Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

DELTA

Übertragbarkeitsanalyse der IEC 62443 Normenreihe für das Laden und Abrechnen in der Elektromobilität

DKE
VDE DIN

DELTA

Datensicherheit und -integrität in der Elektromobilität beim Laden und eichrechtkonformen Abrechnen

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Autoren:
Christian Seipel, DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Mit fachlicher Unterstützung von:
Michael Staubermann, Webolution GmbH
Stephan Cater, innogy SE

Herausgeber und Ansprechpartner:
DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE
Christian Seipel
Stresemannallee 15
60596 Frankfurt am Main
Telefon 069 6308-454
Christian.seipel@vde.com
https://www.dke.com

Design:
Schaper Kommunikation, Bad Nauheim

Diese Publikation ist im Rahmen des Förderprogramms „Elektro Power II“ im BMWi Verbundprojekt „Datensicherheit- und integrität in der Elektromobilität beim Laden und eichrechtkonformen Abrechnen“ (kurz: DELTA) erstellt worden.
Sie ist kostenfrei erhältlich.

Erscheinungsdatum: Dezember 2018

Inhaltsverzeichnis

Verzeichnisse 4
Abbildungsverzeichnis 4
Tabellenverzeichnis 4

Kurzfassung 5
1 Einleitung **7**
1.1 Motivation 7
1.2 Ziel der Übertragbarkeitsanalyse 8
1.3 Vorgehensweise 8
2 Begriffsdefinitionen **9**
3 Einführung in die IEC 62443 Normenreihe **10**
3.1 Zielsetzung der IEC 62443 Normenreihe 10
3.2 Struktur der IEC 62443 Normenreihe 10
4 Schutzziele in der Industrieautomatisierung und Elektromobilität **12**
4.1 Schutzziele in der IT-Sicherheit 12
4.2 Schutzziele in der Industrieautomatisierung 12
4.3 Schutzziele für das Laden und Abrechnen in der Elektromobilität 13
4.4 Relevanz der IEC 62443 für das Laden und Abrechen in der Elektromobilität 14
5 Grundkonzepte der IEC 62443 **15**
5.1 Tiefgestaffelte Verteidigung (Defense-in-Depth) 15
5.2 Zonen und Conduits 16
5.3 Risikobewertung nach VDI/VDE 2182 17
5.4 Sicherheitslevels 19
5.5 Zusammenfassung 21
6 Sicherheitsanforderungen für Systeme **22**
6.1 Allgemeine Vorgehensweise 22
6.2 Sicherheitsanforderungen zur Identifizierung und Authentifizierung 22
6.3 Anwendung für das Laden und Abrechnen in der Elektromobilität 24
7 Sicherheitsanforderungen für Produkte **25**
7.1 Einordnung von Anforderungen für Produkte 25
7.2 Prozessanforderungen für die Produktentwicklung 25
7.3 Sicherheitsanforderungen für Komponenten 27
7.3.1 Allgemeine Vorgehensweise 27
7.3.2 Sicherheitsanforderungen zur Identifizierung und Authentifizierung 27
7.3.3 Sicherheitsanforderungen an Softwareanwendungen 29
7.4 Anwendung für das Laden und Abrechnen in der Elektromobilität 29
8 Ansatz für ein ganzheitliches Schutzkonzepts für das Laden und Abrechnen in der Elektromobilität **30**
8.1 Vorgehensweise zum Aufbau eines ganzheitlichen Schutzkonzeptes 30
8.2 Anlagensicherheit für Fahrzeug, Ladeinfrastruktur und Backend 31
8.3 Netzwerksicherheit für Fahrzeug, Ladeinfrastruktur und Backend 32
8.4 Systemintegrität für Fahrzeug, Ladeinfrastruktur und Backend 33
9 Fazit und Ausblick **34**
Literatur 35

Verzeichnisse

Abbildungsverzeichnis

Abb. 1: Schematische Darstellung des Ökosystems „Elektromobilität“ 7
Abb. 2: Vorgehensweise zur Übertragbarkeit der IEC 62443 in die Elektromobilität 8
Abb. 3: Aufbau der Normenreihe IEC 62443 nach [11] 11
Abb. 4: Priorisierung der Schutzziele in der Office-IT und Produktions-IT 12
Abb. 5: Priorisierung der Schutzziele für das Laden und Abrechnen in der Elektromobilität 13
Abb. 6: Basisrollen und Aufgaben der IEC 62443 [10] 15
Abb. 7: Anwendung von Zonen und Conduits am Beispiel einer Organisation mit drei Fabriken [9] 16
Abb. 8: IT-Sicherheits-Lebenszyklus nach VDI/VDE 2182-1 [15] 18/19
Abb. 9: Iterativer Prozess zur Findung der optimalen Sicherheitslösung (vgl. Kapitel 5.3) 20
Abb. 10: Die „Defense-in-Depth“-Strategie mit möglichen Schutzmaßnahmen für die jeweiligen Schalen 21
Abb. 11: Die „Defense-in-Depth“-Strategie als Schlüsselkonzept für Sicherheit im Produkt-Lebenszyklus [16] 25
Abb. 12: Ganzheitlicher Ansatz - Anlagensicherheit 31
Abb. 13: Ganzheitlicher Ansatz - Netzwerksicherheit 32
Abb. 14: Ganzheitlicher Ansatz - Systemintegrität 33

Tabellenverzeichnis

Tabelle 1: Übersicht der Relevanz von Schutzzielen in den Bereichen Industrieautomation und Elektronmobilität 14
Tabelle 2: Zuordnung von SRs und REs einem zu erreichenden Sicherheitslevel für „Identifizierung und Authentifizierung“ [10] 23
Tabelle 3: Bereiche für Sicherheitsanforderungen [16] 26
Tabelle 4: Sicherheitsanforderungen für den Bereich „Sicherheits-Management“ [16] 26
Tabelle 5: Zuordnung von CRs und REs einem zu erreichenden Sicherheitslevel für „Identifizierung und Authentifizierung“ [20] 28
Tabelle 6: Zuordnung von SARs und REs einem zu erreichenden Sicherheitslevel [20] 29

Kurzfassung

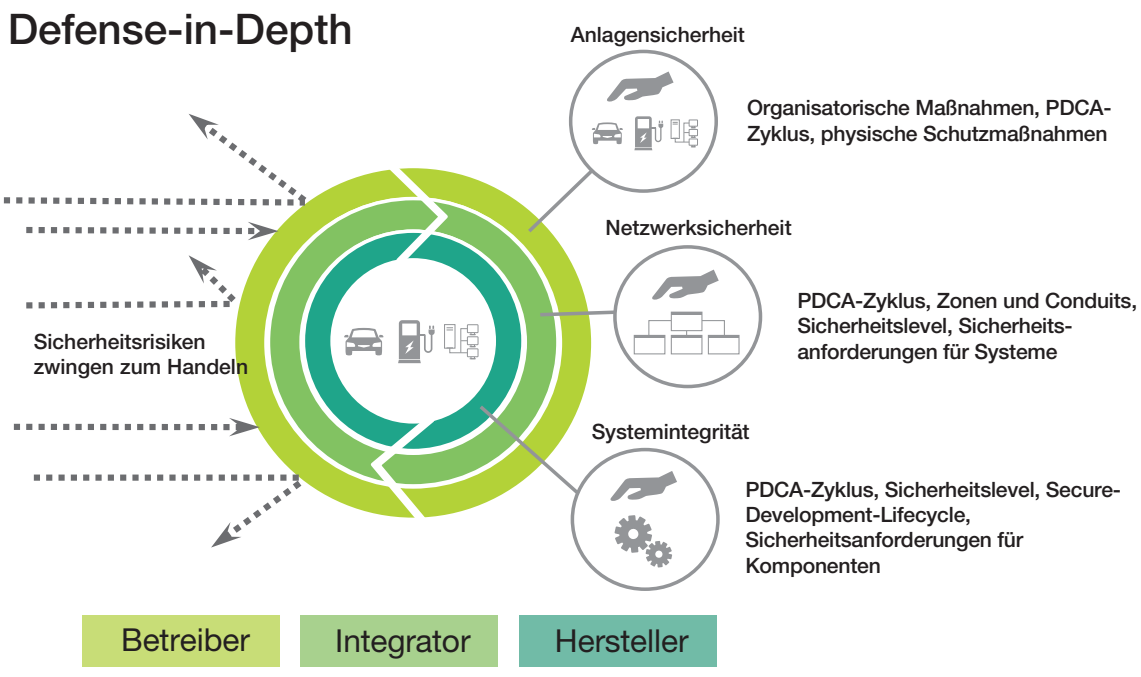
Die Elektromobilität ist mit Elektrofahrzeugen, Ladeinfrastruktur und Backend-Systemen ein verteiltes Ökosystem. Eine Vielzahl von Akteuren ist am Lade- und Abrechnungsvorgang und der Komponentenentwicklung beteiligt. Für den vorhandenen Kommunikationsbedarf der Akteure ist es notwendig eine den Anforderungen entsprechende IKT-Infrastruktur aufzubauen und insbesondere IT-Sicherheits-Aspekte einzubeziehen, da Elektrofahrzeuge, Ladeinfrastruktur und Backend-Systeme in Zukunft als Teil der kritischen Infrastruktur „Energie“ zu sehen sind.

Aus dem Bereich der Industrieautomation bietet sich die Normenreihe IEC 62443 für eine Analyse an. Sie beschreibt Sicherheitskonzepte, Verfahren und Sicherheitsanforderungen und verfolgt einen ganzheitlichen Ansatz, der sowohl technische als auch organisatorische Maßnahmen beinhaltet. Grundlegende Eigenschaften der IT-Sicherheit werden darin widergespiegelt:

- IT-Sicherheit ist nicht durch eine einzelne Maßnahme zu erreichen (Defense-in-Depth)
- IT-Sicherheit ist ein Prozess, der fortlaufende Anpassungen benötigt (PDCA-Zyklus)
- IT-Sicherheit muss von Beginn an in der Produkt- und Systementwicklung berücksichtigt werden (PDCA-Zyklus, Sicherheitslevel)

Die betrachteten Grundkonzepte der IEC 62443 setzten diese Eigenschaften auf unterschiedliche Weise um. Durch ihren grundlegenden Charakter sind diese Konzepte auch für die Elektromobilität und das Laden von Elektrofahrzeugen zu empfehlen. Am Beispiel der „Identifikation und Authentifizierung“ wird gezeigt, wie allgemeine Sicherheitsanforderungen zu System- und Komponentenanforderungen heruntergebrochen werden können. Mit dieser Methodik ist es möglich einen Anforderungskatalog zu erstellen. Eine vollständige Übertragung der Anforderungen von der Industrieautomation auf die Elektromobilität ist jedoch aufgrund unterschiedlicher Rahmenbedingungen nicht möglich. Eine Anpassung der Anforderungen mit vorheriger Bedrohungs- und Risikoanalyse ist zu empfehlen.

Das Sicherheitskonzept der „Defense-in-Depth“ eignet sich Grundlage für ein ganzheitliches Schutzkonzept. Darin können weitere Sicherheitskonzepte integriert werden. Beispielhaft wird eine Zuordnung von Maßnahmen für Anlagensicherheit, Netzwerksicherheit und Systemintegrität jeweils zu Elektrofahrzeug, Ladeinfrastruktur und Backend-Systeme vorgenommen.



Ganzheitliches Sicherheitskonzept der „Defense-in-Depth“ für das Laden und Abrechnen in der Elektromobilität

Abschließend wird empfohlen die Umsetzung der grundlegenden Sicherheitskonzepte aus IEC 62443 und die Anpassung der System- und Komponentenanforderungen für die Elektromobilität in nachfolgenden Aktivitäten zu behandeln. Das Ziel sollte sein, konkrete Anwendungshinweise für alle im Ökosystem „Elektromobilität“ beteiligten Akteure zu entwickeln. Diese Hinweise müssen neben den technischen Sicherheitsanforderungen auch organisatorische Anforderungen gemäß den System-, Komponenten- und Prozessanforderungen der IEC 62443 enthalten. Zusätzlich muss dabei besonders auf spezifische Anforderungen für das Laden von Elektrofahrzeugen geachtet werden. Dazu zählen u. a. der Datenschutz (Vertraulichkeit), die Eichrechtskonformität und die Auswirkung der IT-Sicherheit auf safety-relevante Funktionen.

Für die Erstellung eines umfassenden Anforderungskatalogs sollte jedoch nicht nur IEC 62443 betrachtet werden. Für den Bereich der Energieversorgung beschreibt die IEC 62351 Lösungen, die zur Erfüllung der Anforderungen aus IEC 62443 herangezogen werden können.

1 Einleitung

1.1 Motivation

Für die Elektromobilität und im Speziellen für die Ladeinfrastruktur wurde bisher der Aspekt der IT-Sicherheit normativ kaum behandelt. Mit dem Elektrofahrzeug, der Ladeinfrastruktur und verschiedensten Backend-Systemen sind eine Vielzahl von Akteuren am Lade- und Abrechnungsvorgang beteiligt. Abb. 1 zeigt das Ökosystem „Elektromobilität“ schematisch. Um dieses System aufzubauen und den dort vorhandenen Kommunikationsbedarf der Akteure nachzukommen, ist es notwendig eine den Anforderungen entsprechende IKT-Infrastruktur zu entwickeln. Der Gewährleistung einer angemessenen IT-Sicherheit kommt dabei eine hohe Bedeutung zu: Auf der einen Seite gilt es für die personenbezogenen bzw. personenbeziehbaren Daten, die beim Lade- und Abrechnungsvorgang erfasst, verarbeitet und zwischen den Beteiligten kommuniziert werden, einen adäquaten Datenschutz zu implementieren [1]. Auf der anderen Seite muss eine große Anzahl an Elektrofahrzeugen in Zukunft als Teil der kritischen Infrastruktur[1] „Energie“ betrachtet werden. Der Schutz der kritischen Infrastrukturen gegen Cyberangriffe ist bereits heute eines der wichtigsten Ziele jeder Industrienation. Um eine Einhaltung von IT-Sicherheits-Mindeststandards zu gewährleisten, wurde im Jahr 2015 das IT-Sicherheitsgesetz [2] verabschiedet. Dieses gilt insbesondere für Betreiber von kritischen Infrastrukturen, im Bereich der Elektromobilität entspricht das sowohl den Elektrofahrzeugen, als auch der Ladeinfrastruktur und den Backend-Systemen.

Abb. 1: Schematische Darstellung des Ökosystems „Elektromobilität“

Für die Elektromobilität stellt sich daher die Frage, ob man sich ein eigenes Regelwerk zur IT-Sicherheit geben sollte oder ob man auf vorhandene Regelwerke aufsetzen kann. In der Industrieautomatisierung hat seit einigen Jahren die Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ eine zentrale Rolle für die IT-Sicherheit eingenommen und diente bereits für andere Domänen wie z. B. im Bahnbereich (DIN VDE V 0831-104 [3]) und Smart Home (VDE-AR-E 2849-1 [4]) als Basis für eine umfassende Betrachtung der IT-Sicherheit. Daher soll nicht eine eigenständige Vorgehensweise zur IT-Sicherheit für die Elektromobilität erstellt werden, sondern die Vorgehensweise nach IEC 62443 herangezogen und auf eine mögliche Übertragbarkeit untersucht werden, um passende Schutzkonzepte und Sicherheitsanforderungen zu entwickeln.

