf die Daten des digitalen Zwillings rückgeschlossen werden kann, sind auf dem Fertigungsobjekt hinterlegt. Beispielsweise werden der Referenzwert sowie die erste Prüfsumme der Daten des digitalen Zwillings von einem Prozessor einer Fertigungsanlage verarbeitet. In einer Variante ist der Referenzwert Bestandteil der Prüfsumme, das heißt es erfolgt eine Prüfsummenbildung über einen Datensatz aus den Daten des digitalen Zwillings verknüpft oder konkateniert mit dem Referenzwert.

Auf Basis der Referenz werden die Daten des digitalen Zwillings über den zweiten Kommunikationskanal angefordert. Beispielsweise sind diese auf einer zentralen Steuerungskomponente in einem Speicher hinterlegt. Beispielsweise führt der Prozessor auf Grundlage der über den zweiten Kommunikationskanal, z.B. über ein Industrial Ethernet-System, empfangenen Daten des digitalen Zwillings eine Prüfsummenbildung durch. Somit wird der Hash-Wert der Daten des digitalen Zwillings gebildet. Es handelt sich dabei um die zweite Prüfsumme. Diese beruht auf der Sicherheit des zweiten Kommunikationskanales bzw. der Unversehrtheit des Speichers. Es erfolgt ein Abgleich der beiden Prüfsummen. Sind diese beiden weitgehend identisch, beispielsweise nach Beachtung möglicher auftretender Übertragungsfehler, so liegt eine Konsistenz zwischen den Referenzdaten des Fertigungsobjektes und den Daten des digitalen Zwillings des Fertigungsobjektes vor. Es kann mit erhöhter Sicherheit davon ausgegangen werden, dass weder das Fertigungsobjekt selbst noch der digitale Zwilling manipu-

liert wurde. Somit ermöglicht das Verfahren einen Integritätsschutz der Daten des digitalen Zwillings.

Gemäß einer Ausgestaltung werden als Referenzdaten neben einem Referenzwert zusätzlich ein symmetrischer Schlüssel oder Informationen zur Generierung eines symmetrischen Schlüssels übertragen. Die Daten des digitalen Zwillings werden mit dem symmetrischen Schlüssel in verschlüsselter Form gespeichert und sind mit dem symmetrischen Schlüssel entschlüsselbar. Beispielsweise sind durch einen Prozessor einer Fertigungsmaschine der Referenzwert und der Schlüssel oder die Schlüsselinformationen über den ersten Kommunikationskanal empfangbar, sobald das Werkstück sich im Wirkungsbereich der Fertigungsmaschine befindet. Die Daten des digitalen Zwillings werden in verschlüsselter Form über den zweiten Kommunikationskanal von einem Speicher übertragen.

Nur falls das korrekte Schlüsselmaterial auf der Fertigungsmaschine vorliegt, können die Daten des digitalen Zwillings entschlüsselt werden. Ein Angreifer, welcher die Daten des digitalen Zwillings manipulieren möchte, müsste Kenntnis über den symmetrischen Schlüssel haben, um innerhalb des Kommunikationsnetzwerkes die Daten des digitalen Zwillings in unverschlüsselter Form verfügbar zu haben und dann gegebenenfalls zu manipulieren. Ein Austausch von verschlüsselten Daten durch einen Angreifer und eine Übertragung der manipulierten Daten kann beispielsweise unter Verwendung zusätzlicher Maßnahmen, beispielsweise vorteilhaft bei Verwendung von authenticated encryption, auffallen.

Überdies wird durch die vorgeschlagene Ausführungsform auf vorteilhafte Weise ein Auslesen der Daten des digitalen Zwillings auf Seiten des Kommunikationsnetzwerkes verhindert. Die Daten liegen zu keiner Zeit in unverschlüsselter Form vor. Beispielsweise liegen die Daten in unverschlüsselter Form erst auf der Fertigungseinheit vor und auch erst, nachdem der symmetrische Schlüssel über den ersten Kommunikationskanal ermittelt werden konnte. Vertrauliche Daten im digitalen

Zwilling sind auf vorteilhafte Weise erst lesbar, wenn eine Fertigungseinheit oder Maschine physischen Zugriff auf das Werkstück hat. Ebenso kann die Fertigungseinheit selbst erst dann Zugriff auf die Daten des Zwillings in unverschlüsselter Form bekommen und diese verarbeiten, wenn sie physischen Zugriff auf das Werkstück hat. Insbesondere können auf vorteilhafte Weise vertrauliche Prozessanweisungen innerhalb der Daten des digitalen Zwillings verschlüsselt werden. Weniger kritische Daten können unverschlüsselt vorliegen, um den Rechenaufwand zu reduzieren. Eine Schlüsselvereinbarung oder das Verteilen des Schlüsselmaterials kann beispielsweise in einer vertraulichen Umgebung während einer Initialisierungsphase vorgenommen werden.

Gemäß einer Ausgestaltung werden als Referenzdaten neben einem Referenzwert zusätzlich ein symmetrischer Schlüssel oder Informationen zur Generierung eines symmetrischen Schlüssels übertragen. Neben den Daten des digitalen Zwillings wird zusätzlich ein erster Nachrichtenauthentifizierungscode über die Daten des digitalen Zwillings übertragen und ein zweiter Nachrichtenauthentifizierungscode über die über den zweiten Kommunikationskanal übertragenen Daten des digitalen Zwillings mittels des symmetrischen Schlüssels gebildet. Der erste Nachrichtenauthentifizierungscode wird mit dem zweiten Nachrichtenauthentifizierungscode verglichen und auf Konsistenz hin geprüft. In diesem Szenario liegen zwar die Daten des digitalen Zwillings auch in unverschlüsselter Form innerhalb des Kommunikationsnetzwerkes vor, dafür entfällt ein Entschlüsselungsalgorithmus beispielsweise auf einem Prozessor der Fertigungseinheit und es kann sattdessen eine einfache Bildung eines Nachrichtenauthentifizierungscodes, beispielsweise eines Message Authentication Codes, kurz MAC genannt, durchgeführt werden. Es können auch sogenannte keyed-Hash-Funktionen verwendet werden, die eine Prüfsumme unter Einbeziehung des symmetrischen Schlüssels bilden.

