Mercedes-Benz **MBN 9666-9**
Werknorm Ausgabe: 2021-11
Übergangsfrist: 0 Monate
Seiten insgesamt (inkl. Anhang): 29

Ausführung und Bestimmungen für Produktionsmittel, Betriebsmittel, Maschinen, Anlagen, Einrichtungen und Vorrichtungen

Teil 9: IT-Security Vorgaben für Lieferanten

Vorwort

Die Entwicklungen in der Produktion im Sinne der Industrie 4.0 bringen eine stark steigende Vernetzung mit sich und verändern so massiv die Gefahrenlage für die Produktion. Bei der Beschaffung von Automatisierungslösungen lag der Fokus in der Vergangenheit vor allem auf den Anforderungen der Produktion für einen optimalen und effizienten Funktionsumfang, der eine hohe Verfügbarkeit und Ausbringung garantiert.

Bei neuen oder bestehenden Produktionssystemen oder -linien werden die hierfür benötigten IT-Komponenten meist als direkte Bestandteile der Automatisierungslösung mit eingekauft und ebenfalls nach den oben beschriebenen Kriterien ausgewählt.

Eine Absicherung aus Sicht der Informationssicherheit fand nur rudimentär als untergeordnete Anforderung statt. Ziel dieser Werksnorm – MBN 9666-9 – ist die Etablierung von Mindeststandards für die Informationssicherheit, die bei der Beschaffung von Anlagen, die IT-Equipment enthalten, einzuhalten sind. Die Einhaltung der von Daimler gestellten Mindestanforderungen ist bei der Auswahl von Herstellern und Integratoren zwingend zu berücksichtigen.

Die MBN 9666 besteht aus mehreren Teilen und Beiblättern. Die entsprechenden Werknormteile sowie Beiblätter können über den DocMaster eingesehen werden. Eine Liste aller Dokumentteile der MBN 9666-Reihe kann über DocMaster angezeigt werden.

Wenn im folgenden Verlauf von „Daimler-Konzern“ oder kurz „Daimler“ gesprochen wird, sind die Daimler AG, Daimler Trucks AG und Mercedes-Benz AG miteingeschlossen.

Anwendungsvermerk:

Entsprechend dem Anwendungsbereich ist die Anwendung der vorliegenden Fassung dieser Werknorm übergreifend für neue Fahrzeugprojekte oder Komponenten zu prüfen, für die zum Ausgabedatum dieser Fassung noch kein Konzeptheft/Rahmenheft oder Komponentenlastenheft verabschiedet wurde.

Die verbindliche Anwendung der vorliegenden Fassung dieser Werknorm durch den Zulieferer regeln die jeweiligen Vertragsunterlagen.

Änderungen

Diese Ausgabe ersetzt die vorherige Ausgabe dieser Norm.

Gegenüber der Ausgabe 2019-09 wurden folgende Änderungen vorgenommen:

- Zusammenführung der Inhalte aus der „MBN 9666-9 - Ausgabe 2019-09“ und den „IT-Security Vorgaben für Systemintegratoren – Ausgabe 09.b 2019-03“ der SITS Toolbox.
- Übernahme der Gliederung aus „IT-Security Vorgaben für Systemintegratoren – Ausgabe 09.b 2019-03“ der SITS Toolbox.
- Aufgrund der grundsätzlichen Strukturänderung wurden in den Kapiteln entsprechend Referenz zum inhaltlichen Vergleich auf die vorherige Version der MBN gesetzt.

Inhaltsverzeichnis

1 Anwendungsbereich

Vorliegende MBN 9666-9 definiert Anforderungen an die Informationssicherheit bei der Beschaffung neuer Anlagen und Maschinen durch Daimler.

