

Diskussionspapier

# **Diskussionspapier zur Initiative 62443-Component Use-Cases**

April 2021

Fachverband Automation – LK Industrial Security

## Inhalt

Zielsetzung der Initiative	3
Ergebnis der Initiative	3
Einsatzmöglichkeiten und Grenzen der Ergebnisse der Initiative	4
Sensoren:	4
Speicherprogrammierbare Steuerungen:	5
Verwertung der Ergebnisse der Initiative	5

## Zielsetzung der Initiative

In der Anwendung der IEC 62443 ist die Bestimmung der relevanten oder notwendigen Security Anforderungen nach Normteil IEC 62443-4-2 immer wieder ein praktisches Problem. Ein Teil der Anwender nutzt die vereinfachende Sicht der vier Security Level (SL), das bedeutet die Auswahl aller in der Norm spezifizierten zugehörigen SL-Anforderungen, um unabhängig von der konkreten Einsatzumgebung alle dem SL zugehörigen Anforderungen auszuwählen, was aber oft unpräzise ist. Ein anderer Teil der Anwender nutzt dagegen den ganzheitlichen Ansatz und startet mit einer Risikoanalyse auf Systemebene und leitet dann exakte Security Anforderungen an die Komponenten ab. Diese Herangehensweise stellt für die Entwicklung generischer Komponenten eine Herausforderung dar, da die der Risikoanalyse zugrundeliegende Systemebene nur auf allgemeinen Grundannahmen beruhen kann.

Beide Sichtweisen haben Ihre Berechtigung, stoßen aber auf ihre Grenzen. Um die Akzeptanz zu erhöhen und eine von allen Parteien nachvollziehbare Sichtweise zu erlangen, sollten Hersteller und Nutzer eine Möglichkeit erhalten, ihre Perspektiven einzubringen.

Die gemeinsame Initiative zwischen TeleTrust und Mitgliedern des ZVEI verfolgte das Ziel mit den IEC 62443-Component Use-Cases beispielhaft einen Leitfaden für die beiden nachfolgenden Uses-Cases zu definieren.

Mit der Initiative sollte keine Ergänzung der IEC 62443-4-2 erfolgen, sondern eine einheitliche Anwendung der Norm außerhalb von Projekten oder Produktentwicklungen gefördert werden. Ziel ist es die IEC 62443 als Grundlage zu nutzen, um ihre Akzeptanz bei den Herstellern, den Anwendern und in der horizontalen Produktregulierung zu erhöhen.

In diesem Kontext wurden beispielhafte Use-Cases entwickelt, die aufzeigen sollen, dass auf Basis der Konzepte der IEC 62443 eine Strukturierung von Komponententypen für dedizierte Szenarien möglich ist. Ziel der Initiative war es, an zwei konkreten Beispielen aufzuzeigen, wie diese Strukturierung mittels Use-Cases für ausgewählte Szenarien umgesetzt werden kann. Die Ergebnisse der Initiative können damit zukünftig in der Standardisierung und bei der Definition von Zertifizierungsschemen herangezogen werden.

## Ergebnis der Initiative

Die Arbeitsgruppe zur Entwicklung der Use-Cases hat sich auf zwei Themen fokussiert. Zum einen wurde der *Use-Case Industrial Firewall* von einem Verbund von Herstellern solcher Komponenten entwickelt. Dieser Use-Case basiert daher auf der praktischen Erfahrung und zeigt die aktuelle Umsetzung in Produkten. Der zweite *Use-Case Security Gateway* wurde dagegen auf den Vorarbeiten der DIN SPEC 27070 und den

Ergänzungen der International Data Spaces Association (IDSA) definiert. Hierzu wurden die Vorarbeiten dieses Konsortiums genutzt.

Wichtig ist zu verstehen, dass Security in den Use-Cases nicht die primär abgrenzende Eigenschaft ist, stattdessen erfolgt dies über die eigentliche Funktionalität der Komponente in der Anlage. Hierzu wird ein starker Fokus auf den Verwendungszweck und die Einsatzumgebung der Komponente gelegt. Basierend auf den Security Anforderungen der Norm IEC 62443-4-2 werden im zweiten Schritt die Security-relevanten Eigenschaften der Komponente abgeleitet und definiert, die entsprechend eines sicheren Produktentwicklungslebenszyklus (IEC 62443-4-1) entwickelt und implementiert werden müssen.

Mit den Use-Cases wurde im Verlauf der Abstimmung ein effektives Moderationswerkzeug gefunden, mit dem in planbarer Zeit ein gemeinsames Verständnis zwischen Käufern (oder Integratoren) und Herstellern hergestellt werden kann. Das Werkzeug der Use-Cases ist ebenfalls auch für Branchenverbände, herstellerübergreifende Aktivitäten und Zertifizierungsschemen gut einsetzbar.

Ein ausführlicher Ergebnisbericht der Arbeitsgruppe ist dem Dokument angehängen (-> „Ergebnisbericht der Arbeitsgruppe zur Initiative 62443-Component Use-Cases“).

## **Einsatzmöglichkeiten und Grenzen der Ergebnisse der Initiative**

Mit den zwei Use-Cases wurde skizziert, wie ein strukturierter Prozess zur Ableitung von Security Anforderungen entsprechend IEC 62443-4-2 für Komponenten erfolgen kann. Dies schließt eine große Lücke in der Anwendung der IEC 62443-4-2. Eine Orientierung an funktionalen Use-Cases hat sich als effektiv herausgestellt. Andere Darstellungen waren bisher zu abstrakt und zu allgemein, wie die Component Types in der IEC 62443-4-2. Hinsichtlich Akzeptanz und Bewertung der erarbeiteten Herangehensweise ist eine breite Einbindung von Herstellern und Nutzern, idealerweise auf internationaler Ebene, wünschenswert.