Auf vorteilhafte Weise wird ein Integritätsschutz der Daten des digitalen Zwillings mittels der MAC-Prüfsumme oder der

keyed-Hash-Prüfsumme ermöglicht. Es ist so sichergestellt, dass die Daten des digitalen Zwillings nach einer initialen Hinterlegung der Prüfsumme, beispielsweise auf dem Speicher, auf den das Kommunikationsnetzwerk zugreift, nicht verändert oder manipuliert wurden bzw. Veränderungen der Daten im digitalen Zwilling nur durch autorisierte Entitäten erfolgte, die den zugehörigen Schlüssel kennen. Da zunächst ein erfolgreicher Abgleich zwischen dem ersten Nachrichtenauthentifizierungscode und dem zweiten Nachrichtenauthentifizierungscode erfolgen muss, bevor beispielsweise eine Weiterverarbeitung der Daten des digitalen Zwillings möglich ist, ist zugleich sichergestellt, dass auch die Übertragung über den ersten Kommunikationskanal, welche das Schlüsselmaterial bereitstellt, erfolgreich durchgeführt werden konnte. Da über das physische Werkstück und den ersten Kommunikationskanal also der passende Schlüssel oder das passende Schlüsselmaterial geliefert werden muss, um einen mit dem ersten Nachrichtenauthentifizierungscode übereinstimmende zweiten Nachrichtenauthentifizierungscode ermitteln zu können, wird die Authentizität des Fertigungsobjektes nachgewiesen. Eine erfolgreiche Konsistenzprüfung kann wiederum Voraussetzung für weitere Fertigungsschritte oder Freigaben oder Zugriffserlaubnis im Fertigungsverfahren sein.

Die Mechanismen zum Schutz der Vertraulichkeit und der Sicherstellung der Integrität bzw. Authentizität können vorteilhaft kombiniert werden.

Gemäß einer Ausgestaltung sind die Informationen als Startwert ausgebildet und geeignet zur Generierung des symmetrischen Schlüssels mittels einer Schlüsselableitungsfunktion. Es wird also entweder direkt ein symmetrischer Schlüssel oder ein Input für eine Schlüsselableitung ergänzt. Beispielsweise werden zur Schlüsselableitung sogenannte Key Derivation Functions verwendet.

Gemäß einer Weiterbildung werden ein fertigungsobjektspezifischer Schlüssel oder fertigungsobjektspezifische Informatio-

nen durch Einbeziehen fertigungsobjektspezifischer Merkmale in eine Schlüsselableitungsfunktion bereitgestellt, wobei die fertigungsobjektspezifischen Merkmale insbesondere mittels des Referenzwertes oder mittels einer physikalisch unklonbaren Funktion erzeugt werden. Somit kann ein je Fertigungsobjekt oder Werkstück individueller Schlüssel generiert werden oder übertragen werden. Somit sind die Daten des digitalen Zwillings nur entschlüsselbar oder eine MAC Prüfsumme darüber nur verifizierbar, falls der fertigungsobjektspezifisch passende Schlüssel mit Hilfe des ersten Kommunikationskanals verfügbar gemacht wurde. Beispielsweise kann eine optische physisch unklonbare Funktion, kurz PUF, eingesetzt werden, die die individuelle Oberflächenstruktur eines Werkstücks erfasst. So sind Daten des digitalen Zwillings auf vorteilhafte Weise nur entschlüsselbar, falls von dem passenden Fertigungsobjekt, das über die physikalisch unklonbare Funktion eindeutig charakterisiert ist, die Referenzdaten erfolgreich über den ersten Kommunikationskanal übertragen wurden.

Gemäß einer Ausgestaltung wird als Referenzdaten neben einem Referenzwert zusätzlich ein Eingangswert einer Einwegfunktion übertragen und die Daten des digitalen Zwillings über den zweiten Kommunikationskanal übertragen, falls ein Ergebniswert der Einwegfunktion über den Eingangswert mit einem gespeicherten Ergebniswert übereinstimmt. Es soll beispielsweise gelten, dass ein Ergebniswert E durch das Anwenden einer Hash-Funktion auf einen Eingangswert P erhältlich ist. Den Referenzdaten wird der Eingangswert P beigefügt. Ein Zugriff auf die Daten des digitalen Zwillings über den zweiten Kommunikationskanal soll nur möglich sein, wenn eine Hash-Wertbildung des passenden Ergebniswertes E mittels Anwendens der Hash-Funktion auf den korrekten Eingangswert P nachgewiesen werden kann. Dieser Nachweis erfolgt auf vorteilhafte Weise vor Übertragung der Daten des digitalen Zwillings, so dass die Kenntnis des Eingangswertes als Autorisierungsmerkmal genutzt wird. Alternativ kann eine Prüfung im Nachhinein erfolgen und beispielsweise eine Alarmmeldung bewirken. Dafür

liegt an geeigneter Stelle ein gespeicherter korrekter Ergebniswert vor. Insbesondere ist der korrekte Ergebniswert *E* Bestandteil der Daten des digitalen Zwillings. Es wird die Konsistenz zwischen den Referenzdaten inklusive Eingangswert *P* und den Daten des digitalen Zwillings inklusive Ergebniswert *E* geprüft. Wiederum ist ein Zugriff auf die Daten des digitalen Zwillings durch eine Fertigungseinheit nur möglich, falls auch die physische Nähe zu dem Fertigungsobjekt besteht, da Kenntnis über den Eingangswert *P* erlangt werden muss. Außerdem kann je nach Ausgestaltung des Eingangswertes eine Manipulation der Daten auf dem Werkstück oder Fertigungsobjekt oder des Fertigungsobjektes selbst erkennbar sein, da dann der korrekte Eingangswert in der Regel nicht vorliegen wird. Für Fälle, in denen der korrekte Eingangswert trotz Manipulation der Daten oder des Werkstücks vorliegt, kann zusätzlich ein Abgleich der Daten mit den Referenzdaten erfolgen, um eine Abweichung und so eine Manipulation erkennen zu können.