[1] Nach EU-Richtlinie 2008/114/EG ist eine kritische Infrastruktur eine Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Staat hätte, da diese Funktionen nicht aufrechterhalten werden könnten [5].

1.2 Ziel der Übertragbarkeitsanalyse

Das Ziel der Übertragbarkeitsanalyse der Normenreihe IEC 62443 ist es einen ersten Überblick zu verschaffen, welche Schutzkonzepte auch für eine Anwendung in der Elektromobilität und dem Laden von Elektrofahrzeugen zu empfehlen und welche Akteure dabei beteiligt sind. Ausgehend von den Grundkonzepten ist die Methodik zur Ableitung von System- und Komponentenanforderungen vorgestellt und anhand eines Beispiels erläutert. Sie richtet sich in erster Linie an Automobilhersteller, Hersteller und Betreiber von Ladeinfrastruktur und Backend-Systemen, sowie alle im Umfeld des Laden und Abrechnen von Elektrofahrzeugen beteiligten Akteure.

1.3 Vorgehensweise

Die weitere Vorgehensweise ist in mehrere Schritte unterteilt (Abb. 2). Nach der Einleitung in Kapitel 1, Begriffsdefinitionen in Kapitel 2 und einer Einführung in die IEC 62443 Normenreihe in Kapitel 3 sind in Kapitel 4 die für den Betrachtungsbereich relevanten Schutzziele ermittelt. Aus Sicht der Industrieautomation sind die relevanten Schutzziele in der Normenreihe IEC 62443 beschrieben. Für den Bereich der Elektromobilität sind Studien und Projekte betrachtet. Anschließend wird der Frage nachgegangen, ob es übereinstimmende Schutzziele zur Industrieautomation gibt und ob die dort angewandten allgemeinen Schutzkonzepte zur Erreichung der Schutzziele auch für die Elektromobilität sinnvoll umgesetzt werden können. Dies geschieht im 2. Schritt „Analysieren der Grundkonzepte“ der IEC 62443 (Kapitel 5). Ausgehend von den Grundkonzepten und den involvierten Schutzmaßnahmen sind in Schritt 3 die Sicherheitsanforderungen für Systeme (Kapitel 6) und Produkte (Kapitel 7) untersucht. In Schritt 4 ist ein erster grober Entwurf beschrieben, der die bisherigen gewonnen Erkenntnissen aus IEC 62443 in einem ganzheitlichen Schutzkonzept für die Elektromobilität dargestellt (Kapitel 8). Abschließend ist in Kapitel 9 ein Fazit der betrachteten Grundkonzepte und des entworfenen Schutzkonzeptes dargelegt.

Abb. 2: Vorgehensweise zur Übertragbarkeit der IEC 62443 in die Elektromobilität

2 Begriffsdefinitionen

Für den weiteren Verlauf der Analyse sind Sicherheitsbegriffe zu definieren. Damit lassen sich verschiedene Schutzarten unterscheiden, insbesondere da im Deutschen aus dem Begriff „Sicherheit“ nicht immer genau hervorgeht welcher „Art“ der Sicherheit gemeint ist.

Funktionale Sicherheit (engl. *safety*). Eigenschaft eines Systems ordnungsgemäß unter allen Betriebsbedingungen zu funktionieren und eine Gefahr für Mensch und Umwelt zu minimieren [6].

Informationssicherheit[2] (engl. *security*). Eigenschaft eines Systems nur Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen [6].

Datensicherheit (engl. *protection)*. Eigenschaft eines Systems nur Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und auf Daten führen [6].

Datenschutz (engl. *privacy*). Fähigkeit einer natürlichen Person die Weitergabe von persönlichen Informationen zu kontrollieren [8].

Sicherheitslevel (engl. *security level*). Level, das der erforderlichen Wirksamkeit von Gegenmaß-nahmen und den Sicherheitseigenschaften von Geräten und Systemen entspricht, basierend auf der Risikobewertung [9].

Reifegrad (engl. *maturity level*). Fähigkeit organisatorische Maßnahmen und Prozesse nach dem sogenannten CMMI[3] aktiv zu „leben“.

Schutzlevel (engl. *protection level*). Kombination aus Sicherheitslevel und Reifegrad, die dem tatsächlichen Schutz entspricht [10].

[2] Der Begriff Informationssicherheit statt IT-Sicherheit ist umfassender und wird deshalb mittlerweile zunehmend verwendet. In der Literatur befindet sich jedoch noch überwiegend der Begriff „IT-Sicherheit“. Viele Texte werden aber schrittweise auf die Betrachtung von Informationssicherheit ausgerichtet. Zusätzlich wird das Aktionsfeld der IT-Sicherheit unter dem Begriff „Cyber-Sicherheit“ auf den gesamten Cyberraum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik. [7]

[3] Das Capability Maturity Model Integration, kurz CMMI, ist eine Familie von Referenzmodellen für unterschiedliche Anwendungsgebiete und bietet eine systematische Aufbereitung bewährter Praktiken, um die Verbesserung einer Organisation zu unterstützen.

3 Einführung in die IEC 62443 Normenreihe

3.1 Zielsetzung der IEC 62443 Normenreihe

Die Normenreihe IEC 62443 hat ihren Ursprung in der Automatisierungstechnik der Prozessindustrie, deckt aber mit ihrem Anwendungsbereich alle Industriebereiche und die kritischen Infrastrukturen ab. Sie befasst sich mit der IT-Sicherheit sogenannter ,,Industrial Automation and Control Systems“ (kurz: IACS). Der Begriff IACS beschreibt alle Bestandteile, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind. Dazu gehören sowohl Hardware- als auch Softwarekomponenten. Des Weiteren schließen IACS die organisatorischen Prozesse für die Errichtung und den Betrieb mit ein.

Die Zielsetzung ist Normen, Verfahren, technische Reports und zusätzliche Informationen zur Verfügung zu stellen, die Prozesse für eine sichere Implementierung von IACS definieren. Dies soll eine Hilfestellung für alle darstellen, die für Design, Implementierung, Management, Herstellung und Betrieb von IACS verantwortlich sind. Auch sollen Anwender, Integratoren, Hersteller und Verkäufer adressiert werden.

Im Fokus steht die Verbesserung der Integrität und Verfügbarkeit von Komponenten und Systemen und das zur Verfügung stellen von Kriterien zur sicheren Bereitstellung und Implementierung von IACS. Die Einhaltung dieser Leitfäden soll die Sicherheit in der Produktion und der Komponenten und Systeme verbessern und soll helfen Schwachstellen zu identifizieren und zu adressieren. Damit kann das Risiko von kompromittierten Informationen oder Produktionsausfällen stark reduziert werden.

3.2 Struktur der IEC 62443 Normenreihe

Die Normenreihe IEC 62443 kann grundsätzlich in vier Bereiche eingeteilt werden, die jeweils mehrere Dokumente beinhalten. Abb. 3 zeigt die verschiedenen Bereiche mit den dazugehörigen Normenteilen und Spezifikationen.

Der erste allgemeine Bereich beschreibt übergeordnete Aspekte wie Terminologien und Methoden, aber auch Messgrößen zur Bestimmung der Konformität. In Kapitel 5 sind einige Grundkonzepte aus diesem Bereich beschrieben und für eine Übertragbarkeit in die Elektromobilität untersucht.

Der zweite Bereich definiert Leitlinien und Leitfäden für eine Umsetzung von organisatorischen Maßnahmen und gibt Empfehlungen für ein Patch-Management. Die organisatorischen Maßnahmen aus den Teilen der IEC 62443-2 sind nicht Teile dieser Übertragbarkeitsanalyse.

Der dritte Bereich behandelt im Vergleich zu den beiden bereits beschriebenen Bereichen technische Aspekte. Sicherheitstechnologien, Risikoanalyse, Sicherheitslevel und Sicherheitsanforderungen sind definiert, die hilfreich sind um ein möglichst sicheres System zu erreichen. In Kapitel 6 sind Sicherheitsanforderungen aus diesem Bereich erläutert.

Der vierte und letzte Bereich der Normenreihe IEC 62442 behandelt die Komponenten-Ebene. Dort werden Anforderungen an die Produktentwicklung und an Komponenten festgelegt. In Kapitel 7 sind diese Anforderungen näher beschrieben.

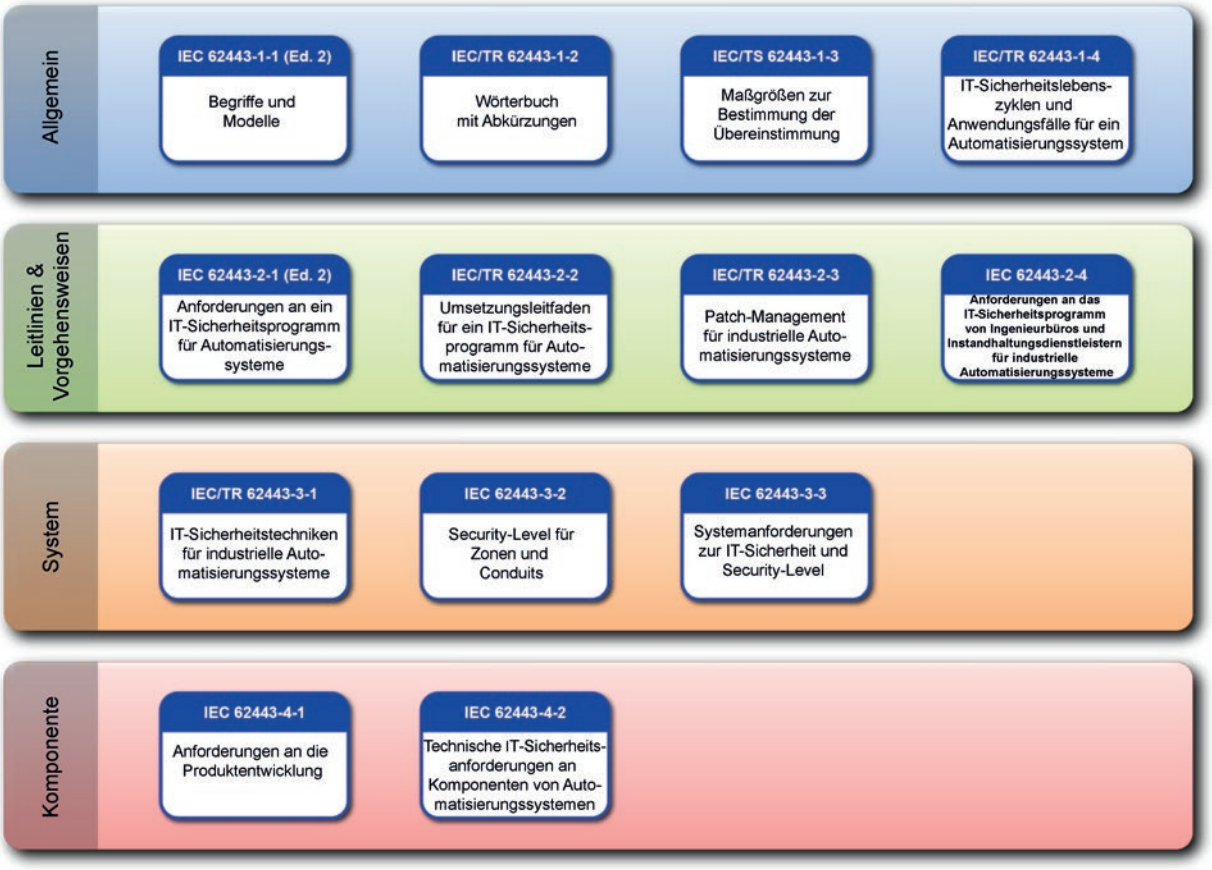


Abb. 3: Aufbau der Normenreihe IEC 62443 nach [11]

4 Schutzziele in der Industrieautomatisierung und Elektromobilität

4.1 Schutzziele in der IT-Sicherheit

In der IT-Sicherheit werden drei allgemeine Schutzziele definiert [6]:

Vertraulichkeit: Daten dürfen nur von autorisierten Benutzern bearbeitet werden

Integrität: Daten dürfen nicht unbemerkt verändert werden

Verfügbarkeit: der autorisierte Zugriff auf Daten muss gewährleistet sein

Diese Ziele sind die Grundlage für die weitere Betrachtung in den Bereichen Industrieautomatisierung und Elektromobilität. Es gilt festzustellen, ob diese Schutzziele übereinstimmen oder ob es Abweichungen gibt. Bei einer Übereinstimmung ist es sinnvoll die Grundkonzepte und tiefergehende Sicherheitsstrategien für eine Übertragbarkeit zu untersuchen. Bei Abweichungen ist festzustellen in wie weit dadurch Grundkonzepte nicht anwendbar sind und welche Alternativen es gibt.

4.2 Schutzziele in der Industrieautomatisierung

Die IT-Sicherheit im Bereich der Industrieautomatisierung hat den Schwerpunkt Produktionsanlagen vor gewollten und ungewollten Missbrauch durch Cyberangriffe zu schützen. Vorrangiges Ziel ist es die **Verfügbarkeit** und **Integrität** der Anlage zu gewährleisten. Es muss sichergestellt sein, dass die Produktion aufrechterhalten bleibt, auch wenn die Anlage durch Fehlhandlungen oder Angriffe beeinträchtigt wird. Der Schutz von Informationen gegen Datendiebstahl steht oft nicht im Vordergrund, obwohl auch vertrauliche Daten bearbeitet werden. Für diese Priorität der Ziele wurde der Begriff „Industrial Security“ eingeführt, um sich von der Office-IT zu unterscheiden [9]. Abb. 4 zeigt die Priorisierung der Schutzziele in der Office-IT und Produktions-IT bzw. „Industrial Security“.