Sind aus Anbietersicht zu einzelnen Punkten Abweichungen aus technischen/technologischen Gesichtspunkten notwendig, so sind diese im Angebot auszuweisen und müssen vorab von der jeweiligen Daimler-Fachabteilung/Projektleitung schriftlich genehmigt werden.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

MBN 9666-1	Teil 1: Allgemeine Anforderungen
MBN 9666-3	Teil 3: Elektrische Ausrüstung

3 Begriffe und Definitionen

Begriff	Definition
Lieferanten	Der Begriff Lieferant fasst verschiedene Vertragspartner zusammen. Zur Abgrenzung der einzelnen Formen, wurden die Akteure hier weiter spezifiziert (Definitionen in dieser Tabelle): Integrator (auch Systemintegrator/Anlagenintegrator) Anlagenlieferant (auch Anlagenhersteller) Es ist möglich, dass die einzelnen Lieferanten nicht immer eindeutig unterschieden werden können bzw. dass ein Akteur mehrere Rollen übertragen bekommt. Dies muss projektspezifisch betrachtet werden.
Integrator	Der Integrator ist für den Aufbau und die Inbetriebnahme einer Anlage beim Auftraggeber zuständig. Es kann sich dabei um den Anlagenlieferanten selbst handeln, aber auch um einen weiteren Akteur. Die Rolle kann von einem internen Mitarbeiter oder einem externen Lieferanten übernommen werden.
Anlagenlieferant	Der Anlagenlieferant (auch Anlagenhersteller) liefert technische Anlagen oder Teile davon. Diese müssen die von der Daimler AG definierten informationssicherheitsrelevanten Anforderungen erfüllen.
Komponentenhersteller	Der Komponentenhersteller liefert einzelne Systemkomponenten für die Automatisierungslösungen (keine Anlagen) direkt an Daimler oder an Anlagenlieferanten oder Integratoren, die diese Komponenten in den Anlagen für Daimler verbauen. Diese müssen die von der Daimler AG definierten informationssicherheitsrelevanten Anforderungen erfüllen.
Betreiber	Der Betreiber ist während des gesamten Lebenszyklus der Automatisierungslösung für den Betrieb, die Wartung und notwendige Anpassungen bis hin zum Abbau verantwortlich.
Automatisierungslösung	Unter einer Automatisierungslösung werden alle Komponenten verstanden, die automatisiert oder teilautomatisiert am Produktionsprozess beteiligt sind.
Incident	Unter einem Incident versteht man eine Störung im IT-Betrieb.
Security Development	Unter Security Development werden Methoden der Softwareentwicklung verstanden, die zum Ziel haben, im Sinne der Informationssicherheit möglichst robuste und widerstandsfähige Software zu entwickeln.

Single Sign-on (SSO)	Bei Single Sign-on handelt es sich um eine Authentifizierungsmethode, die nach einmaliger Authentifizierung einen Zugriff auf weitere berechtigte Systeme und Dienste ohne erneute Authentifizierung ermöglicht.
Industrial Control System (ICS)	Bei einem Industrial Control System handelt es sich um ein Automatisierungs- oder Prozesssteuersystem.
Standard-Betriebssysteme	Von Daimler vorgegebene und vorkonfigurierte Betriebssysteme.
Verantwortliche/r des Bereiches für Informationssicherheit	Vom jeweiligen Bereich benannte Person, die während des gesamten Lebenszyklus von IT-Komponenten die Belange der Informationssicherheit verantwortet.
Updates	Ein Update erweitert den Funktionsumfang einer Software, kann aber auch, wie ein Patch, Fehlerbehebungen enthalten.
Patch	Bei einem Patch handelt es sich um ein Stück Software, das einen Fehler oder eine Sicherheitslücke in der Software korrigiert.

4 Allgemeine Anforderungen

Im Hinblick auf Sicherheitsanforderungen und Produktqualität sowie zur Erfüllung der Zertifizierungsanforderungen sind alle relevanten rechtlichen Vorschriften und Gesetze zu erfüllen. Zusätzlich gelten die relevanten Anforderungen des Daimler Konzerns.

In Bezug auf Inhaltsstoffe und Wiederverwertbarkeit müssen Materialien, Verfahrens- und Prozesstechnik, Bauteile und Systeme alle geltenden gesetzlichen Bestimmungen erfüllen.

5 Anforderungen der Informationssicherheit

Eine wesentliche Zielsetzung der Informationssicherheit ist es, die Verfügbarkeit, Vertrauenswürdigkeit und Integrität von Produktionsanlagen sicherzustellen. Hierzu ist die Implementierung einer umfassenden Sicherheitsstrategie basierend auf den in diesem Dokument beschriebenen Anforderungen und Maßnahmen notwendig. Neben der Implementierung geeigneter Maßnahmen direkt in den eingesetzten Komponenten (Hard- und Software) ist die Einbindung in die zentralen Sicherheits- und Betriebswerkzeuge ein entscheidender Schritt, um das notwendige Sicherheitslevel kontinuierlich aufrecht zu halten.