Eine kritische Eigenschaft eines Use-Cases ist der Detailgrad der Definition. Ein Use-Case sollte nicht zu generisch sein, z. B. eine generisch einsetzbare SPS oder ein generischer Sensor. Gleichzeitig darf diese aber auch nicht zu spezifisch definiert sein. Die nachfolgenden Beispiele zeigen die Anwendbarkeit aber auch die Grenzen des Use-Case Vorgehens auf.

### **Sensoren:**

In einer komplexen Anlage über "den Sensor" zu sprechen würde die Sache zu einfach darstellen. In dem Beispiel des low-power Sensors wird die Security vermutlich eher im Rahmen eines Security Konzepts für die ganze Anlage adressiert, sodass kein

sinnvoller Component Use-Case definiert werden kann. Für diese Art der Sensoren würden eine grundlegende Sicherheitsfunktionen (Baseline Security) ein adäquates Schutzniveau darstellen.

Geht man davon aus, dass in dieser Anlage weitere Sensoren, z. B. für die Bilderkennung zum Einsatz kommen und diese mit Schnittstellen zur Datenanalyse ausgestattet wären, würden die Security Anforderungen nach IEC 62443-4-2 anwendbar sein. In diesem Fall kann ein anerkannter Use-Case definiert werden, unter der Annahme, dass diese Kamerasensoren ggf. über ein Betriebssystem verfügen, Software-Applikationen verwenden, welche Daten vorverarbeiten können, und über eine Netzwerkschnittstelle Daten zur zentralen Datenanalyse versenden.

Die beiden Sensor-Beispiele zeigen die existierende Spannbreite. Daher kann es auf keinen Fall nur einen generischer Sensor Use-Case , auch im Hinblick auf die Sicherheit von Komponenten nach IEC 62443-4-2, geben. Hier wird deutlich, dass bei einfachen Sensoren der Baseline Ansatz der Richtige wäre und die noch erforderlichen Sicherheitskontrollen dann auf der Systemebene implementiert (gemäß IEC 62443-3-3) werden. Bei Bedarf und höheren Anforderungen als den Baseline-Anforderungen könnte man über verschiedene Use-Cases für Sensoren nachdenken.

### Speicherprogrammierbare Steuerungen:

Eine generische SPS hat gleichfalls zu viele Use-Cases, sodass sich diese über eine einzelne Beschreibung nicht fassen lässt. Auch wäre es möglich einen sehr konkreten Anwendungsfall einer SPS im Rahmen einer Use-Case-Beschreibung zu definieren, wie z.B. eine SPS in einer Kläranlage oder im Energienetz. Insbesondere ein Use-Case für eine SPS in Energienetzen würde zu dem Detailniveau dieses Sektors passen. Beispielsweise die IEC 62351-5 gibt bereits konkrete Anforderungen für die „Anwenderschicht mittels Zugriffsberechtigung auf kritische Ressourcen einer Unterstation“ vor.

Die Anwendbarkeit der Component-Use-Cases für generische Komponenten bedarf einer fundierten Betrachtung, da u. a. auch bewertet werden muss, ob aufgrund der Vielzahl an möglichen Einsatzszenarien einzelne Component-Use-Cases sinnhaft und letztendlich praktikabel sind.

## Verwertung der Ergebnisse der Initiative

Bei der Entwicklung der beiden beispielhaften Component-Use-Cases hat sich gezeigt, dass für z. B. Sensoren oder SPS aufgrund ihrer unterschiedlichen Einsatzbedingungen (in einem System oder als Standalone-Komponente) und Verwendung in unterschiedlichsten Sektoren, ein allgemein gültiger Component-Use-Case nicht sinnvoll handhabbar ist.

Ziel ist es die in der Arbeitsgruppe gesammelten Erfahrungen hinsichtlich Erstellung und Anwendbarkeit von IEC 62443 Component-Use-Cases in die internationalen Diskussionen zur Bewertung von Komponenten einzubringen. Dazu zählen Aspekte wie die Steigerung der Akzeptanz von Herstellerselbsterklärungen oder Zertifizierungen von Komponenten auf Basis der IEC 62443-4-2 oder auch die Mitarbeit in den bei der IEC gestarteten Aktivitäten zur Definition von Regeln für IEC 62443 Profile.

Dieses Diskussionspapier bezieht sich auf die TeleTrust-Initiative **62443-Component Use-Cases**, die Ergebnisse können unter der folgenden Adresse aufgerufen werden: <https://www.teletrust.de/publikationen/teletrust-iec-62443-4-2/>



**Diskussionspapier zur Initiative 62443-  
Component Use-Cases**

Herausgeber:  
ZVEI - Zentralverband Elektrotechnik-  
und Elektronikindustrie e. V.  
Fachverband Automation / LK Industrial  
Security

Lyoner Str. 9  
60528 Frankfurt am Main

Verantwortlich:  
Marcel Hug  
Telefon: +49 69 6302-432  
E-Mail: Marcel.Hug@zvei.org

[www.zvei.org](http://www.zvei.org)

April 2021

Das Werk einschließlich aller seiner Teile ist  
urheberrechtlich geschützt.

Jede Verwertung außerhalb der engen Grenzen  
des Urheberrechtsgesetzes ist ohne  
Zustimmung des Herausgebers unzulässig.

Das gilt insbesondere für Vervielfältigungen,  
Übersetzung, Mikroverfilmungen und die Ein-  
speicherung und Verarbeitung in elektronischen  
Systemen.