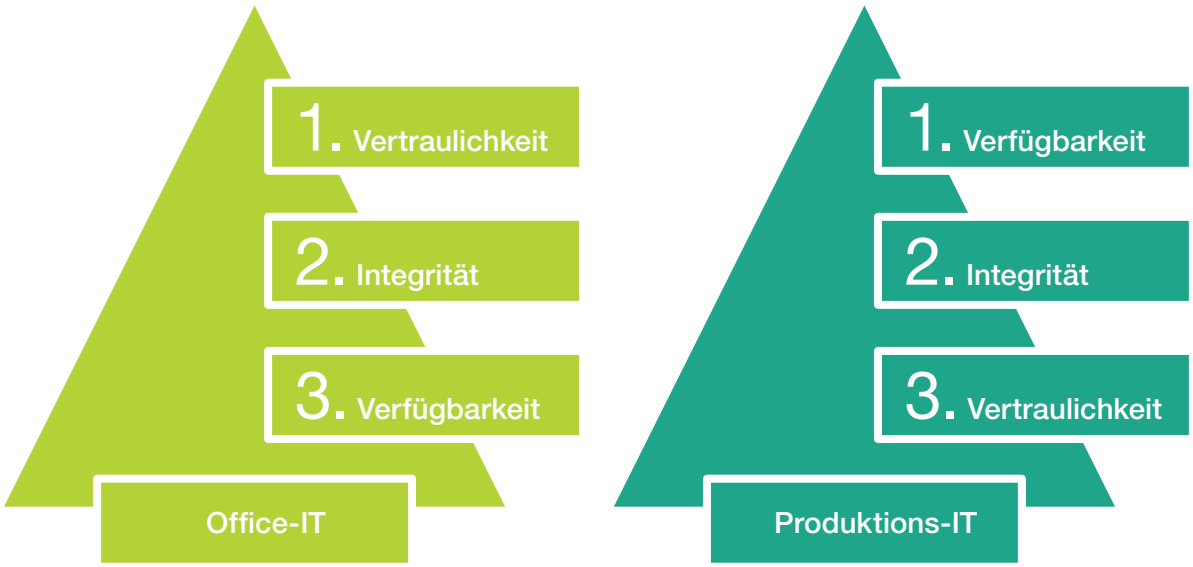


Abb. 4: Priorisierung der Schutzziele in der Office-IT und Produktions-IT

4.3 Schutzziele für das Laden und Abrechnen in der Elektromobilität

Elektrofahrzeuge werden in Zukunft in hohem Ausmaß mit ihrer Umgebung kommunizieren. Insbesondere beim Lade- und Abrechnungsvorgang wird nicht nur Energie transferiert, sondern es kommt auch zu einem umfangreichen Austausch von Daten. Durch die Einbindung dieser Fahrzeuge in das intelligente Stromnetz[4] werden diese zu einem Teil der kritischen Infrastruktur „Energie". Die Energieversorgung ist ein zentraler Bereich Kritischer Infrastrukturen, der sich im Fall von Ausfällen oder Störungen extrem und unmittelbar auch auf die anderen Sektoren der Kritischen Infrastrukturen und somit auf Staat, Wirtschaft und Gesellschaft auswirkt [12]. Im Falle einer kompromittierten Ladeinfrastruktur mit zahlreichen angeschlossen Elektrofahrzeugen können synchrone Lastabwürfe oder –aufnahmen Auswirkungen auf das Stromnetz haben. Das macht die **Integrität** und die **Verfügbarkeit** zu einem sehr wichtigen Schutzziel.

Mit dem Elektrofahrzeug, der Ladeinfrastruktur und verschiedensten Backend-Systemen sind eine Vielzahl von Akteuren beim Lade- und Abrechnungsvorgang beteiligt. Dabei werden auch personenbezogene und personenbeziehbare Daten erfasst, verarbeitet und zwischen den Beteiligten kommuniziert. Diese Daten müssen hinsichtlich Datensicherheit, Datenschutz und **Vertraulichkeit** entsprechend abgesichert sein und diese Aspekte sind grundlegend und übergreifend sicherzustellen, damit die Elektromobilität eine breite Akzeptanz erfährt [1].

Eine Priorisierung der Schutzziele für die Elektromobilität wird im Rahmen dieser Analyse nicht vorgenommen. Klar ist jedoch dass alle drei allgemeinen Schutzziele von Bedeutung sind (s. Abb. 5).

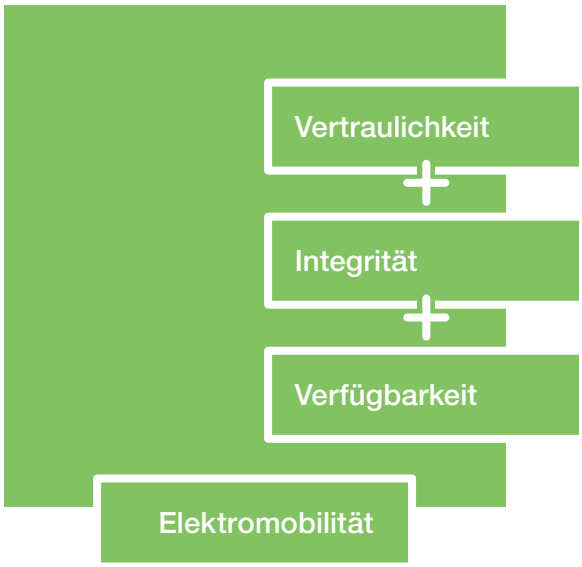


Abb. 5: Priorisierung der Schutzziele für das Laden und Abrechnen in der Elektromobilität

[4] Intelligente Stromnetze (engl. smart grids) umfassen die kommunikative Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen der Elektrizitätsversorgung. Das bedeutet, dass in einem Smart Grid nicht nur Energie sondern auch Daten transportiert werden. Ziel ist die Sicherstellung der Energieversorgung auf Basis eines effizienten und zuverlässigen Systembetriebs [13]. Das Smart Grid ist ein zentraler Bestandteil zur Umsetzung des Gesetzes zur Digitalisierung der Energiewende [14].

4.4 Relevanz der IEC 62443 für das Laden und Abrechen in der Elektromobilität

Mit den bekannten Schutzzielen in der Industrieautomatisierung und in der Elektromobilität kann nun ein Abgleich stattfinden. Eine Übersicht mit der Relevanz der Schutzziele zeigt Tabelle 1.

Schutzziele der IT-Sicherheit	Industrieautomatisierung	Elektromobilität
Vertraulichkeit	Datenvertraulichkeit kann ein Rolle spielen, jedoch steht der Datenschutz oft nicht im Vordergrund	Personenbezogene und personenbeziehbare Daten sind zu schützen
Integrität	Produktionsanlagen vor gewollten und ungewollten Missbrauch schützen	Elektrofahrzeuge, Ladesäulen und Backend-Systeme als Teil der Kritischen Infrastruktur sind vor gewollten und ungewollten Missbrauch zu schützen
Verfügbarkeit	Produktion muss aufrecht erhalten bleiben, auch wenn die Anlage durch einen Angriff beeinträchtigt ist	Elektrofahrzeuge, Ladesäulen und Backend-Systeme als Teil der Kritischen Infrastruktur erfordern einen autorisierten Zugriff auf Infrastruktur und Kommunikation

Tabelle 1: Übersicht der Relevanz von Schutzzielen in den Bereichen Industrieautomation und Elektronmobilität

In beiden Bereichen sind Verfügbarkeit und Integrität von sehr hoher Bedeutung. Mit dieser Übereinstimmung sind im weiteren Verlauf Schutzkonzepte, die in IEC 62443 diesbezüglich vorgeschlagen werden, für eine Übertragbarkeit in die Elektromobilität untersucht. Hingegen spielen Datenschutzaspekte, die in der Elektromobilität ebenso von hoher Relevanz sind, in der Industrieautomatisierung keine große Rolle. Die Normenreihe IEC 62443 legt den Fokus nicht auf die Vertraulichkeit und bietet aufgrund dessen keine expliziten Lösungsansätze dafür an.

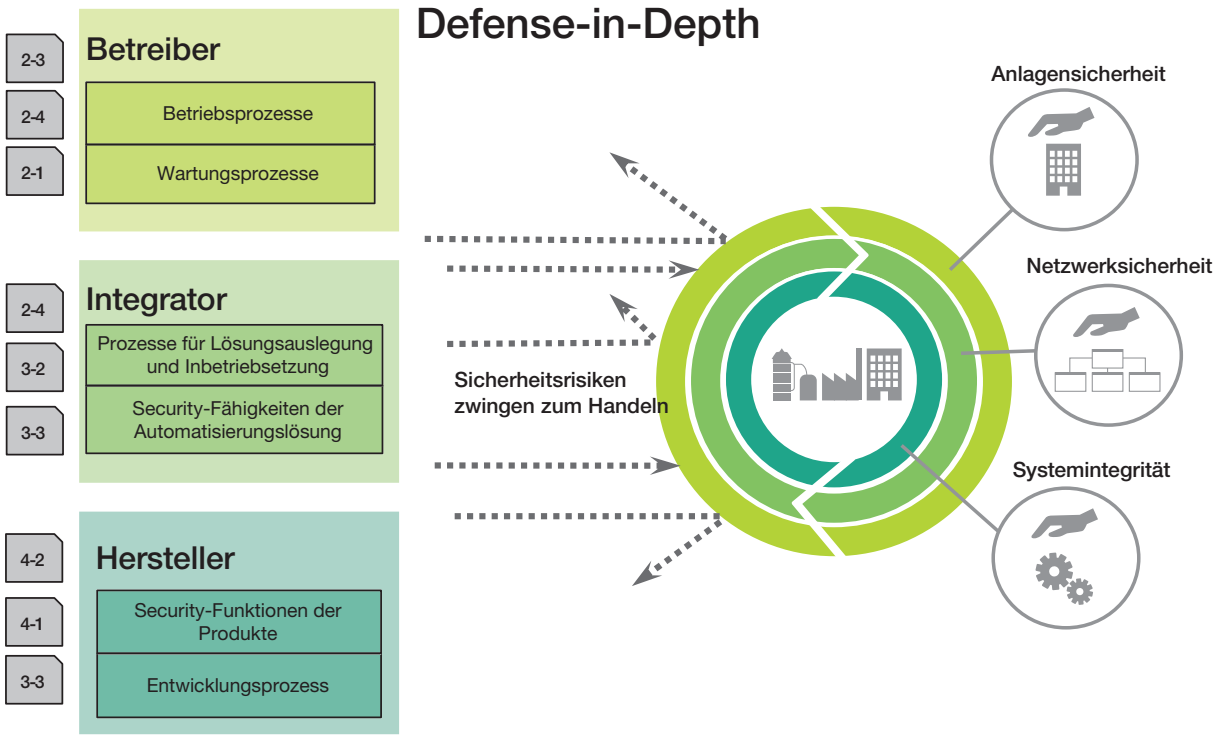
Bei der Analyse der IEC 62443 sind in den nächsten Kapiteln die Verfügbarkeit und die Integrität im Vordergrund. Auf Einhaltung der Vertraulichkeit wird in Kapitel 9 kurz eingegangen.

5 Grundkonzepte der IEC 62443

Die Normenreihe IEC 62443 beschreibt im Teil 1-1 allgemeine Grundkonzepte, die die Schutzziele Verfügbarkeit und Integrität berücksichtigen [9]. Im Folgenden sind einige Grundkonzepte grob beschrieben und abschließend eine Anwendung in der Elektromobilität analysiert.

5.1 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Dieses Grundkonzept beschreibt die Tatsache, dass der Schutz der Anlagen nicht nur mit einer einzigen Maßnahme erreicht werden kann. Ein umfassender Schutz ist nur möglich wenn alle Beteiligten ihren Beitrag dazu liefern. Die IEC 62443 beschreibt drei Basisrollen: Hersteller, Integrator und Betreiber. Abb. 6 zeigt die genannten Rollen mit ihren Aufgaben im Bereich der IACS und den entsprechenden relevanten Normenteilen.



„Defense-in-Depth“ involviert alle Beteiligten: Betreiber, Integrator, Hersteller

Abb. 6: Basisrollen und Aufgaben der IEC 62443 [10]

Für einen umfassenden Schutz müssen sämtliche Beteiligte eine abgestimmte und koordinierte Strategie umsetzen. Ein gutes Beispiel dafür sind Zwiebeln. Diese haben mehrere („gestaffelte“) Zwiebelschalen. Hat ein Angreifer eine Schale durchbrochen, steht er vor der Nächsten. Die Normenreihe IEC 62443 beschreibt wie diese Strategie im Bereich von industriellen Anlagen angewendet werden kann.

Als erste Schale und Grundvoraussetzung für alle nachfolgenden Schalen gilt, den Mitarbeiter für die Gefahren von Cyberangriffen zu sensibilisieren. Dazu gehören entsprechende Schulungen, aber auch klare Strukturen in der Organisation mit Rollen und Rechten. Neben diesen organisatorischen Maßnahmen, zählen auch der physische Schutz der Anlage sowie eine Zugangskontrolle zu den Grundvoraussetzungen für eine gestaffelte Verteidigung. Grundsätzlich ist es die Aufgabe des Betreibers diese Maßnahmen umzusetzen. Verteidigungsschalen, die der Integrator umsetzt, befinden sich auf der Netzwerk- oder Systemebene. Dazu zählen Maßnahmen wie z.B. die Auslegung von „Zonen und Conduits“ um geschützte Bereiche zu schaffen oder einen Zugriffsschutz mit Passwörtern zu installieren. Das Konzept der „Zonen und Conduits“ ist in Kapitel 5.2 näher beschrieben. In der inneren Verteidigungsschale sind die Geräte und Komponenten von Bedeutung. Sicherheitsfunktionen gehören zu den Maßnahmen, ebenso der kritische Blick auf den Entwicklungsprozess, in dem z. B. Risikoanalysen, Programmierrichtlinien und Codeanalysen durchgeführt werden. Diese Verteidigungsschale ist dem Hersteller zuzuordnen.

Das Konzept der tiefgestaffelten Verteidigung beschränkt sich jedoch nicht nur auf das Zusammenwirken der Beteiligten. Eine weitere Anwendung ist bspw. die Zugangsbeschränkung in einem eingebetteten Gerät. Wird die Zugangsbeschränkung überwunden, könnte durch ein rollenbasiertes Rechtemanagement der Zugang weiter eingeschränkt werden. Wird auch diese Schutzmaßnahme überwunden, könnte das System so ausgelegt sein, dass nur temporäre Daten verändert werden können.

5.2 Zonen und Conduits

Für große oder komplexe Systeme ist es oft nicht angebracht den gleichen Sicherheitslevel für alle Komponenten zu verwenden, da diese unterschiedliche Bedrohungen und Risiken aufweisen. Unterschiede können durch das Konzept der „Sicherheitszone" dargestellt werden. Eine Sicherheitszone ist eine logische Gruppierung von physikalischen Betrachtungsgegenständen, die die gleichen Sicherheitsanforderungen haben. Die Grenze der Sicherheitszone definiert welche Komponenten innerhalb und welche außerhalb der Zone liegen. Prinzipiell gibt es zwei Arten von Sicherheitszonen: Physikalische und virtuelle Zonen. Physikalische Zonen beziehen sich auf den Ort des Betrachtungsgegenstandes, während virtuelle Zonen sich auf den funktionalen Charakter beziehen.

In vernetzten Systemen können einzelne Komponenten meistens keine Funktionalität vollständig durchführen. Komponenten oder Teilsysteme sind auf Informationen von anderen angewiesen, die auch in unterschiedlichen Sicherheitszonen liegen können. Um den benötigten Informationsfluss in und aus einer Sicherheitszone zu gewährleisten, werden sogenannte Kommunikationsleitungen definiert. Diese Verbindungen zwischen Sicherheitszonen werden auch „Conduits" genannt und haben die Aufgabe die Kommunikation zu sichern. Eine Kommunikation außerhalb von Conduits ist dabei nicht zulässig.