Die Konsistenzprüfung kann je nach Ausgestaltung ein direktes Abgleichen zweier Datensätze, insbesondere zweier Prüfsummen, beinhalten oder eine Plausibilitätsprüfung eines Referenzwertes, der aus entschlüsselten Referenzdaten gewonnen wird, oder eine Prüfung auf Übereinstimmung zweier verwendeter Schlüssel oder eine Abfrage eines Geheimnisses.

Die Erfindung betrifft ferner ein Computerprogrammprodukt mit einem Computerprogramm, das Mittel zur Durchführung des oben beschriebenen Verfahrens aufweist, wenn das Computerprogramm auf einer programmgesteuerten Einrichtung zur Ausführung gebracht wird.

Ein Computerprogrammprodukt, wie beispielsweise ein Computerprogrammmittel, kann beispielsweise als Speichermedium, wie beispielsweise Speicherkarte, USB-Stick, CD-ROM, DVD oder auch in Form einer herunterladbaren Datei von einem Server in ein Netzwerk bereitgestellt oder geliefert werden. Dies kann z.B. in einem drahtlosen Kommunikationsnetzwerk durch die Übertragung einer entsprechenden Datei mit dem Computerpro-

grammprodukt oder dem Computerprogrammmittel erfolgen. Als programmgesteuerte Einrichtung kommt insbesondere eine Steuereinrichtung, wie z.B. ein Mikroprozessor, in Frage.

Die Erfindung betrifft ferner eine Fertigungseinheit aufweisend eine erste Schnittstelle zu einem Fertigungsobjekt, wobei über die erste Schnittstelle Referenzdaten des Fertigungsobjektes empfangbar sind, wobei eine erste Übertragung der Referenzdaten an eine physische Nähe zwischen Fertigungseinheit und Fertigungsobjekt gekoppelt ist, sowie eine zweite Schnittstelle zu einem Kommunikationsnetzwerk einer Fertigungsanlage, wobei über die zweite Schnittstelle Daten eines digitalen Zwillings des Fertigungsobjektes empfangbar sind, wobei eine zweite Übertragung der Daten des digitalen Zwillings an einen Zugriff auf das Kommunikationsnetzwerk gekoppelt ist, sowie eine Prüfeinheit zum Prüfen einer Konsistenz zwischen Referenzdaten des Fertigungsobjektes und den Daten des digitalen Zwillings des Fertigungsobjektes.

Die Erfindung betrifft ferner eine Anordnung aus Fertigungsobjekt, Fertigungseinheit, Speichereinheit und Prozessor mit einem ersten Kommunikationskanal zwischen Fertigungsobjekt und Fertigungseinheit beruhend auf einer physischen Nähe zwischen Fertigungseinheit und Fertigungsobjekt zur Übertragung von Referenzdaten des Fertigungsobjektes und mit einem zweiten Kommunikationskanal eines Kommunikationsnetzwerkes zwischen Fertigungseinheit und Speichereinheit zur Übertragung von Daten eines digitalen Zwilling des Fertigungsobjektes, wobei der Prozessor geeignet ist zur Prüfung einer Konsistenz zwischen den Referenzdaten und den Daten des digitalen Zwillings.

Gemäß einer Ausgestaltung ist der Prozessor in die Fertigungseinheit integriert oder wird durch einen Cloud-Service bereitgestellt oder ist in eine Steuerungseinheit einer Fertigungsanlage integriert, insbesondere gemeinsam mit der Speichereinheit.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe der Figuren näher erläutert. Es zeigen:

Figur 1 schematische Darstellung eines Werkstückes beim Durchlaufen eines Ausschnittes einer Fertigungsstraße gemäß dem Ausführungsbeispiel der Erfindung;

Figur 2 schematische Darstellung der Kommunikationsschritte gemäß einer ersten Variante des Ausführungsbeispiels;

Figur 3 schematische Darstellung der Kommunikationsschritte gemäß einer zweiten Variante des Ausführungsbeispiels;

Figur 4 schematische Darstellung der Kommunikationsschritte gemäß einer dritten Variante des Ausführungsbeispiels;

Figur 5 schematische Darstellung der Kommunikationsschritte gemäß einer vierten Variante des Ausführungsbeispiels.

In den Figuren sind funktionsgleiche Elemente mit denselben Bezugszeichen versehen, sofern nichts anderes angegeben ist.

In Figur 1 ist schematisch das Durchlaufen mehrerer Fertigungsschritte durch ein Werkstück in einer automatisierten Fertigungsanlage gezeigt. Es handelt sich beispielsweise um eine Fertigungsstraße, bei welcher ein Werkstück WP je Fertigungseinheit Pa, Pb einen oder mehrere Produktionsschritte durchläuft. Beispielsweise handelt es sich um das Zusammenbauen mehrerer Komponenten oder um ein Veredeln des Werkstücks, oder ein Beschichten, oder um ein Umlagern auf einem Werkstückträger. Das Werkstück WP wird dabei beispielsweise mit Hilfe eines Förderbandes C in den Wirkungsbereich verschiedener Fertigungseinheiten Pa, Pb transportiert. Bei-

spielsweise wird durch eine erste Fertigungseinheit Pa die Oberfläche des Werkstückes WP bearbeitet. Es handelt sich beispielsweise um eine Schleifmaschine. Bei der darauffolgenden Fertigungseinheit Pb handelt es sich beispielsweise um eine Maschine zum Auftragen einer Beschichtung oder zum Anbringen von Hilfsmitteln, wie Schrauben oder ähnlichem. Das Werkstück WP weist einen Speicher auf, welcher einen Referenzdatensatz D1 speichern kann. Es kann sich dabei beispielsweise um einen Barcode oder NFC-Chip handeln. Beispielsweise ist ein passiver Marker vorgesehen, bei welchem eine Energieversorgung von außen über eine Antenne erfolgt. Sobald dieser Chip in die Nähe eines Lesers der ersten Fertigungseinheit Pa gelangt, kann der erste Kommunikationskanal Ch1 zwischen Werkstück WP und Fertigungseinheit Pa benutzt werden. Über diesen ersten Kommunikationskanal Ch1, der also auf der Nähe des Werkstücks WP zu einer ersten Schnittstelle IF1 beruht, wird ein Referenzwert übertragen, welcher das Werkstück WP identifiziert. Der Referenzwert ist Teil des Referenzdatensatzes D1.