Bei allen Abstimmungen zu Anforderungen oder sonstigen Themen aus diesem Dokument ist der Verantwortliche des Bereiches für Informationssicherheit einzubinden.

In den folgenden Abschnitten werden die von Daimler gestellten Anforderungen bezüglich IT-Sicherheit für Anlagen und Maschinen aufgezeigt.

6 Sicherheitsanforderungen an Lieferanten

6.1 Organisatorische Sicherheitsanforderungen

6.1.1 IT-Security Awareness Training

Jegliches Personal, das bei Lieferung, Aufbau, sowie Inbetriebnahme einer Anlage beteiligt ist, dies inkludiert Mitarbeiter, Auftragnehmer, Subunternehmer, sowie Consultants, müssen eine IT-Security Awareness Schulung nachweisen. Folgende Anforderungen sind zu erfüllen:

- Nachweis einer IT-Security Schulung des Personals. Diese soll zumindest folgende Themen beinhalten:
  - Grundlegende Informationen zur Informations- und Datensicherheit
  - Bedrohungspotenzial durch Schadsoftware
  - Gefährdungspotenzial durch Social Engineering (Phishing, E-Mails)
  - Physische Sicherheit am Arbeitsplatzrechner und Programmiergerät
  - Umgang mit mobilen Datenspeichern
  - Risiken und Gefahren bei der Verwendung von mobilen Geräten (Hotspots, Speicherung von Firmendaten)
  - Erkennen und Identifizierung von sicherheitsrelevanten Ereignissen, Unregelmäßigkeiten und Veränderungen in Prozessen, Systemen, Netzwerkverkehr, Applikationen und Daten
  - Verhalten bei sicherheitsrelevanten Ereignissen
  - Informationspflichten bei erkannten Ereignissen oder Gefahren, sowie vertragliche Meldungspflichten
- Der Lieferant muss die erfolgreiche Teilnahme jeglichen Personals an der Schulung sicherstellen.
- Der Lieferant muss einen Ansprechpartner definieren, der während allen Phasen der Anlagenlieferung, dies inkludiert die Angebotsphase, Lieferung, Aufbau und Inbetriebnahme, für den Bereich der IT-Sicherheit verantwortlich ist.
- Der Lieferant soll durch eine Richtlinie die regelmäßige Aktualisierung der Schulungen sicherstellen.

Referenz		IEC 62443-2-4: SP.01.01, SP.01.02, SP.01.03

6.1.2 Einsatz freigegebener Systeme und Komponenten

Im Rahmen der Beschaffung von IT-Systemen für die Produktion, sind die durch Daimler vorgegebenen Systeme bei der Beschaffung verpflichtend zu berücksichtigen. Aktuelle Informationen zu den durch Daimler definierten Systemen sind über den Einkauf und den jeweiligen Projektverantwortlichen (Daimler) einzuholen. Abweichungen von den definierten Standards sind mit dem jeweiligen Projektverantwortlichen (Daimler) und dem Informationssicherheits-Verantwortlichen des Werkes abzustimmen.

Der Lieferant ist verpflichtet durch Daimler freigegebene Komponenten in der Anlage einzusetzen. Folgende Anforderungen sind zu erfüllen:

- Die in der Anlage einzusetzenden Komponenten müssen durch Daimler freigegeben werden. Freigegebene Komponenten sind in einer Daimler-spezifischen Materialfreigabeliste, siehe spezifische Anforderungen, definiert.
- Sobald Komponenten eingesetzt werden, die nicht durch Daimler freigegeben sind, sind diese durch den Integrator nach Daimler-Vorgaben sicherheitstechnisch zu untersuchen und durch Daimler freizugeben.