Beim Entwurf von Zonen und Conduits sollten die Schutzziele und Sicherheitsanforderungen der Komponenten und bestenfalls die Architektur des Gesamtsystems bekannt sein, um eine sinnvolle Gruppierung zu definieren. Sowohl Zonen als auch Conduits werden mit verschiedenen Attributen definiert. Zum Beispiel vorhandene Sicherheitsrichtlinien, Zugangsanforderungen, Bedrohungen und Verwundbarkeit und Autorisierungstechnologie. Ein Beispiel für die Anwendung von Zonen und Conduits zeigt Abb. 7:

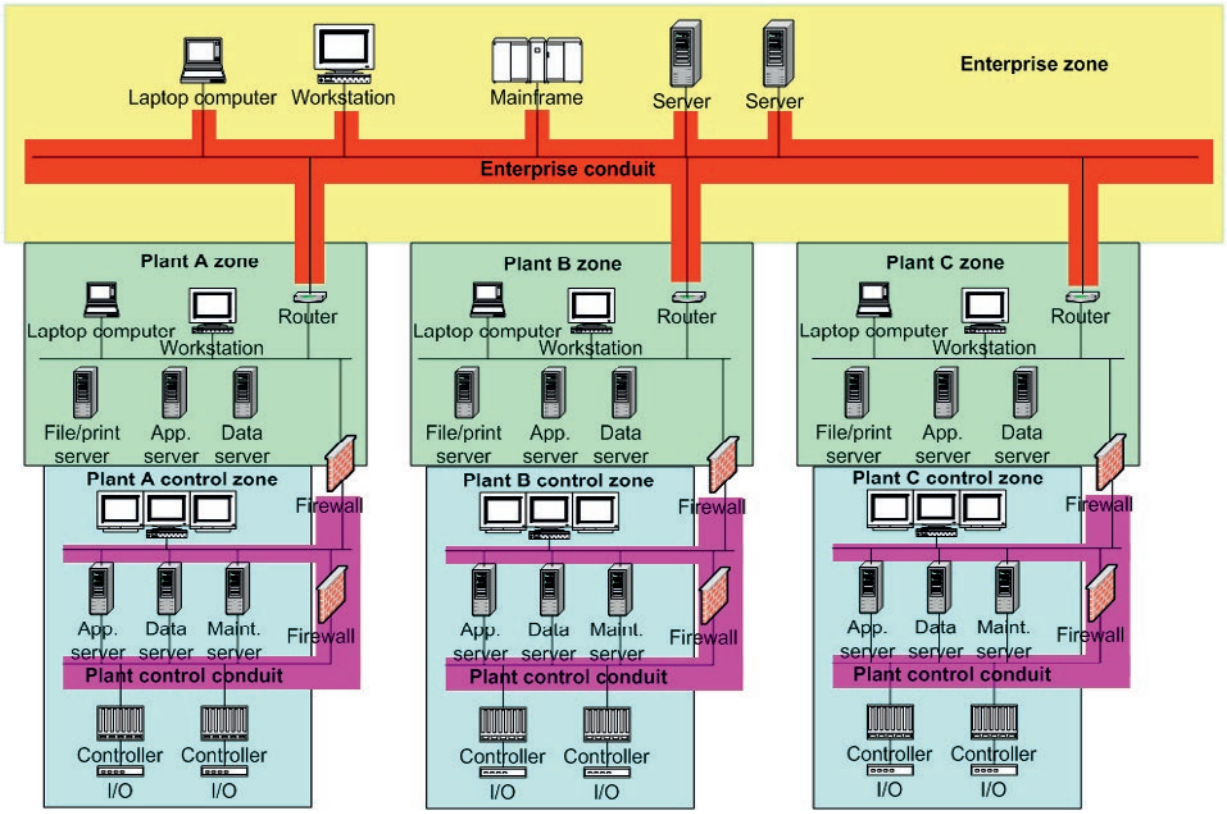


Abb. 7: Anwendung von Zonen und Conduits am Beispiel einer Organisation mit drei Fabriken [9]

Die drei Fabriken (in Abb. 7 mit Plant A, B und C bezeichnet) sind über das Unternehmens-Conduit zum einen mit der Zentrale und zum anderen gegenseitig verbunden. Die einzelnen Fabriken sind wiederum in zwei Zonen unterteilt, die über ein weiteres Conduit miteinander verbunden sind. Mit solch einer Einteilung kann der unterschiedliche Schutzbedarf von Zonen und Conduits mit entsprechenden Schutzmaßnahmen erfüllt werden. Gleichzeitig kann durch die Segmentierung und Verwendung von mehreren und unterschiedlichen Schutzmaßnahmen das Konzept der „Defense-in-Depth" realisiert werden.

5.3 Risikobewertung nach VDI/VDE 2182

Sicherheit ist kein statischer Zustand, der einmal erreicht wird und dann unverändert bleibt. Ständige Änderungen von Geschäftsprozessen, Infrastrukturen, rechtlichen Rahmenbedingungen, aber auch neue Angriffsmethoden oder Schwachstellen machen es unabdingbar IT-Sicherheit dauerhaft aufrechtzuerhalten und kontinuierlich zu verbessern. Um geeignete Schutzmaßnahmen gegen Cyberangriff ableiten zu können, müssen die Bedrohungen und Auswirkungen bei einem Angriff bewertet werden. Dies gilt für alle Beteiligten: Hersteller, Integratoren und Betreiber. Grundsätzlich gliedert sich dieser Prozess in vier Phasen, die zyklisch wiederholt werden [6]:

- Planen (Anforderungen und Risiken)
- Ausführung (Realisierung)
- Prüfen (Messung und Validierung)
- Anpassen (Verbesserung)

Diese Vorgehensweise wird auch als „Plan-Do-Check-Act" oder kurz PDCA-Zyklus[5] bezeichnet und wird von der Normenreihe IEC 62443 von allen Beteiligten vorausgesetzt [9]. Die Richtlinie VDI/VDE 2182 [15] beschreibt diesen Prozess detailliert und zeigt auch die Abhängigkeiten zwischen den Beteiligten auf. Eine prinzipielle Vorgehensweise zur Anwendung eines PDCA-Zyklus besteht nach der Richtlinie aus acht Schritten:

- Betrachtungsgegenstand identifizieren
- Bedrohungen analysieren
- Relevante Schutzziele ermitteln
- Risiken analysieren und bewerten
- Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten
- Schutzmaßnahmen auswählen
- Schutzmaßnahmen umsetzen
- Prozessaudit durchführen

Ordnet man diese Schritte zyklisch und für alle Beteiligten an, so ergibt sich die Darstellung in Abb. 8. Der Austausch zwischen den Beteiligten geschieht auf der einen Seite über die Vermittlung von Anforderungen und auf der anderen Seite über die Bereitstellung von Dokumentation.

[5] Der PDCA-Zyklus beschreibt einen iterativen vierphasigen Prozess zur Sicherung und Verbesserung der Qualität von Produkten, Systeme und Prozessen. [7]

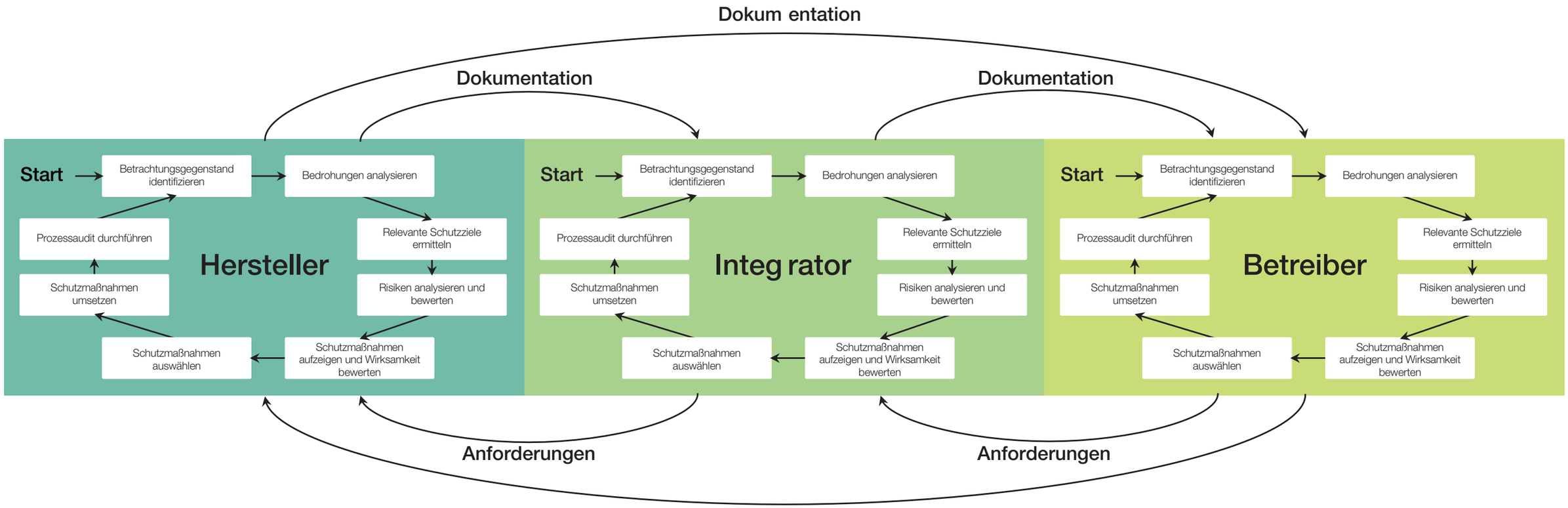


Abb. 8: IT-Sicherheits-Lebenszyklus nach VDI/VDE 2182-1 [15]

Für den Hersteller beginnt ein Zyklus mit den Eingangsinformationen bestehend aus Anforderungen des Integrators und Betreibers. Diese Anforderungen sind wiederum Ausgangsinformationen aus den Zyklen des Integrators und Betreibers. Darin müssen alle erforderlichen IT-Sicherheits-Funktionen und – Eigenschaften, sowie z.B. verwendete Protokolle und Anforderungen an die IT-Infrastruktur, enthalten sein. Nur damit ist der Hersteller in der Lage IT-Sicherheits-relevante Anforderungen von Beginn an in den Systemansätzen und der Produktentwicklung zu berücksichtigen (gemäß „Security-by-design“[6]) und während der Lebenszeit des Betrachtungsgegenstands einen fortlaufenden Support zu leisten.

Die Eingangsinformation für den Integrator sind IT-Sicherheitsanforderungen des Betreibers. Da IT-Sicherheitsanforderungen oft durch verschiedene Maßnahmen erfüllt werden können, müssen die PDCA-Zyklen des Integrators und des Betreibers in enger Zusammenarbeit erfolgen. Der Integrator muss alle relevanten Informationen für einen sicheren Betrieb dem Betreiber zur Verfügung stellen. Diese stellen die Eingangsinformationen für den Betreiber dar.

Der Betreiber ist für den sicheren Betrieb und Schutz des Betrachtungsgegenstands über den gesamten Lebenszyklus verantwortlich. Für Maßnahmen, die nur ein Betreiber umsetzen kann (vgl. Kapitel 5.1), kann durch eine veränderte Bedrohungslage eine Anpassung erforderlich sein. Wie für den Hersteller und den Integrator gilt auch für den Betreiber, den entsprechenden PDCA-Zyklus regelmäßig zu durchlaufen, um aktuellen Bedrohungen eine möglichst kleine Angriffsfläche zu bieten.

[6] Wenn bei der Entwicklung von Hard- wie Software bereits von Anfang an darauf geachtet wird, die Systeme so frei von Schwachstellen wie möglich und so unempfindlich gegen Angriffe wie möglich zu konzipieren, dann spricht man auch von „Security by design“.

5.4 Sicherheitslevels

Das Konzept der Sicherheitslevels wurde entworfen um einen qualitativen Ansatz zur Bestimmung des Schutzes einer Zone oder eines Conduits zur Verfügung zu haben. Im Gegensatz zur funktionalen Sicherheit ist die Komplexität jedoch wesentlich höher, da eine größere Anzahl an Faktoren Einfluss nehmen kann und Schutzmaßnahmen völlig unabhängig voneinander agieren können. Nach IEC 62443-1-1 sind z.B. die Effektivität von Schutzmaßnahmen und die Expertise und Ressourcen des Angreifers Faktoren, die einen Sicherheitslevel beeinflussen [9]. Mit diesen Faktoren werden vier Einstufungen des Sicherheitslevels (kurz SL) vorgenommen:

- SL1: Schutz gegen ungewollte, zufällige Angriffe
- SL2: Schutz gegen gewollte Angriffe mit einfachen Mitteln, niedrigen Aufwand, allgemeiner Expertise und niedriger Motivation
- SL3: Schutz gegen gewollte Angriffe mit fortgeschrittenen Mitteln, mittleren Aufwand, spezifischer Expertise und mittlerer Motivation
- SL4: Schutz gegen gewollte Angriffe mit fortgeschrittenen Mitteln, erheblichen Aufwand, spezifischer Expertise und hoher Motivation

Die unspezifischen Begriffe „niedrig“, „mittel“ etc. müssen dabei vom Betreiber für den jeweiligen Betrachtungsgegenstand definiert werden. Des Weiteren wird eine Ausprägung der genannten Sicherheitslevels definiert:

- **SL (target):** Ziel-Sicherheitslevels können für Zonen und Conduits während des zuvor beschriebenen PDCA-Zyklus ermittelt werden. Sie stellen den zu erreichenden Sicherheitslevel dar.

- **SL (achieved):** Erreichte Sicherheitslevels werden für Zonen und Conduits verwendet, um zu bewerten, ob die Sicherheitsmaßnahmen des Betrachtungsgegenstandes ihren Zweck und damit die Vorgaben des Ziel-Sicherheitslevels erfüllen. Man muss beachten, dass der erreichte Sicherheitslevel mit der Zeit abnimmt. Die Gründe sind u.a. eine Verschlechterung der Sicherheitsmaßnahmen, neue Schwachstellen, angepasste Bedrohungen oder Angriffsmethoden.

- **SL (capability):** Erreichbare Sicherheitslevels werden für Produkte und Systeme verwendet und stellen den maximalen Level dar, der unter der Verwendung von Sicherheitsmaßnahmen und –funktionen erreicht werden kann. In Kapitel 6 Sicherheitsanforderungen werden diese mit erreichbaren Sicherheitslevels verknüpft.