Über eine zweite Schnittstelle IF2 kann die Fertigungseinheit Pa den zweiten Kommunikationskanal nutzen. Insbesondere wird ein IT-Kommunikationsnetzwerk genutzt, über welches der Fertigungseinheit Pa Daten des digitalen Zwillings D2 des Werkstückes WP übermittelt werden. Das IT-Kommunikationsnetzwerk kann ferner zum Datenverkehr der verschiedenen Fertigungseinheiten Pa, Pb einer Fertigungsanlage untereinander sowie von Fertigungseinheiten mit Steuereinheiten vorgesehen sein. Insbesondere greift die Fertigungseinheit Pa über den zweiten Kommunikationskanal Ch2 auf Daten aus einem Speicher M eines Steuerungsrechners zu. Die Konsistenzprüfung erfolgt insbesondere auf einem auf der Fertigungseinheit vorgesehenen Prozessor oder auf einer separaten Einheit, die zugleich einen Zugriff der Fertigungseinheit auf Daten über den zweiten Kommunikationskanal Ch2 nur in Abhängigkeit vom Ergebnis der Konsistenzprüfung freigibt.

Figur 2 zeigt zu einer ersten Variante des Ausführungsbeispiels eine schematische Darstellung der über die verschiedenen Kommunikationskanäle übertragenen Daten. Die Reihenfolge der Datenübertragungsschritte ist jeweils von oben nach unten aufzufassen. Zunächst wird beispielsweise gemäß der ersten Variante als Referenzdatensatz D1 der Referenzwert R1 sowie eine Prüfsumme H1 über die Daten des digitalen Zwillings übertragen. Es handelt sich beispielsweise bei der Prüfsumme H1 um den Hash-Wert der Daten des digitalen Zwillings. Somit sind auf dem Werkstück WP die Daten des digitalen Zwillings D2 des Werkstücks WP, welche einen Fertigungsplan oder Konfigurationsparameter oder ähnliches enthalten, nicht in direkt zugänglicher Weise gespeichert, sondern lediglich durch eine Prüfsumme geschützt hinterlegt.

Die Fertigungseinheit Pa, welche das Werkstück WP beispielsweise auf Grundlage der Daten des digitalen Zwillings D2 weiterverarbeiten soll, verwendet den Referenzwert R1, um über einen zweiten Kommunikationskanal Ch2 beispielsweise von einer zentralen Steuerungseinheit oder einem Cloud-Service die Daten des digitalen Zwillings D2, die dort auf einem Speicher M hinterlegt sind, anzufordern. Die Daten des digitalen Zwillings D2 werden der Fertigungseinheit bereitgestellt und diese bildet auf Basis der digitalen Daten D2 eine zweite Prüfsumme H2. Unter Anwendung der gleichen Funktion für die Prüfsummenberechnung wie bei der Berechnung der ersten Prüfsumme H1 sollte so ein identischer Wert bei der Prüfsummenberechnung ermittelt werden, so dass sich H1=H2 ergibt. Dann besteht eine Konsistenz zwischen den Referenzdaten D1 und den Daten des digitalen Zwillings D2 und es kann eine Authentizität der über das IT-Kommunikationsnetzwerk erhaltenen angenommen werden. Ergibt sich eine abweichende Prüfsumme, so kann auf eine Veränderung der Daten des digitalen Zwillings D2 oder eine Veränderung der ersten Prüfsumme H1 oder eine fehlerhafte Referenz R1 geschlossen werden. In jedem Fall ist von einer Integrität der Daten des digitalen Zwillings nicht ohne weiteres auszugehen.

Je nach Wahrscheinlichkeit für Schwachstellen können nun Fehlerquellen oder Manipulationsangriffe auf die Fertigungsanlage gesucht werden. Insbesondere werden auf vorteilhafte Weise Angriffe erkannt, welche eine Manipulation der Daten des digitalen Zwillings D2 bewirken. Ebenso wird ein Austausch des Werkstücks WP oder eine Manipulation des Werkstücks WP erkannt, sofern die eindeutige Referenz nicht mehr zum digitalen Zwilling passt oder die Prüfsumme H1 zur Sicherung der digitalen Daten des Zwillings D2 ausgetauscht oder verändert wurde.

Gemäß einer zweiten Variante übermittelt das Werkstück WP mit dem Referenzdatensatz D1 einen Referenzwert R1 sowie kryptographisches Schlüsselmaterial K. Diese Variante ist in Figur 3 veranschaulicht. Es wird insbesondere direkt ein Schlüssel, beispielsweise ein symmetrischer Schlüssel, übermittelt. Die Fertigungseinheit Pa erhält gemäß dieser Variante Daten des digitalen Zwillings D2 in verschlüsselter Form D2ENC. Dies geschieht über den zweiten Kommunikationskanal Ch2. Somit werden gemäß dieser Variante zu keinem Zeitpunkt Daten des digitalen Zwillings D2 in unverschlüsselter Form auf einem der Kommunikationskanäle der Fertigungsanlage übermittelt. Insbesondere wird mittels des Referenzwertes der dazugehörige verschlüsselte Datensatz D2ENC angefordert. Alternativ sind insbesondere die Datensätze von potentiellen Fertigungsobjekten, d.h. deren Digital-Twin-Daten, in verschlüsselter Form bereits auf der Fertigungseinheit Pa vorhanden und mittels des Referenzwertes wird die spätere Konsistenzprüfung durchgeführt.