Der Zusammenhang zwischen den verschiedenen Ausprägungen der Sicherheitslevel lässt sich folgendermaßen darstellen (Abb. 9):

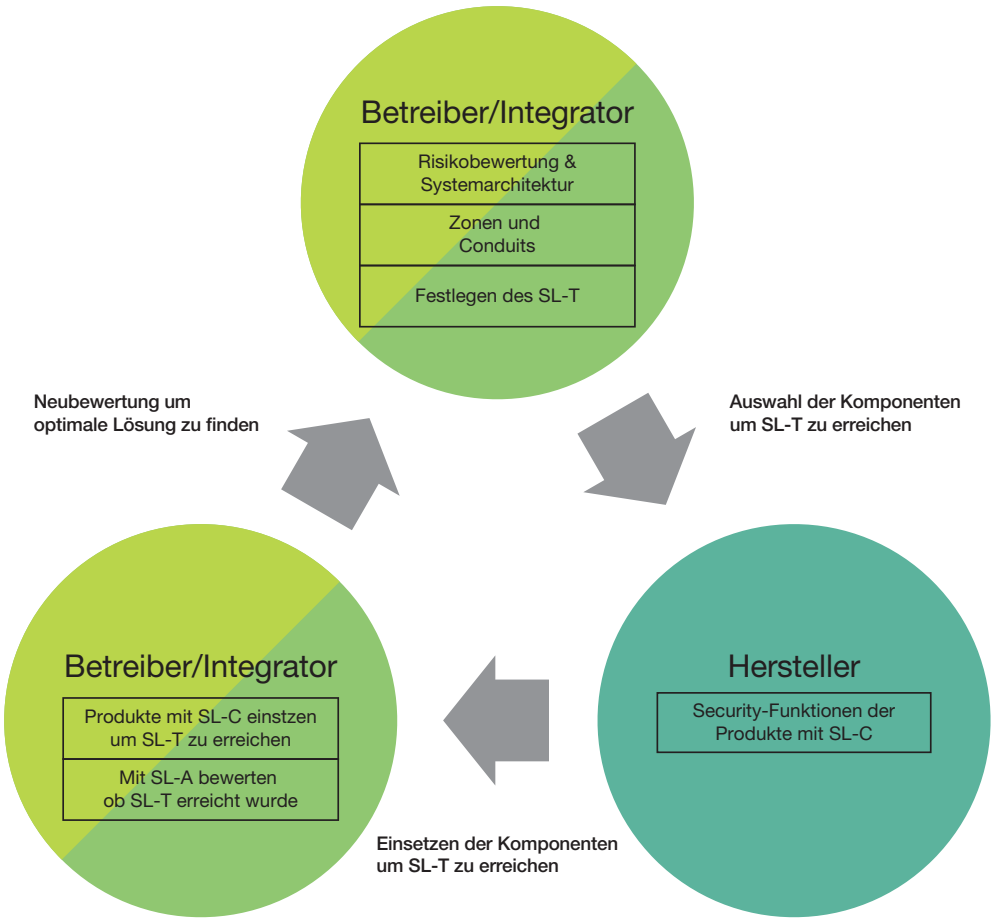


Abb. 9: Iterativer Prozess zur Findung der optimalen Sicherheitslösung (vgl. Kapitel 5.3)

Nach einer durchgeführten Risikobewertung und mit einer definierten Systemarchitektur und Zonen und Conduits kann der zu erreichende Sicherheitslevel SL-T vom Betreiber oder Integrator ermittelt werden. Mit dem SL-T kann nun die Auswahl der Komponenten und Produkte für den Betrachtungsgegenstand ausgeführt werden. Jede dieser Komponenten und Produkte hat dabei einen vom Hersteller festgelegten erreichbaren Sicherheitslevel SL-C. Mit dem Einsetzen der ausgewählten Komponenten kann anschließend der Betreiber oder Integrator die Erfüllung des SL-T überprüfen. Das Ergebnis dieser Überprüfung ist der erreichte Sicherheitslevel SL-A. Ändert sich mit der Zeit die Bedrohungslage des Betrachtungsgegenstandes ist mit Hilfe des in Kapitel 5.3. beschrieben PDCA-Zyklus eine erneute Risikobewertung und ggfs. eine Anpassung der Systemarchitektur notwendig. Das kann dazu führen, dass andere oder neue Komponenten eingesetzt werden müssen.

5.5 Zusammenfassung

Die vier beschriebenen Grundkonzepte bedienen unterschiedliche Ebenen der Sicherheit. Das Konzept der „Defense-in-Depth“ zielt auf eine sehr hohe und grundlegende Ebene ab. Im Gegensatz dazu ist das Zonen und Conduits Konzept auf einer niedrigeren Ebene (Systemebene) zu finden und umzusetzen. Alle Konzepte sind prinzipiell nicht nur einer Domäne zuzuordnen, sondern bilden eine solide Basis bei der Betrachtung von IT-Sicherheit in informationstechnischen Systemen, Anlagen und Prozessen.

Die „Defense-in-Depth“-Strategie adressiert eines der wichtigsten Merkmale bei der Betrachtung von IT-Sicherheit: eine Schutzmaßnahme allein ist nicht ausreichend. Abb. 10 zeigt das Konzept der „Defense-in-Depth“ mit möglichen Maßnahmen und Sicherheitskonzepten für die jeweiligen Schalen. Zu beachten ist, dass insbesondere der PDCA-Zyklus nicht nur für die IT-Sicherheit in der Produktion oder Fertigung (Systemintegrität) anwendbar ist, sondern auch für Geschäftsprozesse und organisatorische Maßnahmen (Anlagensicherheit) und die IT-Infrastruktur (Netzwerksicherheit) [7]. Der PDCA-Zyklus deckt damit ein weiteres wichtiges Merkmal bei der Betrachtung von IT-Sicherheit ab: Security ist ein Prozess. Das Konzept der Zonen und Conduits kann als Verfeinerung der „Defense-in-Depth“-Strategie in der Netzwerk- bzw. Systemebene gesehen werden (vgl. Kapitel 5.2). Die Sicherheitslevel und die grundlegenden Anforderungen (siehe Kapitel 6.1) und den daraus abgeleiteten Sicherheitsanforderungen für Systeme (siehe Kapitel 6) und Komponenten (siehe Kapitel 7) sind der Netzwerksicherheit bzw. der Systemintegrität zuzuordnen. Damit zeigt sich, dass die „Defense-in-Depth“-Strategie durch alle anderen Sicherheitskonzepte unterstützt wird und sich als Grundlage für detailliertere Betrachtungen anbietet.

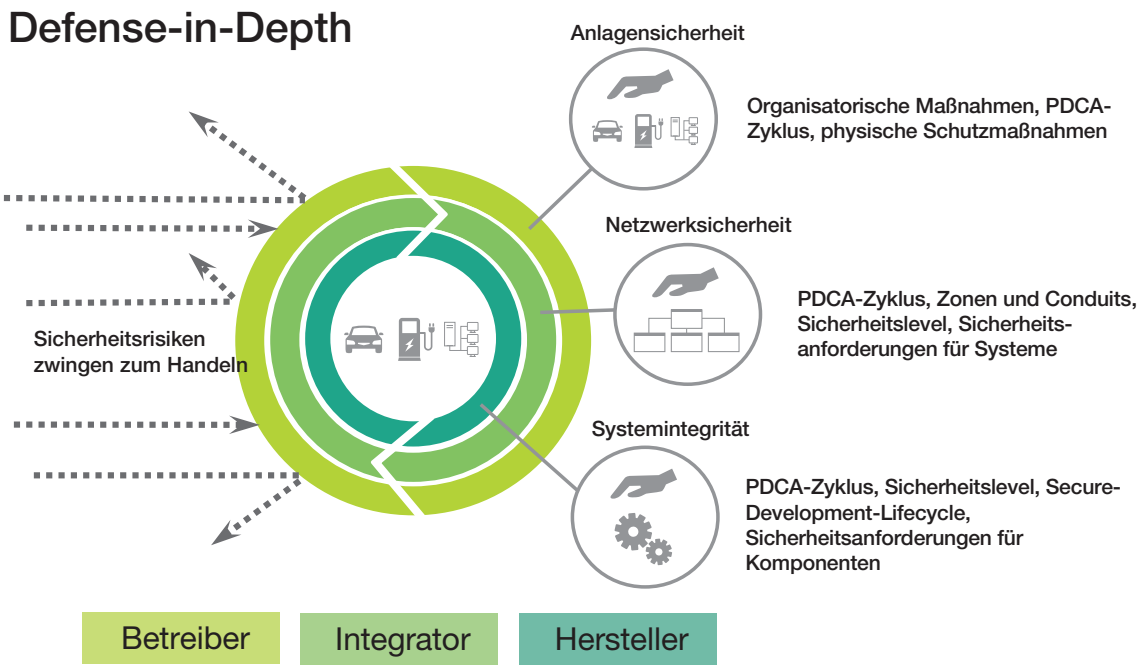


Abb. 10: Die „Defense-in-Depth“-Strategie mit möglichen Schutzmaßnahmen für die jeweiligen Schalen

Die betrachteten Grundkonzepte sind zwar für eine Anwendung in der Industrieautomation in Teil 1-1 der IEC 62443 beschrieben, aber durch ihren grundlegenden Charakter für die Betrachtung der IT-Sicherheit auch für andere Domänen zu empfehlen. Für die Elektromobilität mit ihren verteilten Systemen und Funktionalitäten in Fahrzeug, Ladeinfrastruktur und Backend-Systemen eignet sich die Aufteilung in Zonen und Conduits besonders gut. Jede Zone kann so gestaltet werden, wie es die Bedrohungs- und Risikoanalyse erfordert. In Anlehnung an Abb. 1 ist eine Zuordnung von Rollen zu Zonen möglich.

Die prinzipielle Anwendbarkeit der Grundkonzepte und insbesondere eine vollständige Umsetzung aller Konzepte können jedoch zu erheblichen finanziellen Kosten führen. Gerade für neue Geschäftsmodelle und für das sich entwickelnde Ökosystem der Elektromobilität ist es deshalb wichtig, von Beginn an Security-by-Design zu berücksichtigen und umzusetzen. Damit kann man die Sicherheit erreichen, die nötig ist, und verhindert wirkungslose Investitionen.

6 Sicherheitsanforderungen für Systeme

6.1 Allgemeine Vorgehensweise

Sicherheitsanforderungen für Systeme richten sich vor allem an Integratoren und Hersteller (vgl. Abb. 6). Diese setzen die Anforderungen mit technischen Maßnahmen um. Im Folgenden wird zunächst die allgemeine Vorgehensweise nach IEC 62443-3-3 erläutert und anschließend eine Sicherheitsanforderung beispielhaft beschrieben.

Die in Kapitel 5.4 eingeführten Sicherheitslevels und deren Ausprägung bieten einen ersten qualitativen Ansatz zur Bestimmung des Schutzes des Betrachtungsgegenstandes oder auch Teilen davon. Um diesen Ansatz der Sicherheitslevels umzusetzen sind im Teil 1-1 der IEC 62443 sogenannte grundlegende Anforderungen (FR, en: foundational requirements) festgelegt [9]:

- FR 1 – Identifizierung und Authentifizierung (IAC, *en: identification and authentification control*)
- FR 2 – Nutzungskontrolle (UC, *en: use control*)
- FR 3 – Systemintegrität (SI, *en:system integrity*)
- FR 4 – Vertraulichkeit der Daten (DC, *en: data confidentiality*)
- FR 5 – Eingeschränkter Datenfluss (RDF, *en: restricted data flow*)
- FR 6 – Rechtzeitige Reaktion auf Ereignisse (TRE, *en: timely response to events*)
- FR 7 – Verfügbarkeit der Ressourcen (RA, *resource availability*)

Diese sieben Anforderungen bilden die Grundlage für die erreichbaren Sicherheitslevels (SL-C) des Betrachtungsgegenstandes. Daraus lassen sich anhand festgelegter Zonen und Conduits zu erreichende Sicherheitslevels (SL-T) entwickeln. Die grundlegenden Anforderungen werden durch technische Systemanforderungen (SR, *en: system requirements*) und erweiterte Anforderungen (RE, *en: requirements enhancements*) weiter detailliert. Beim Umsetzen dieser Systemanforderungen durch Sicherheitsmaßnahmen ist besonders darauf zu achten, dass keine wesentlichen Funktionen des Betrachtungsgegenstandes beeinträchtigt werden. Insbesondere ein Einfluss auf die Funktionssicherheit (*en: safety*) darf nicht nachteilig sein. Wie eine Detaillierung von FRs zu SRs und REs in IEC 62443-3-3 durchgeführt ist zeigt das Kapitel 6.2.

6.2 Sicherheitsanforderungen zur Identifizierung und Authentifizierung

Als Beispiel für das Runterbrechen von Anforderungen ist im Folgenden FR 1 – „Identifizierung und Authentifizierung“ beschrieben und in Tabelle 2 zusammengefasst. Das Ziel der „Identifizierung und Authentifizierung“ ist es, den Betrachtungsgegenstand dadurch zu schützen, dass die Identität eines jeden Nutzers geprüft wird, der Zugriff zum Betrachtungsgegenstand anfordert bevor die Kommunikation aktiviert wird. Dazu werden zunächst die allgemeinen Sicherheitslevels 1 bis 4 (vgl. Kapitel 5.4) an FR 1 angepasst und als erreichbarer Sicherheitslevel SL-C(IAC) formuliert. Nach Teil 3-3 der IEC 62443 ergibt das [11]:

- SL1: Identifizieren und Authentifizieren aller Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen gelegentlichen oder zufälligen Zugang von nicht authentifizierten Stellen schützen.
- SL2: Identifizieren und Authentisieren alle Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Stellen, die mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fertigkeiten und geringer Motivation vorgehen, schützen.

- **SL3:** Identifizieren und Authentisieren alle Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Stellen, die mit raffinierten Mitteln, mittleren Ressourcen, automatisierungstechnischen Fertigkeiten und mittlerer Motivation vorgehen, schützen.

- **SL4:** Identifizieren und Authentisieren alle Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Stellen, die mit raffinierten Mitteln, erheblicher Ressourcen, automatisierungstechnischen Fertigkeiten und hoher Motivation vorgehen, schützen.

Im nächsten Schritt wird die Anforderung nach einer „Identifizierung und Authentifizierung" genauer spezifiziert. Bspw. in das SR 1.1 „Identifizierung und Authentifizierung von menschlichen Nutzern" oder SR 1.3 „Nutzerkontenverwaltung". Auch diese Anforderungen werden wiederum detaillierter beschrieben. Z.B. in SR 1.1 RE 1 „Eindeutige Identifikation und Authentifizierung" und SR 1.1 RE 2 „Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze". Diese Anforderungen, sowohl SR als auch RE, können nun dem zuvor angepassten Sicherheitslevel zugeordnet werden, den diese bei einer Umsetzung erreichen können. Dieser System-Sicherheitslevel wird mit SL-C(IAC, System) 1 bis 4 beschrieben. Tabelle 2 zeigt solch eine Zuordnung für das FR 1 „Identifizierung und Authentifizierung".

Systemanforderungen (SR) und erweiterte Anforderungen (RE)		SL1	SL2	SL3	SL4
FR 1	Identifizierung und Authentifizierung (IAC)				
SR 1.1	Identifizierung und Authentifizierung von menschlichen Nutzern	✔	✔	✔	✔
SR 1.1	RE 1 Eindeutige Identifizierung und Authentifizierung		✔	✔	✔
SR 1.1	RE 2 Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze			✔	✔
SR 1.1	RE 3 Multifaktor-Authentifizierung über alle Netze				✔
SR 1.2	Identifizierung und Authentifizierung von Softwareprozessen und Geräten		✔	✔	✔
SR 1.2	RE 1 Eindeutige Identifizierung und Authentifizierung			✔	✔
SR 1.3	Nutzerkontenverwaltung	✔	✔	✔	✔
SR 1.3	RE 1 Einheitliche Nutzerkontenverwaltung			✔	✔
SR 1.4	Verwaltung der Kennungen	✔	✔	✔	✔
SR 1.5	Verwaltung der Authentifizierer	✔	✔	✔	✔
SR 1.5	RE 1 Beglaubigung der Identität von Softwareprozessen durch Hardwaremaßnahmen			✔	✔
SR 1.6	Management drahtloser Zugriffverfahren	✔	✔	✔	✔
SR 1.6	RE 1 Eindeutige Identifizierung und Authentifizierung		✔	✔	✔
SR 1.7	Stärke der Authentifizierung durch Passwörter	✔	✔	✔	✔
SR 1.7	RE 1 Erzeugung und Lebensdauerbeschränkung von Passwörtern für alle menschlichen Nutzer			✔	✔
SR 1.7	RE 2 Lebensdauerbeschränkung von Passwörtern für alle Nutzer				✔
SR 1.8	PKI-Zertifikate		✔	✔	✔
SR 1.9	Stärke der Authentifizierung durch öffentliche Schlüssel		✔	✔	✔
SR 1.9	RE 1 Beglaubigung öffentlicher Schlüssel durch Hardwaremaßnahmen			✔	✔
SR 1.10	Rückmeldung vom Authentifizierer	✔	✔	✔	✔
SR 1.11	Erfolglose Anmeldeversuche	✔	✔	✔	✔
SR 1.12	Nutzungshinweise	✔	✔	✔	✔
SR 1.13	Zugriff über nicht vertrauenswürdige Netze	✔	✔	✔	✔
SR 1.13	RE 1 Genehmigung ausdrücklicher Anmeldebegehren		✔	✔	✔

Tabelle 2: Zuordnung von SRs und REs einem zu erreichenden Sicherheitslevel für „Identifizierung und Authentifizierung" [10]

6.3 Anwendung für das Laden und Abrechnen in der Elektromobilität

Die in Teil 1-1 der IEC 62443 definierten grundlegenden Anforderungen (FR, en: foundational requirements) sind nicht spezifisch für die Industrieautomation, sondern spiegeln Bereiche wider, die in allen informationsverarbeitenden Systemen und Anlagen vorkommen können. Am Beispiel der Identifikation und Authentifizierung ist gezeigt worden, wie allgemeine Anforderungen zu detaillierteren Systemanforderungen heruntergebrochen werden können und gleichzeitig eine Verknüpfung mit dem Konzept der Sicherheitslevel stattfinden kann. Mit einer durchgeführten Bedrohungs- und Risikoanalyse und angepassten Sicherheitslevels ergibt sich nach dieser Methodik ein Anforderungskatalog, der zur Umsetzung durch technische Maßnahmen herangezogen werden kann.

Die Identifikation und Authentifizierung von Nutzern ist ein wichtiger Teil im Ablauf eines Ladevorgangs, hat aber aufgrund der Lage und Zugänglichkeit der Ladeinfrastruktur andere Rahmenbedingungen als im Umfeld der Industrieautomation. Z. B. ist die Verwendung von Passwörtern zur Authentifizierung an Ladesäulen nur bedingt umsetzungsfähig. Eine 1zu1-Anwendung der Systemanforderungen in der Elektromobilität ist ohne aussagekräftige Bedrohungs- und Risikoanalyse und ohne Berücksichtigung von Rahmenbedingungen dementsprechend nicht zielführend. Vielmehr sind die Methodik der grundlegenden Anforderungen und das Ableiten von Systemanforderungen sowie die Verknüpfung mit angepassten Sicherheitslevels auch für das Laden und Abrechnen in der Elektromobilität als Basis zu sehen. Davon ausgehend ist ein Anpassen der Systemanforderungen für die Elektromobilität zu empfehlen.

Ein weitere nützlicher Schritt könnte sein die in der Automobile Branche etablierten Methoden der Funktionalen Sicherheit (ISO 26262) oder des Software-Qualitätsmanagement (ISO/IEC 15504) auf die neuen Herausforderungen zu erweitern und anzupassen.

7 Sicherheitsanforderungen für Produkte

7.1 Einordnung von Anforderungen für Produkte

Sicherheitsanforderungen für Produkte richten sich an den Hersteller informationstechnischer Systeme und Anlagen (vgl. Abb. 6). Die Normenreihe IEC 62443 hat dafür zwei Teile entwickelt. In Teil 4-1 werden Prozessanforderungen für die Produktentwicklung definiert. Teil 4-2 beschreibt technische Sicherheitsanforderungen für Komponenten. Beide Teile sind in diesem Kapitel kurz erläutert und in Relation zur Elektromobilität gebracht.

7.2 Prozessanforderungen für die Produktentwicklung

Der Teil 4-1 der IEC 62443 spezifiziert Prozessanforderungen für die sichere Produktentwicklung von IACS. Es wird ein Sicherheits-Entwicklungs-Lebenszyklus („Secure Development Life-cycle", SDL) definiert, der sämtliche Phasen und Maßnahmen beinhaltet. Dazu gehören z.B. Sicherheitsanforderungen, sichere Implementierung, Verifikation und Validierung, Patch-Management und Zurückziehen des Produkts. Das übergeordnete Ziel der Anforderungen ist es, ein Rahmenwerk zur Verfügung zu stellen, um den „Security by design" und „Defense-in-Depth"-Ansatz im Design, Aufbau, Wartung und Zurückziehen der Produkte zu adressieren. Des Weiteren ist die Aufgabe der Anforderungen den Entwicklungsprozess an den Sicherheitsbedürfnissen der Anwender auszurichten. Das bedeutet, dass der Prozess Ergebnisse wie z. B. gut dokumentierte Sicherheitskonfigurationen und Richtlinien für ein Patch-Management hervorbringen muss, ebenso wie eine klare und kurze Kommunikation bei der Entdeckung von Schwachstellen und Vorfällen.

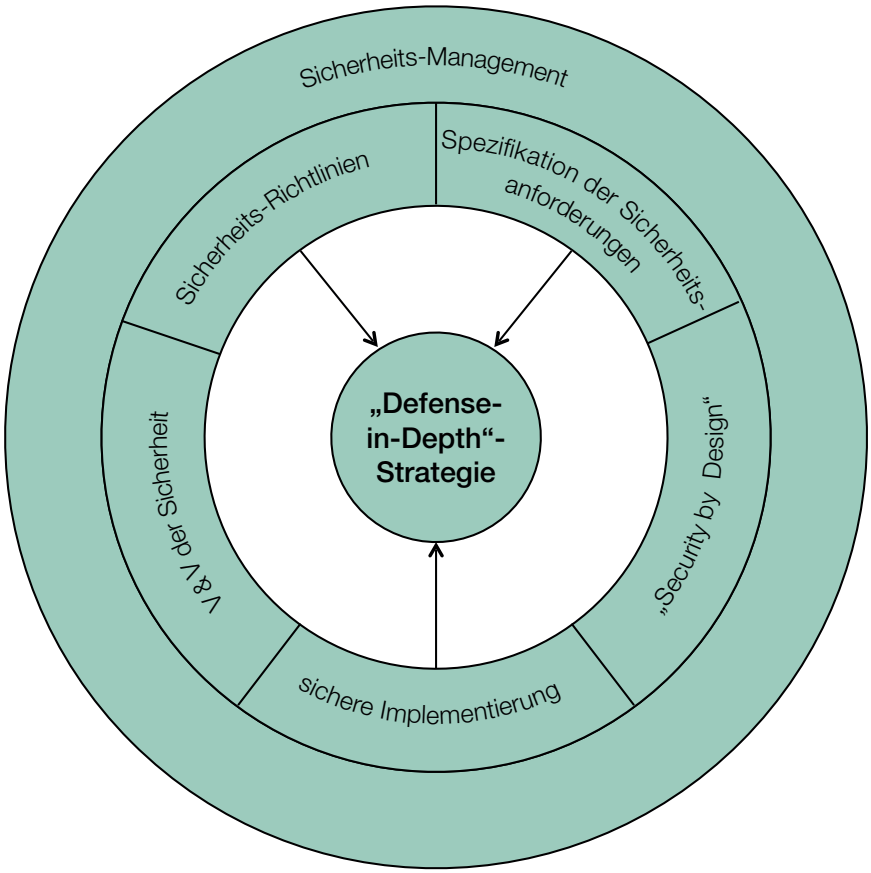


Abb. 11: Die „Defense-in-Depth"-Strategie als Schlüsselkonzept für Sicherheit im Produkt-Lebenszyklus [16]

Abb. 11 zeigt wie die „Security-by-design"-Prinzipien in der „Defense-in-Depth"-Strategie mitwirken. Nicht dargestellt sind die Mängelbehebung und das Patch-Management, die als Teil der sicheren Implementierung zu sehen sind. Im äußeren Ring befindet sich das Sicherheits-Management als übergeordneter Bereich. Dieser soll sicherstellen dass alle anderen Bereiche korrekt verfolgt und gehandhabt werden.

Die IEC 62442-4-1 ordnet allen Bereichen Anforderungen zu, ähnlich Teil 3-3 (vgl. Kapitel 6). Tabelle 3 zeigt alle Bereiche für Sicherheitsanforderungen, Tabelle 4 zeigt beispielhaft die Sicherheitsanforderungen für den Bereich des Sicherheits-Managements.

Bereiche für Sicherheitsanforderungen	
1	Sicherheits-Management (*en: Security management*)
2	Spezifikation der Sicherheitsanforderungen (*en: Specification of security requirements*)
3	„Security-by-Design“ *(en: Secure by design)*
4	Sichere Implementierung (*en: Secure Implementation*)
5	Verifikation & Validierung der Sicherheit (*en: Security verification and validation testing*)
6	Mängelbehebung (*en: Management of security-related issues*)
7	Patch-Management (*en: Security update management*)
8	Sicherheits-Richtlinien (*en: Security guidelines*)

Tabelle 3: Bereiche für Sicherheitsanforderungen [16]

Bereich 1 – Sicherheits-Management	
SM-1	Entwicklungsprozess (en: Development process)
SM-2	Identifikation der Verantwortlichkeiten (en: Identification of responsibilities)
SM-3	Identifikation der Verwendbarkeit (en: Identification of applicability)
SM-4	Sicherheits-Expertise (en: Security expertise)
SM-5	Prozessabgrenzung (en: Process scoping)
SM-6	Datei-Integrität (en: File integrity)
SM-7	Sicherheit der Entwicklungsumgebung (en: Development environment security)
SM-8	Kontrolleinrichtungen für private Schlüssel (en: Controls for private keys)
SM-9	Sicherheitsanforderungen für extern bereitgestellte Komponenten (en: Security requirements for externally provided components)
SM-10	Kundenspezifisch entwickelte Komponenten von Drittzulieferern (en: Custom developed components from third-party suppliers)
SM-11	Bewerten und Zuweisen von sicherheitsrelevanten Aspekten (en: Assessing and addressing security-related issues)
SM-12	Prozessverifikation (en: Process verification)
SM-13	Kontinuierliche Verbesserung (en: Continuous improvement)

Tabelle 4: Sicherheitsanforderungen für den Bereich „Sicherheits-Management“ [16]

Die Anforderung, beispielsweise zu SM-2 Identifikation der Verantwortlichkeiten, lautet nach [16] sinngemäß: „Ein Prozess muss zum Einsatz kommen, der organisatorische Rollen und personelle Verantwortliche für jeden notwendigen Prozess im Rahmen der Produktentwicklung, der Instandhaltung und des Supports identifiziert.“ Dieser Prozess ist notwendig um sicherzustellen dass die Verantwortlichkeiten zu einzelnen Prozessschritten zugeordnet werden. Eine mögliche Umsetzung dieser Anforderung ist die Einführung einer sogenannten RACI-Matrix[7], die eine Zuordnung der Verantwortlichkeiten vornimmt.

[7] RACI steht für Responsible (verantwortlich), Accountable (rechenschaftsplichtig), Consulted (konsultiert) und Informed (informiert). Die RACI-Matrix kann je nach Anwendung in verschiedene Varianten umgesetzt werden [19].

7.3 Sicherheitsanforderungen für Komponenten

7.3.1 Allgemeine Vorgehensweise

Sicherheitsanforderungen für Komponenten richten sich an den Hersteller informationstechnischer Produkte und Komponenten (vgl. Abb. 6). In Teil 4-2 der IEC 62443 werden Komponentenanforderungen für die technische Umsetzung von Maßnahmen definiert.

Die Vorgehensweise bei Sicherheitsanforderungen für Komponenten ist vergleichbar mit der Vorgehensweise bei Sicherheitsanforderungen für Systeme (vgl. Kapitel 6.1). Aus den technischen Systemanforderungen (SR, en: system requirements) aus Teil 3-3 der IEC 62443 werden technischen Komponentenanforderungen (CR, en: component requirements) und weitergehende Anforderungen (RE, en: requirement enhancement) abgeleitet [20]. Vier Arten von Komponenten werden durch die Komponentenanforderungen adressiert:

- Softwareanwendungen (SAR)
- Eingebettete Geräte (EDR)
- Host-Geräte (HDR)
- Netzwerkkomponenten (NDR)

Die meisten Komponentenanforderungen gelten für alle vier Komponentenarten und werden allgemein mit CR bezeichnet. Gerätespezifische Anforderungen erhalten die Abkürzung der jeweiligen Komponentenart. Beim Umsetzen der Komponentenanforderungen durch Sicherheitsmaßnahmen ist wie bei den Systemanforderungen besonders darauf zu achten, dass keine wesentlichen Funktionen des Betrachtungsgegenstandes beeinträchtigt werden. Wie eine Detaillierung von SRs zu CRs und REs in der IEC 62443-4-2 durchgeführt ist, zeigt das Kapitel 7.2.2, gerätespezifische Anforderungen beschreibt Kapitel 7.2.3.

7.3.2 Sicherheitsanforderungen zur Identifizierung und Authentifizierung

Als Beispiel für das Runterbrechen von Anforderungen ist im Folgenden FR 1 – „Identifizierung und Authentifizierung“ beschrieben und in Tabelle 5 zusammengefasst. Das Ziel der „Identifizierung und Authentifizierung“ ist es, wie bei der Ableitung der Systemanforderungen, den Betrachtungsgegenstand dadurch zu schützen, dass die Identität eines jeden Nutzers geprüft wird, der Zugriff zum Betrachtungsgegenstand anfordert bevor die Kommunikation aktiviert wird. Dazu werden die allgemeinen Sicherheitslevels 1 bis 4 (vgl. Kapitel 5.4) an FR 1 angepasst und als SL-C(IAC) formuliert (vgl. Kapitel 6.2).