Es wird nun von der Fertigungseinheit Pa bzw. einem darauf befindlichen Prozessor ein Entschlüsselungsalgorithmus angewandt, um aus den entschlüsselten Daten D2ENC des digitalen Zwillings unter Anwendung des kryptographischen Schlüssels K die Daten des digitalen Zwillings D2 in unverschlüsselter Form zu erhalten. Ist die Entschlüsselung erfolgreich, was beispielsweise mittels des Referenzwertes R1 geprüft werden kann, so erfolgt eine Weiterverarbeitung der entschlüsselten

Daten des digitalen Zwillings D2. Andernfalls wird beispielsweise eine Alarmmeldung von der Fertigungseinheit Pa ausgegeben, um eine Manipulation der auf dem Speicher M gespeicherten verschlüsselten Daten D2ENC des digitalen Zwillings oder eine Manipulation des Werkstückes WP zu melden.

Figur 4 veranschaulicht eine Alternative zur Variante in Figur 3, bei welcher ein Message Authentication Code MAC2 über den zweiten Kommunikationskanal Ch2 an die Fertigungseinheit Pa übertragen wird. Es handelt sich um eine mittels eines kryptographischen Schlüssels gebildete Prüfsumme über die Daten des digitalen Zwillings D2. Mittels des über den ersten Kommunikationskanal Ch1 empfangenen kryptographischen Schlüssel K wird ein zweiter Message Authentication Code MAC2 gebildet und dieser wird mit dem ersten Message Authentication Code MAC1 verglichen. Stimmen diese überein oder bis auf Übertragungsfehler überein, so liegt eine Konsistenz zwischen den Referenzdaten, inklusive des Schlüsselmaterials, und den Daten des digitalen Zwillings, mittels MAC geschützt, vor. Es kann daraus geschlossen werden, dass der über den ersten Kommunikationskanal Ch1 übertragene Referenzwert R1 sowie der kryptographische Schlüssel K von dem korrekten, zu dem digitalen Zwilling passenden Werkstück WP übermittelt wurden und nicht manipuliert wurden. Außerdem kann so sichergestellt werden, dass die Daten des digitalen Zwillings D2, welche beispielsweise auf einem Cloud-Server in unverschlüsselter Form gespeichert sind, seit Berechnen des Message Authentication Codes MAC1 nicht verändert wurden. Daher sollte die Berechnung in einer frühen, vertrauenswürdigen Phase erfolgen. Alternativ kann die Berechnung durch entsprechend autorisierte Entitäten zur Laufzeit erfolgen.

Bei einer vierten Variante, welche in Figur 5 veranschaulicht ist, wird über den ersten Kommunikationskanal neben dem Referenzwert R1 ein Eingangswert P1 oder ein sogenanntes Pre-Image übertragen. Es gilt, dass eine kryptographische Prüfsumme, beispielsweise eine Hash-Funktion, über den Eingangswert P1 das Ergebnis E1 liefert. Der Eingangswert P1 wird

über den zweiten Kommunikationskanal Ch2 im Kommunikationsnetzwerk der Fertigungsanlage übermittelt, insbesondere an eine zentrale Steuerungseinheit mit Prozessor. Diese berechnet das Ergebnis E1 des Anwendens einer Hash-Funktion auf den Eingangswert P1. Die Fertigungseinheit Pa muss gegenüber einer Prüfeinheit in der Lage sein, den korrekten Eingangswert P1 vorzuweisen. Aufgrund der Einwegeigenschaft der Hash-Funktion ist dies nur möglich, wenn der Eingangswert P1 der Fertigungsanlage über den ersten Kommunikationskanal übermittelt wurde. Über den zweiten Kommunikationskanal ist der korrekte Eingangswert P1 hingegen nicht erhältlich. Insbesondere liegt innerhalb des Kommunikationsnetzwerkes lediglich ein Referenzergebnis E2 vor, mit welchem E1 übereinstimmen muss, damit die Daten des digitalen Zwillings D2 ebenfalls über den zweiten Kommunikationskanal auf die Fertigungseinheit Pa übertragen werden.

Obwohl die Erfindung im Detail durch die Ausführungsbeispiele näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

Patentansprüche

1. Verfahren zur Prüfung einer Konsistenz zwischen Referenzdaten (D1) eines Fertigungsobjektes (WP) und Daten eines digitalen Zwillings (D2) des Fertigungsobjektes (WP), wobei die Referenzdaten (D1) über einen ersten Kommunikationskanal (Ch1) und die Daten des digitalen Zwillings (D2) über einen zweiten Kommunikationskanal (Ch2) übertragen werden, und wobei eine erste Übertragung über den ersten Kommunikationskanal (Ch1) an eine physische Verfügbarkeit des Fertigungsobjektes (WP) innerhalb einer Fertigungsanlage gekoppelt ist und eine zweite Übertragung über den zweiten Kommunikationskanal (Ch2) an einen Zugriff auf ein Kommunikationsnetzwerk der Fertigungsanlage gekoppelt ist.

2. Verfahren nach Anspruch 1, wobei der erste Kommunikationskanal (Ch1) auf einer physischen Nähe beruht und insbesondere für ein optisches Kommunikationsverfahren oder für Nahfeld-Kommunikationsverfahren ausgerichtet ist.

3. Verfahren nach Anspruch 1 oder 2, wobei der zweite Kommunikationskanal (Ch2) auf einer Kommunikationsinfrastruktur beruht, insbesondere auf einer Profibus oder Industrial Ethernet-Struktur.

4. Verfahren nach einem der vorstehenden Ansprüche, wobei als Referenzdaten (D1) neben einem Referenzwert zusätzlich eine erste Prüfsumme über die Daten des digitalen Zwillings (D2) übertragen wird und wobei eine zweite Prüfsumme über die über den zweiten Kommunikationskanal (Ch2) übertragenen Daten des digitalen Zwillings (D2) gebildet wird und die zweite Prüfsumme mit der ersten Prüfsumme verglichen und auf Konsistenz hin geprüft wird.

5. Verfahren nach einem der vorstehenden Ansprüche, wobei als Referenzdaten (D1) neben einem Referenzwert zusätzlich ein symmetrischer Schlüssel oder Informationen zur Generierung eines symmetrischen Schlüssels übertragen werden und wobei

die Daten des digitalen Zwillings (D2) in mit dem symmetrischen Schlüssel verschlüsselter Form gespeichert werden und mit dem symmetrischen Schlüssel entschlüsselbar sind.