Die Anforderung nach einer „Identifizierung und Authentifizierung“ wird im nächsten Schritt genauer spezifiziert. Bspw. in das CR 1.1 „Identifizierung und Authentifizierung von menschlichen Nutzern“ oder CR 1.3 „Nutzerkontenverwaltung“. Auch diese Anforderungen werden wiederum detaillierter beschrieben. Z.B. in CR 1.1 RE 1 „Eindeutige Identifikation und Authentifizierung“ und CR 1.1 RE 2 „Multifaktor-Authentifizierung über alle Schnittstellen“. Diese Anforderungen, sowohl CR als auch RE, können nun einem zuvor angepassten Sicherheitslevel zugeordnet werden, den diese bei einer Umsetzung erreichen können. Dieser Komponenten-Sicherheitslevel wird mit SL-C(IAC, Komponente) 1 bis 4 beschrieben. Tabelle 5 zeigt solch eine Zuordnung für das FR 1 „Identifizierung und Authentifizierung“.

Komponentenanforderungen (CR) und erweiterte Anforderungen (RE)			SL1	SL2	SL3	SL4
FR 1	Identifizierung und Authentifizierung (IAC)					
CR 1.1	Identifizierung und Authentifizierung von menschlichen Nutzern		✔	✔	✔	✔
CR 1.1	RE 1	Eindeutige Identifizierung und Authentifizierung		✔	✔	✔
CR 1.1	RE 2	Multifaktor-Authentifizierung über alle Schnittstellen				✔
CR 1.2	Identifizierung und Authentifizierung von Softwareprozessen und Geräten			✔	✔	✔
CR 1.2	RE 1	Eindeutige Identifizierung und Authentifizierung			✔	✔
CR 1.3	Nutzerkontenverwaltung		✔	✔	✔	✔
CR 1.4	Verwaltung der Kennungen		✔	✔	✔	✔
CR 1.5	Verwaltung der Authentifizierer		✔	✔	✔	✔
CR 1.5	RE 1	Hardwaresicherheit für Authentifizierer			✔	✔
CR 1.6	Verwaltung drahtloser Zugriffverfahren					
CR 1.7	Stärke der Authentifizierung durch Passwörter		✔	✔	✔	✔
CR 1.7	RE 1	Erzeugung und Lebensdauerbeschränkung von Passwörtern für menschlichen Nutzer			✔	✔
CR 1.7	RE 2	Lebensdauerbeschränkung von Passwörtern für alle Nutzer				✔
CR 1.8	PKI-Zertifikate			✔	✔	✔
CR 1.9	Stärke der Authentifizierung durch öffentliche Schlüssel			✔	✔	✔
CR 1.9	RE 1	Hardwaresicherheit für eine Authentifikation durch öffentliche Schlüssel			✔	✔
CR 1.10	Rückmeldung vom Authentifizierer		✔	✔	✔	✔
CR 1.11	Erfolglose Anmeldeversuche		✔	✔	✔	✔
CR 1.12	Nutzungshinweise des Systems		✔	✔	✔	✔
CR 1.13	Zugriff über nicht vertrauenswürdige Netzwerke					
CR 1.14	Stärke der Authentifikation durch symmetrische Schlüssel			✔	✔	✔
CR 1.14	RE 1	Hardwaresicherheit für eine Authentifikation durch symmetrische Schlüssel			✔	✔

Tabelle 5: Zuordnung von CRs und REs einem zu erreichenden Sicherheitslevel für „Identifizierung und Authentifizierung“ [20]

7.3.3 Sicherheitsanforderungen an Softwareanwendungen

Für Softwareanwendungen (SAR) beschreibt die IEC 62443-4-2 gerätespezifische Anforderungen. Diese sind keinem FR zugeordnet, sondern können verschiedene FRs adressieren. Im Fall von SAR sind das FR 2 – „Nutzungskontrolle“ und FR 3 – „Systemintegrität“. Tabelle 6 zeigt die Komponentenanforderungen für Softwareanwendungen.

Komponentenanforderungen für Softwareanwendungen (SAR) und erweiterte Anforderungen (RE)		SL1	SL2	SL3	SL4
FR 2	Nutzungskontrolle				
SAR 2.4	Mobiler Code	✔	✔	✔	✔
SAR 2.4	RE 1 Authentizitätsüberprüfung für mobilen Code		✔	✔	✔
FR 3	Systemintegrität				
SAR 3.2	Schutz vor böswilligem Code	✔	✔	✔	✔

Tabelle 6: Zuordnung von SARs und REs einem zu erreichenden Sicherheitslevel [20]

7.4 Anwendung für das Laden und Abrechnen in der Elektromobilität

Die in Teil 4-1 der IEC 62443 beschriebenen Bereiche für Sicherheitsanforderungen (vgl. Tab. 3) sind wie die grundlegenden Anforderungen aus Teil 1-1 nicht spezifisch für die Industrieautomation. Sie spiegeln Teile wider, die in allen informationsverarbeitenden Systemen und Anlagen vorkommen können und können somit als Basis gesehen werden. Der beschriebene Secure Development Life-cycle benötigt jedoch einen allgemeinen Produktentwicklungszyklus auf dem aufgesetzt werden kann. Die Grundlagen dazu stehen bspw. in der ISO 9001 oder ISO/IEC 27034, [16]. Für eine Übertragung der Anforderungen an die Produktentwicklung sollte sich deswegen nicht nur an die IEC 62443-4-1 gehalten werden. Des Weiteren ist es notwendig die Entwicklungsumgebung entsprechend sicher zu gestalten. Hierbei bieten ISO/IEC 27001 und ISO/IEC 27002 die Grundlagen für ein Informationssicherheits-Managementsystem[8] (ISMS). Insbesondere für die Elektromobilität sei hier auf den branchenspezifischen Sicherheitsstandard der Energieversorgung die ISO/IEC 27019 hingewiesen [18].

Die Komponentenanforderungen aus Teil 4-2 der IEC 62443 lassen sich aufgrund der gleichen Methodik ähnlich handhaben wie die Systemanforderungen aus Teil 3-3 (vgl. Kapitel 6.3). Durch die unterschiedlichen Rahmenbedingungen zwischen Industrieautomation und Elektromobilität ist eine 1zu1-Anwendung nicht sinnvoll. Als Beispiel ist wieder die Verwendung von Passwörtern zur Authentifizierung an Ladesäulen zu nennen. Die abgeleiteten Komponentenanforderungen sind Teil der Methodik der grundlegenden Anforderungen und der Sicherheitslevel, sodass ein Anpassen dieser Anforderungen für das Laden und Abrechnen in der Elektromobilität zu empfehlen ist.

[8] Ein Informationssicherheits-Managementsystem (ISMS) ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen [17].

8 Ansatz für ein ganzheitliches Schutzkonzept für das Laden und Abrechnen in der Elektromobilität

8.1 Vorgehensweise zum Aufbau eines ganzheitlichen Schutzkonzeptes

Für den ganzheitlichen Schutz ist es notwendig sich der Bedrohungen und der Risiken im Umfeld der Elektromobilität bewusst zu sein. Die Herausforderung besteht dabei, Fahrzeug, Ladeinfrastruktur und Backend-Systeme mit ihren unterschiedlichen Stakeholdern in Einklang zu bringen. Vertrauen in Sicherheitsmaßnahmen und die Fähigkeiten der Mitarbeiten spielen dabei ebenso eine wichtige Rolle.

Das Schutzkonzept der tiefgestaffelten Verteidigung (Defense-in-Depth) in Kapitel 5.1 zeigt die wichtigen Merkmale für ein ganzheitliches Schutzkonzept auf. Eine Schutzmaßnahme allein ist nicht ausreichend um einen umfassenden Schutz zu gewähren. Ein Gesamtkonzept, das alle Risiken minimieren und einen effektiven Schutz bieten soll, muss sowohl technische als auch organisatorische Maßnahmen beinhalten. Alle Beteiligten müssen dabei nicht nur ihren Beitrag dazu leisten, sondern die Schutzmechanismen müssen ineinandergreifen um keine Lücke entstehen zu lassen. Gegen unterschiedliche Bedrohungen muss mit verschiedenen und sich ergänzenden Konzepten vorgegangen werden. Im Kontext der Elektromobilität heißt das z. B., dass ein Fahrzeug auch von der Ladeinfrastruktur und umgekehrt zu schützen ist. Als Vorgehensweise für ein ganzheitliches Schutzkonzept eignet sich deshalb die Aufteilung in Anlagensicherheit, Netzwerksicherheit und Systemintegrität der Defense-in-Depth-Strategie (vgl. Abb. 6). In den folgenden Kapiteln wird diese Aufteilung für die Elektromobilität angewendet und in die Bereiche Fahrzeug, Ladeinfrastruktur und Backend unterteilt.

8.2 Anlagensicherheit für Fahrzeug, Ladeinfrastruktur und Backend

Für die Anlagensicherheit ist im Wesentlichen der Betreiber zuständig. Sie beinhaltet sowohl einen physikalischen Zugangsschutz als auch organisatorische Maßnahmen. Abb. 12 zeigt den Anteil der Anlagensicherheit für den ganzheitlichen Ansatz der „Defense-in-Depth"-Strategie. Bei der Ladeinfrastruktur und Backend-Systemen sind die Zuordnung der Verantwortlichkeit und die Maßnahmen klar: der Betreiber muss sicherstellen dass der Zugang von nicht autorisierten Personen verhindert wird. D.h. die Backend-Server müssen entsprechend aufbewahrt werden und mittels Zäunen, Zugangsberechtigungen, Schutztüren, etc. gesichert werden. Bei Ladeinfrastrukturen im öffentlichen Raum können solche Maßnahmen nur bedingt umgesetzt werden. Hier muss die Ladesäule mit einem Gehäuse und weiteren Maßnahmen zum Schutz vor unbefugten Personen gesichert werden. Für das Fahrzeug als „mobilen Rechner" ist die Zuständigkeit des Betreibers für die Anlagensicherheit nicht klar zu zuordnen. Der Automobilhersteller sollte die Fahrzeugschnittstellen so gestalten, dass diese nur dem Fachpersonal und evtl. dem Fahrzeugnutzer zugänglich sind. Für den Fahrzeuginhaber könnten sich evtl. Anforderungen ergeben, bei Beschädigungen der Schnittstellen unverzüglich eine Werkstatt aufzusuchen.

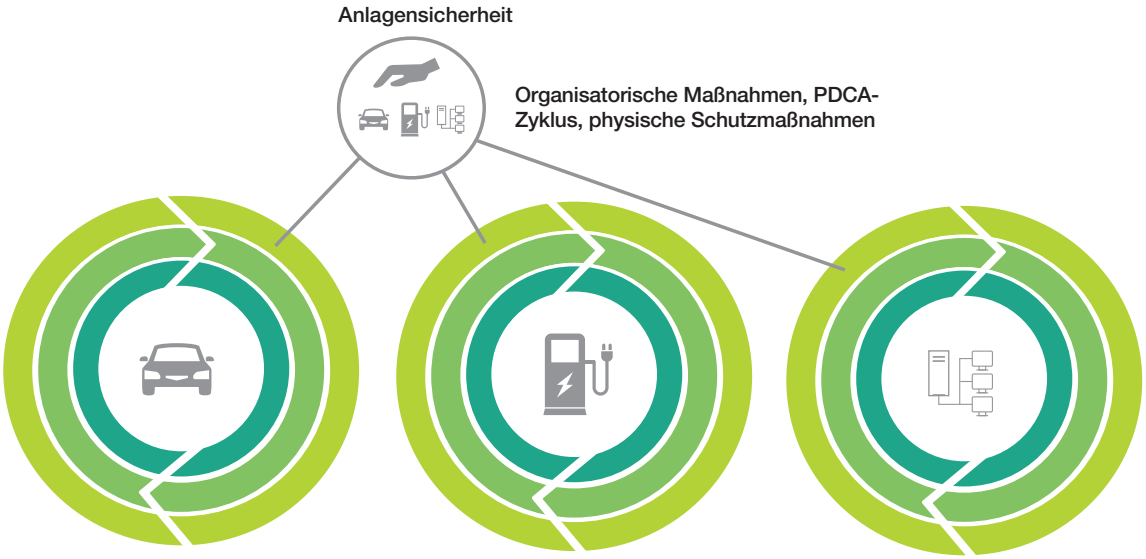


Abb. 12: Ganzheitlicher Ansatz - Anlagensicherheit

Zu den organisatorischen Maßnahmen gehört die Einführung und Etablierung von Sicherheitsmanagement-Prozessen. Im Vorfeld ist dabei eine Analyse der Bedrohungen und Risiken durchzuführen. Als Hilfsmittel ist dafür die in Kapitel 5.3 beschrieben Risikobewertung nach VDI/VDE 2182 und die einschlägigen Normen für ein Informationssicherheits-Managementsystem (vgl. Kapitel 7.3) zu empfehlen. Ohne diese Bewertung besteht die Gefahr, dass wirkungslose Maßnahmen getroffen werden und Schwachstellen nicht erkannt werden. Die Sicherheits-Prozesse sind von den Betreibern der Ladeinfrastruktur und der Backend-Systeme durchzuführen. Für die Automobilhersteller gilt, Sicherheits-Prozesse einzuführen, die nach dem Verkauf des Fahrzeugs zum Tragen kommen um z. B. Software-Updates zur Verfügung zu stellen.

8.3 Netzwerksicherheit für Fahrzeug, Ladeinfrastruktur und Backend

Die Netzwerksicherheit ist in der Regel vom Integrator sicherzustellen. Eine enge Abstimmung mit dem Betreiber ist jedoch zu empfehlen. Abb. 13 zeigt den Anteil der Netzwerksicherheit für den ganzheitlichen Ansatz der „Defense-in-Depth"-Strategie. Zwei wesentliche Aufgaben für die Netzwerksicherheit sind der Schutz bzw. die Kontrolle aller Schnittstellen und der Schutz der Kommunikation gegenüber Manipulation. Die Sicherung der Schnittstellen zu anderen Netzwerken kann z. B. mittels Firewalls und VPNs erfolgen. So kann der Zugriff gemäß Zonen und Conduits auf Fahrzeuge, Ladesäulen und Backend-Systeme kontrolliert werden. In Anlehnung an Abb.1 ist es möglich den dort dargestellten Beteiligten bzw. Rollen Sicherheitszonen zuzuweisen und so eine sicherheitstechnische Segmentierung zu definieren. Von zentraler Bedeutung für die Netzwerksicherheit ist wie auch für die Anlagensicherheit die Bedrohungs- und Risikoanalyse (vgl. Kapitel 5.3). Nach einer Analyse und der Netzwerksegmentierung können in Zusammenarbeit mit Betreibern, Integratoren und Herstellern Sicherheitslevel eingeführt werden (vgl. Kapitel 5.4). Das Ergebnis ist, dass bestimmte Komponenten z. B. Gateways oder Kommunikations-Controller sowohl im Fahrzeug, als auch in der Ladeinfrastruktur und im Backend Sicherheits-Eigenschaften besitzen müssen.

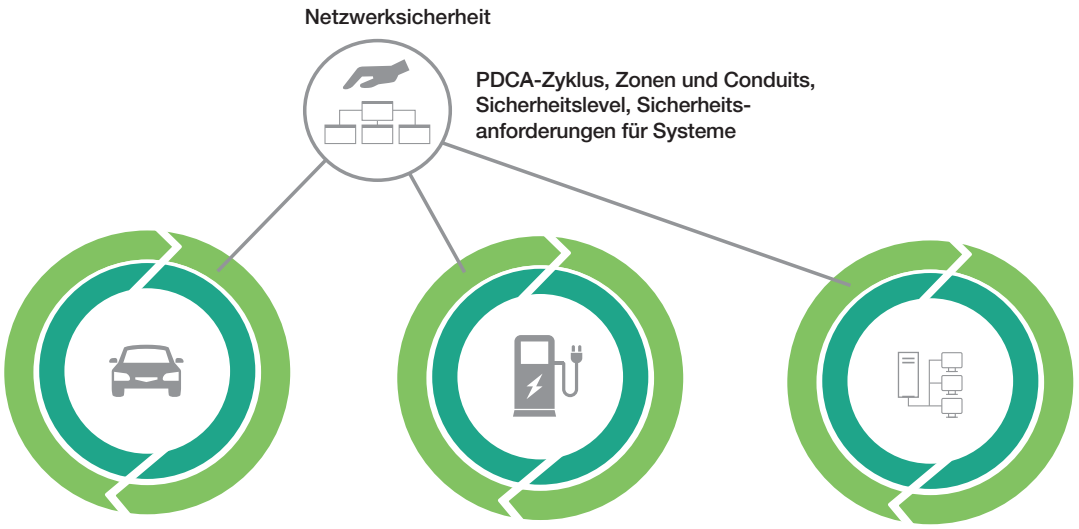


Abb. 13: Ganzheitlicher Ansatz - Netzwerksicherheit

Das Ökosystem Elektromobilität besteht aus vielen verteilten Systemen und Beteiligten, die über das Internet miteinander verbunden sind. Viele Funktionalitäten benötigen Fernzugriffe auf Geräte oder Systeme. Das macht die Absicherung besonders wichtig. Hacker haben es hier vergleichsweise einfach einen ungesicherten Zugang zu finden. Maßnahmen dagegen sind z. B. die Verschlüsselung der Kommunikation und die Authentifizierung und Autorisierung der Teilnehmer durch die Verwendung von VPN-Technologien. Auch können Geräte mittels Zertifikate als vertrauenswürdig eingestuft werden. Der Aufbau und Betrieb einer Public-Key Infrastruktur[9] (kurz PKI) kann das Zertifikatsmanagement für Beteiligte im Ökosystem Elektromobilität umsetzen.

[9] Zur Erzeugung und Verwaltung von Zertifikaten werden spezielle Infrastrukturen eingesetzt. Im Bereich der der asymmetrischen Kryptosysteme hat sich für die Gesamtheit der Komponenten, die hierfür benötigt werden, der Begriff der Public-Key Infrastruktur (PKI) eingebürgert [6].

8.4 Systemintegrität für Fahrzeug, Ladeinfrastruktur und Backend

Die Systemintegrität ist maßgeblich durch den Hersteller der Komponenten sicherzustellen. Als Komponentenentwickler kommen auf ihn die Aufgaben zu, einen sicheren Entwicklungsprozess zu etablieren und Sicherheits-Eigenschaften ausgehend von dem zuvor festgelegten Sicherheitslevel zu implementieren. Für die Systemintegrität spielt dabei der PDCA-Zyklus eine entscheidende Rolle (vgl. Kapitel 5.3). Abb. 14 zeigt den Anteil der Systemintegrität für den ganzheitlichen Ansatz der „Defense-in-Depth"-Strategie.

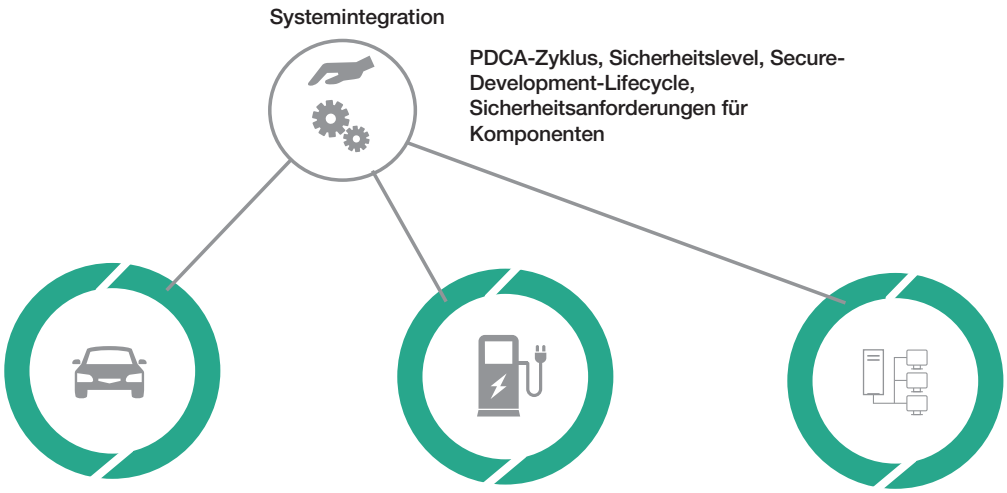


Abb. 14: Ganzheitlicher Ansatz - Systemintegrität

Allgemein gilt für die Sicherheitseigenschaften und -anforderungen an Fahrzeug-, Ladeinfrastruktur- und Backend-Komponenten die Verfügbarkeit der Funktionen und die Integrität der Daten zu gewährleisten. Zur Umsetzung kann z. B. ein Passwortschutz oder Kopierschutz von Softwareanteilen genutzt werden, ebenso ist die Verwendung von Hardware-Sicherheitsmodulen[10] (kurz: HSM) zur sicheren Durchführung von kryptografischen Berechnungen eine Möglichkeit.

[10] Der Begriff Hardware-Sicherheitsmodul (HSM) bezeichnet ein internes oder externes Peripheriegerät für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen. Dies ermöglicht zum Beispiel, die Vertrauenswürdigkeit und die Integrität von Daten und den damit verbundenen Informationen in geschäftskritischen IT-Systemen sicherzustellen [21].

9 Fazit und Ausblick

Die Normenreihe IEC 62443 beschreibt Sicherheitskonzepte, Verfahren und Sicherheitsanforderungen für den Bereich der Industrieautomation, die auch für kritische Infrastrukturen anwendbar sind. Sie verfolgt einen ganzheitlichen Ansatz, der sowohl technische als auch organisatorische Maßnahmen beinhaltet und dadurch grundlegende Eigenschaften der IT-Sicherheit widerspiegelt: IT-Sicherheit ist nicht durch eine einzelne Maßnahme zu erreichen. IT-Sicherheit ist ein Prozess, der fortlaufende Anpassungen benötigt. IT-Sicherheit muss von Beginn an in der Produkt- und Systementwicklung berücksichtigt werden. Durch ihren umfassenden Charakter ist die Normenreihe bereits heute das Regelwerk für IT-Sicherheit in der Industrieautomation schlechthin und diente bereits anderen Normungsaktivitäten in den Bereichen Bahn und Heimautomatisierung als Referenz. Aktuell gibt es Bestrebungen aus dem Automobil- und Medizingerätesektor die Normenreihe IEC 62443 als Basis für weitere sektorspezifische Normen zu verwenden.

Für eine Anwendung der Sicherheitskonzepte und -anforderungen in andere Bereiche wurden als erstes die Schutzziele betrachtet. Die Schutzziele in der sogenannten „Industrial Security“ unterscheiden sich dabei nur geringfügig von den Schutzzielen in der Elektromobilität. Die Verfügbarkeit und Integrität spielen in beiden Bereichen eine wichtige Rolle. Die Vertraulichkeit bzw. der Datenschutz ist jedoch in der Elektromobilität ebenso von Bedeutung und ist in der Industrieautomation niedriger priorisiert. Dieser Umstand muss bei der Analyse der IEC 62443 stets bedacht werden.

Die Grundkonzepte der Normenreihe IEC 62443 aus Teil 1-1 sind allesamt so ausgelegt, dass sie in allen informationstechnischen Systemen, Anlagen und Prozessen angewendet werden können. Insbesondere das Konzept der „Defense-in-Depth“ und die Bedrohungs- und Risikoanalyse (PDCA-Zyklus) sind fundamental für eine ganzheitliche Betrachtung von IT-Sicherheit. Die eingeführten Sicherheitslevels (SL) und grundlegende Anforderungen (FR) bieten einen Ansatz um den Schutz des Betrachtungsgegenstandes qualitativ zu bestimmen. Die daraus abgeleiteten System- und Komponentenanforderungen sind, wie am Beispiel der „Identifizierung und Authentifizierung“ gezeigt wurde, für eine Umsetzung in der Elektromobilität anzupassen.

Die Umsetzung der grundlegenden Sicherheitskonzepte aus der IEC 62443 und die Anpassung der System- und Komponentenanforderungen für das Laden und Abrechnen in der Elektromobilität sollten Gegenstand weiterer Aktivitäten sein. Das Ziel sollte sein, konkrete Anwendungshinweise für Automobilhersteller, Ladesäulenbetreiber und –hersteller sowie Backend-Betreiber zu entwickeln. Diese Hinweise müssen neben den technischen Sicherheitsanforderungen auch organisatorische Anforderungen gemäß den System-, Komponenten- und Prozessanforderungen der IEC 62443 enthalten. Zusätzlich muss darauf geachtet werden, spezifische Anforderungen für den Bereich Elektromobilität wie an Eichrechtskonformität und die Auswirkung der IT-Sicherheit auf safety-relevante Funktionen zu berücksichtigen. Der Zusammenhang zwischen funktionaler Sicherheit und IT-Sicherheit wird u.a. in der DKE im Gremium des TBINK Arbeitskreises „IT-Security und Security by Design“ bearbeitet. Dort wurde eine VDE-Anwendungsregel erstellt, die diesen Aspekt allgemeingültig darlegt [22]. Weitere spezifische Anforderungen sind aus dem Datenschutz abzuleiten. Dabei sind die erweiterten Schutzziele Authentizität, Verbindlichkeit, Anonymisierung/Pseudonymisierung [6], die in dieser Studie nicht thematisiert worden sind, zu berücksichtigen. Einen Ansatz um dem Datenschutz Rechnung zu tragen zeigt eine Analyse des Fraunhofer-Instituts für Sichere Informationstechnik (FhG SIT) in [23].

Für diese Erstellung eines umfassenden Anforderungskatalogs ist jedoch die alleinige Betrachtung der IEC 62443 nicht ausreichend. Im Bereich der Energieversorgung, gibt es seit vielen Jahren die Normenreihe IEC 62351. Diese Reihe beschreibt technische Sicherheitslösungen für die Kommunikation in der Energieautomatisierung. Einzelne Normenteile behandeln z. B. die rollenbasierte Zugriffskontrolle, das Schlüsselmanagement oder Sicherheitsanforderungen für Protokolle wie TCP/IP. Aus der IEC 62351 können somit Sicherheitsanforderungen und Lösungsansätze für eine sichere Kommunikation im Ökosystem Elektromobilität gewonnen werden. Für organisatorische Sicherheitsanforderungen im Rahmen eines ISMS ist der branchenspezifische Sicherheitsstandard der Energieversorgung die ISO/IEC 27019 bzw. die allgemeinen Standards ISO/IEC 27001 und ISO/IEC 27002 zu berücksichtigen.

Literatur

[1] IKT für Elektromobilität II, *Innovationsacht 2014,* Bundeswirtschaftministerium für Wirtschaft und Energie (BMWi), Januar 2014

[2] IT-Sicherheitsgesetz: *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in der Fassung der Bekanntmachung vom 24. Juli 2015*

[3] DIN VDE V 0831-104: *Elektrische Bahn-Signalanlagen - Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage der IEC 62443 (DIN VDE V 0831-104:2015-10)*

[4] VDE-AR-E 2849-1: *Elektrische Systemtechnik in Heim und Gebäude - IT-Sicherheit und Datenschutz - Allgemeine Anforderungen* (VDE-AR-E 2849-1:2017-08)

[5] EU-Richtlinie 2008/114/EG *des Europäischen Rates in der Fassung der Bekanntmachung vom 08.12.2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern*

[6] C. Eckert, *IT-Sicherheit,* München: De Gruyter Oldenbourg Verlag, 10. Auflage, 2018

[7] IT-Grundschutz – Arbeitshandbuch: Bundesanzeiger Verlag, 2. Auflage 2017

[8] EU-DSGVO: *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates in der Fassung der Bekanntmachung vom 27.04.2016 (Europäische Datenschutzgrund-verordnung)*

[9] IEC 62443-1-1: *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models* (IEC/TS 62443-1-1:2009-07)

[10] P. Kobes, *Leitfaden Industrial Security,* Berlin: VDE Verlag, 2016

[11] IEC 62443-3-3: *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* (DIN IEC 62443-3-3 VDE 0802-3-3:2013-08 + Cor.:2014-04)

[12] KRITIS, URL *https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/Energie,* (Aufgerufen am 20.03.2018)

[13] Umweltbundesamt, URL *https://www.umweltbundesamt.de/service/uba-fragen/was-ist-ein-smart-grid,* (Aufruf am 20.03.2018)

[14] Bundesministerium für Wirtschaft und Energie, URL *https://www.bmwi.de/Redaktion/ DE/Artikel/Energie/intelligente-netze.html*, (Aufruf am 25.07.2018)

[15] VDI/VDE 2182: *Informationssicherheit in der industriellen Automatisierung - Blatt 1: Allgemeines Vorgehensmodell* (VDI/VDE 2182:2011-01)

[16] IEC 62443-4-1: *Industrial communication networks - Network and system security - Part 4-1: Secure product development lifecycle requirements* (IEC 62443-4-1:2018-01)

[17] ISO/IEC 27000: *Information technology - Security techniques - Information security management systems - Overview and vocabulary* (ISO/IEC 27000:2018-04)

[18] ISO/IEC 27019: *Information technology - Security techniques - Information security controls for the energy utility industry* (ISO/IEC 27019: 2017-10)

[19] *https://de.wikipedia.org/wiki/RACI*, (Aufruf am 24.04.2018).

[20] IEC 62443-4-2: *Industrial communication networks - Network and system security - Part 4-2: Technical security requirements for IACS components* (prEN 62443-4-2:2017-10)

[21] *https://de.wikipedia.org/wiki/Hardware-Sicherheitsmodul* (Aufruf am 08.08.2018)

[22] VDE-AR-E 2802-10-1: *Zusammenhang zwischen funktionaler Sicherheit und Informationssicherheit am Beispiel der Industrieautomation – Teil 1: Grundlagen* (VDE-AR-E 2802-10-1:2017-04)

[23] Daniel Zelle, Markus Springer, Maria Zhdanova, und Christoph Krauß, *Anonymous Charging and Billing of Electric Vehicles:* ACM, New York, 2018

DELTA

Datensicherheit und -integrität in der Elektromobilität beim Laden und eichrechtkonformen Abrechnen

VDE Verband der Elektrotechnik
Elektronik Informationstechnik

DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE
Stresemannallee 15
60596 Frankfurt

Tel. +49 69 6308-0
dke@vde.com
www.dke.de

DKE
VDE DIN