6. Verfahren nach einem der vorstehenden Ansprüche, wobei als Referenzdaten (D1) neben einem Referenzwert zusätzlich ein symmetrischer Schlüssel oder Informationen zur Generierung eines symmetrischen Schlüssels übertragen wird und wobei neben den Daten des digitalen Zwillings (D2) zusätzlich ein erster Nachrichtenauthentifizierungscode über die Daten des digitalen Zwillings (D2) übertragen wird und wobei ein zweiter Nachrichtenauthentifizierungscode über die über den zweiten Kommunikationskanal (Ch2) übertragenen Daten des digitalen Zwillings (D2) mittels des symmetrischen Schlüssels gebildet wird und der erste Nachrichtenauthentifizierungscode mit dem zweiten Nachrichtenauthentifizierungscode verglichen und auf Konsistenz hin geprüft wird.

7. Verfahren nach Anspruch 5 oder 6, wobei die Informationen als Startwert ausgebildet sind geeignet zur Generierung des symmetrischen Schlüssels mittels einer Schlüsselableitungsfunktion.

8. Verfahren nach einem der Ansprüche 5 bis 7, wobei ein fertigungsobjektspezifischer Schlüssel oder fertigungsobjektspezifische Informationen durch Einbeziehen fertigungsobjektspezifischer Merkmale in eine Schlüsselableitungsfunktion bereitgestellt werden, wobei die fertigungsobjektspezifischen Merkmale insbesondere mittels des Referenzwertes oder mittels einer physikalisch unklonbaren Funktion erzeugt werden.

9. Verfahren nach einem der vorstehenden Ansprüche, wobei als Referenzdaten (D1) neben einem Referenzwert zusätzlich ein Eingangswert einer Einwegfunktion übertragen wird und wobei die Daten des digitalen Zwillings (D2) über den zweiten Kommunikationskanal (Ch2) übertragen werden, falls ein Ergebniswert der Einwegfunktion über den Eingangswert mit einem gespeicherten Ergebniswert übereinstimmt.

10. Computerprogrammprodukt mit einem Computerprogramm, das Mittel zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 9 aufweist, wenn das Computerprogramm auf einer programmgesteuerten Einrichtung zur Ausführung gebracht wird.

11. Fertigungseinheit (Pa) aufweisend
- eine erste Schnittstelle (IF1) zu einem Fertigungsobjekt (WP), wobei über die erste Schnittstelle (IF1) Referenzdaten (D1) des Fertigungsobjektes empfangbar sind, wobei eine erste Übertragung der Referenzdaten (D1) an eine physische Nähe zwischen Fertigungseinheit (Pa) und Fertigungsobjekt (WP) gekoppelt ist, sowie

- eine zweite Schnittstelle (IF2) zu einem Kommunikationsnetzwerk einer Fertigungsanlage, wobei über die zweite Schnittstelle (IF2) Daten eines digitalen Zwillings (D2) des Fertigungsobjektes (WP) empfangbar sind, wobei eine zweite Übertragung der Daten des digitalen Zwillings (D2) an einen Zugriff auf das Kommunikationsnetzwerk gekoppelt ist, sowie eine Prüfeinheit zum Prüfen einer Konsistenz zwischen Referenzdaten (D1) des Fertigungsobjektes (WP) und den Daten des digitalen Zwillings (D2) des Fertigungsobjektes (WP).

12. Fertigungseinheit nach Anspruch 11, wobei als Prüfeinheit ein Prozessor vorgesehen ist und der Prozessor in die Fertigungseinheit (Pa) integriert ist oder durch einen Cloud-Service bereitgestellt wird oder in eine Steuerungseinheit der Fertigungsanlage integriert ist, insbesondere gemeinsam mit einer Speichereinheit (M) zur Speicherung der Daten des digitalen Zwillings (D2).

13. Anordnung aus Fertigungsobjekt (WP), Fertigungseinheit (Pa), Speichereinheit (M) und Prozessor, mit einem ersten Kommunikationskanal (Ch1) zwischen Fertigungsobjekt (WP) und Fertigungseinheit (Pa) beruhend auf einer physischen Nähe zwischen Fertigungseinheit (Pa) und Fertigungsobjekt (WP) zur Übertragung von Referenzdaten (D1) des Fertigungsobjektes

(WP) und mit einem zweiten Kommunikationskanal (Ch2) eines Kommunikationsnetzwerkes zwischen Fertigungseinheit (Pa) und Speichereinheit (M) zur Übertragung von Daten eines digitalen Zwillings (D2) des Fertigungsobjektes (WP), wobei der Prozessor geeignet ist zur Prüfung einer Konsistenz zwischen den Referenzdaten (D1) und den Daten des digitalen Zwillings (D2).

14. Anordnung nach Anspruch 13, wobei der Prozessor in die Fertigungseinheit (Pa) integriert ist oder durch einen Cloud-Service bereitgestellt wird oder in eine Steuerungseinheit einer Fertigungsanlage integriert ist, insbesondere gemeinsam mit der Speichereinheit (M).

FIG 1

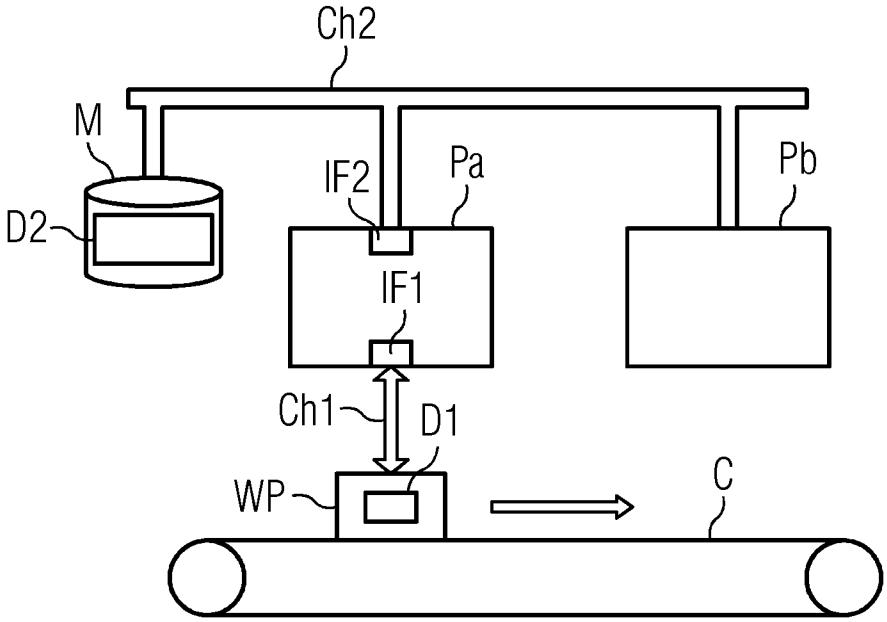

Ch2
M
D2
IF2
Pa
Pb
IF1
Ch1
D1
WP
C

FIG 2

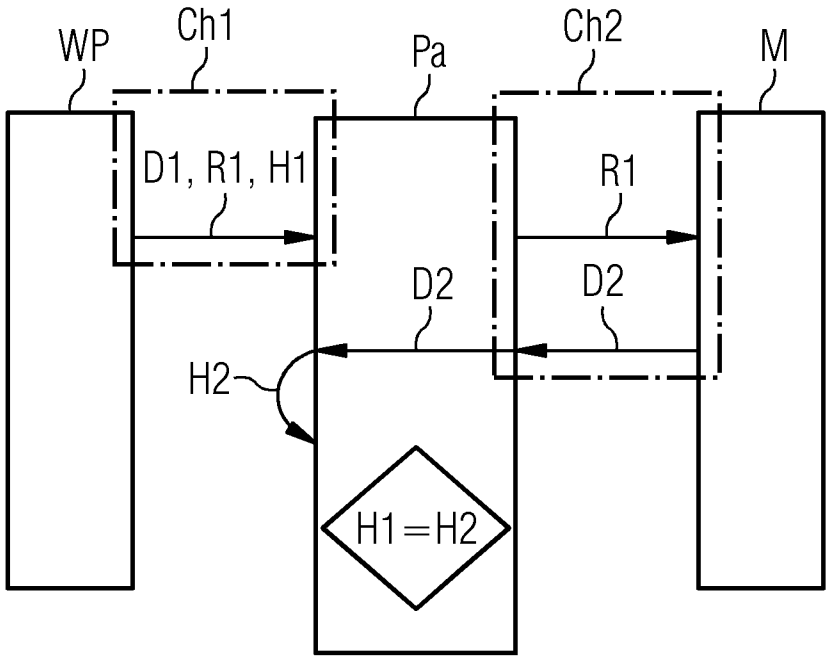

WP
Ch1
Pa
Ch2
M
D1, R1, H1
R1
D2
D2
H2
H1=H2

FIG 3

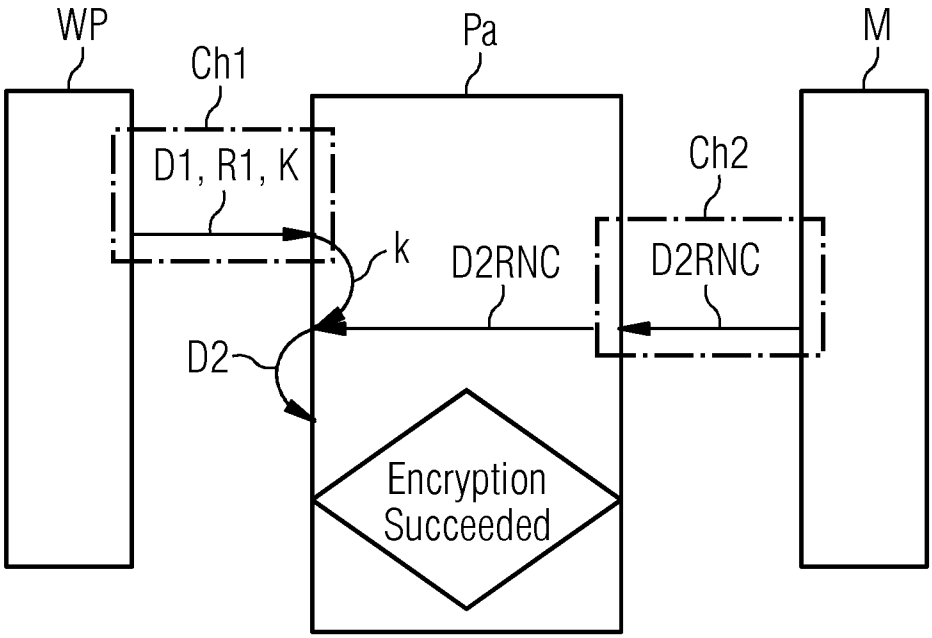

WP
Ch1
Pa
M
D1, R1, K
Ch2
k
D2RNC
D2RNC
D2
Encryption
Succeeded

FIG 4

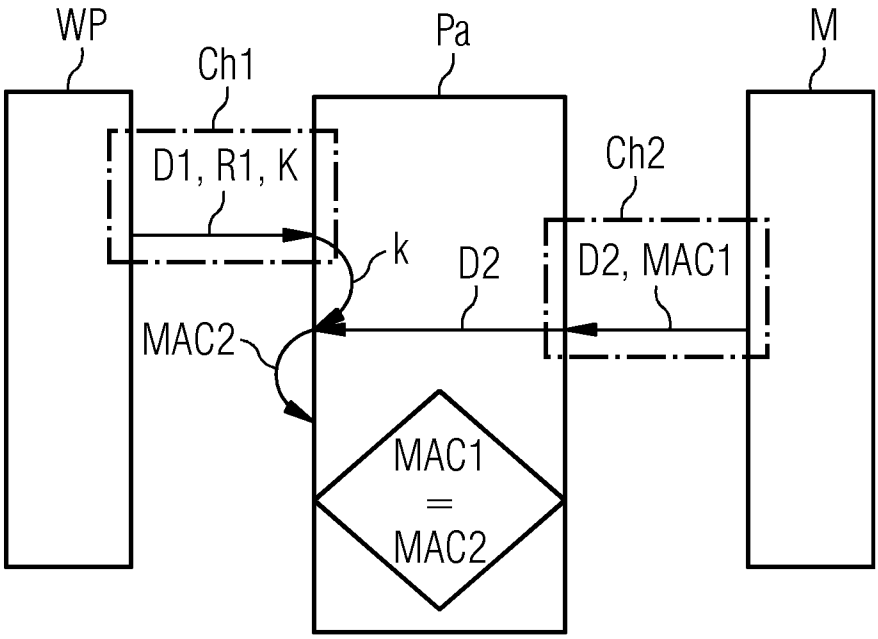
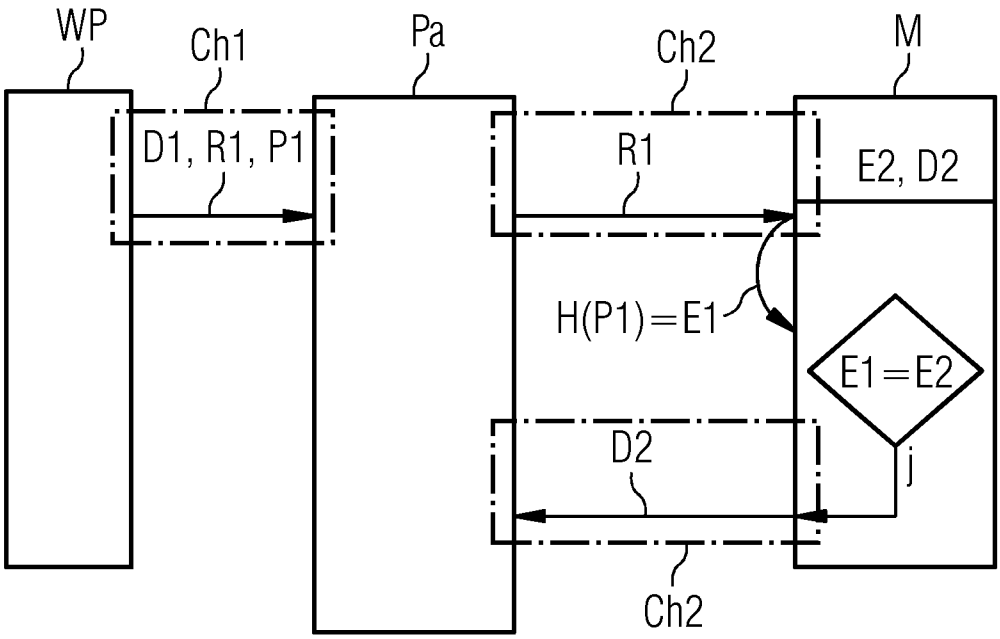

WP
Ch1
Pa
M
D1, R1, K
Ch2
k
D2
D2, MAC1
MAC2
MAC1
=
MAC2

FIG 5



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/064785

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/10
ADD. H04W4/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/158795 A1 (MARKHAM CHARLES EARL [US] ET AL) 21 August 2003 (2003-08-21) paragraphs [0202] - [0211]; figures 1, 2	1-14
A	US 2012/213366 A1 (BROWN DANIEL R [CA] ET AL) 23 August 2012 (2012-08-23) paragraphs [0002] - [0018]	1-14
A	WO 2007/056712 A2 (KESTREL WIRELESS INC [US]) 18 May 2007 (2007-05-18) paragraphs [0005] - [0009], [0029] - [0033]; figure 1	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 September 2016	29/09/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Winkelbauer, Andreas

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/064785

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003158795 A1	21-08-2003	AU 2002360803 A1	24-07-2003
		EP 1468380 A1	20-10-2004
		US 2003158795 A1	21-08-2003
		US 2006149407 A1	06-07-2006
		WO 03058506 A1	17-07-2003
US 2012213366 A1	23-08-2012	CA 2662675 A1	13-03-2008
		CN 101535845 A	16-09-2009
		EP 2076799 A1	08-07-2009
		EP 2680046 A1	01-01-2014
		JP 5260523 B2	14-08-2013
		JP 2010503295 A	28-01-2010
		JP 2013118706 A	13-06-2013
		JP 2013118707 A	13-06-2013
		US 2008069347 A1	20-03-2008
		US 2008150702 A1	26-06-2008
		US 2008164976 A1	10-07-2008
		US 2012213366 A1	23-08-2012
		WO 2008028291 A1	13-03-2008
WO 2007056712 A2	18-05-2007	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2016/064785

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 H04W12/10
ADD. H04W4/00

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L H04W

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2003/158795 A1 (MARKHAM CHARLES EARL [US] ET AL) 21. August 2003 (2003-08-21) Absätze [0202] - [0211]; Abbildungen 1, 2	1-14
A	US 2012/213366 A1 (BROWN DANIEL R [CA] ET AL) 23. August 2012 (2012-08-23) Absätze [0002] - [0018]	1-14
A	WO 2007/056712 A2 (KESTREL WIRELESS INC [US]) 18. Mai 2007 (2007-05-18) Absätze [0005] - [0009], [0029] - [0033]; Abbildung 1	1-14

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
14. September 2016	29/09/2016

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Winkelbauer, Andreas

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2016/064785

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003158795 A1	21-08-2003	AU 2002360803 A1	24-07-2003
		EP 1468380 A1	20-10-2004
		US 2003158795 A1	21-08-2003
		US 2006149407 A1	06-07-2006
		WO 03058506 A1	17-07-2003
US 2012213366 A1	23-08-2012	CA 2662675 A1	13-03-2008
		CN 101535845 A	16-09-2009
		EP 2076799 A1	08-07-2009
		EP 2680046 A1	01-01-2014
		JP 5260523 B2	14-08-2013
		JP 2010503295 A	28-01-2010
		JP 2013118706 A	13-06-2013
		JP 2013118707 A	13-06-2013
		US 2008069347 A1	20-03-2008
		US 2008150702 A1	26-06-2008
		US 2008164976 A1	10-07-2008
		US 2012213366 A1	23-08-2012
		WO 2008028291 A1	13-03-2008
WO 2007056712 A2	18-05-2007	KEINE	