Spezifische Anforderungen
2.1.2 Mercedes-Benz Powertrain
2.1.2 Mercedes-Benz Aufbau

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.1, 5.3.2	

6.1.3 Physische Sicherheit und Zugangsschutz

Physische Sicherheit wird eingesetzt, um unautorisierte Zugriffe auf Systeme und Komponenten zu erkennen, zu verzögern, sowie zu verhindern, um die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme oder Daten nicht zu beeinträchtigen. IT-Komponenten und IT-nahe Produktionsendgeräte sind durch den Integrator so aufzubauen, dass sie ab- oder eingeschlossen betrieben werden. Folgende Anforderungen sind durch den Integrator zu erfüllen:

- Peripherie und Schnittstellen, die für administrative Zwecke genutzt werden, müssen verschlossen sein und dürfen nur einem beschränkten Personenkreis zugänglich sein. Nur für den normalen Betrieb notwendige Peripherie und Schnittstellen dürfen frei zugänglich sein.
- Die Komponenten sind laut Daimler Vorgabe vor unbefugtem Zugriff zu schützen. Nur für den normalen Betrieb notwendige Peripherie und Schnittstellen dürfen frei zugänglich sein. Die Ports der Komponenten sollen nicht frei zugänglich sein. Schnittstellen für den administrativen Zugang sollten nicht frei zugänglich sein.
- Kabel zu und von den Komponenten sind laut Daimler Vorgabe zu verlegen. Bei keiner definierten Vorgabe sind diese zumindest verdeckt (z.B. Kabelkanal) zu verlegen.
- Der Zugangsschutz der Anlage und der Anlagenkomponenten, soll im gesamten Zeitraum des Aufbaus, sowie während der Inbetriebnahme-und Servicetätigkeiten sichergestellt sein. Dies beinhaltet, dass nur berechtigte Personen Zugriff / Zugang zu der Anlage bzw. der Anlagenkomponenten erhalten. Jegliche Auffälligkeiten, Änderungen und Verletzungen der IT-Sicherheitsvorgaben, siehe Kapitel 6.1.1, sollen umgehend gemeldet werden, siehe 6.2.2.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.1	

6.2 Awareness und Verhalten während des Aufbaus

6.2.1 Verhalten während der Inbetriebnahme und bei Serviceeinsätzen

Jegliches Personal, das bei Aufbau, Inbetriebnahme und Serviceeinsätzen einer Anlage beteiligt ist, dies inkludiert Mitarbeiter, Auftragnehmer, Subunternehmer, sowie Consultants, müssen alle Arbeiten unter Einhaltung der Daimler IT-Sicherheitsvorgaben durchführen. Folgende Anforderungen sind zu erfüllen:

- Der Umgang mit Hardware und anderem IT-Equipment soll unter Berücksichtigung der IT-Sicherheits-Themen der Awareness Schulung, siehe Kapitel 6.1.1, nach Best Practice Guidelines, sowie nach Daimler Vorgaben eingehalten werden.
- Der Umgang mit Arbeitsgeräten, welche auf das Netzwerk von Daimler zugreifen können, Zugriff zu Komponenten in der Anlage haben, sowie für die Programmierung von Komponenten eingesetzt werden (z.B. Programmiergeräte, Mobiltelefone, Notebooks), muss nach Best Practice IT-Sicherheitsguidelines (siehe Anhang C) erfolgen. Dies inkludiert zumindest folgende Punkte:
    - Einhaltung der IT-Sicherheitsvorgaben.
    - Der Einsatz von unerlaubter, potentiell bösartiger Software ist nicht gestattet.
    - Der Zugriff auf unbekannte, potentiell bösartige, Daten und Webseiten außerhalb des Daimler Netzwerks ist verboten.
    - Sämtliche Anlagen-spezifische Daten und Programme auf den Endgeräten sind vor unautorisiertem Zugriff zu schützen (z.B. durch Ändern von Standard-Passwörtern, siehe 6.5.2).
    - Bewusstsein über Informationspflichten, Meldung und Verhalten bei sicherheitsrelevanten Ereignissen oder erkannten Gefahren.
- Jegliches IT-Equipment muss über einen aktuellen Virenscanner verfügen, sofern anwendbar. Vor dem Einsatz in der Daimler Infrastruktur sind die Geräte auf Malware zu prüfen. Dies kann stichprobenartig durch Daimler überprüft werden.
- Für den Anschluss an das Daimler-Netzwerk muss der Betreiber eine Genehmigung beim Standortverantwortlichen des Werkes einholen. (MBN 5.3.1)

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.3.1	IEC 62443-2-4: SP.10.05 BR

6.2.2 Identifizierung und Meldung von IT-Sicherheitsproblemen

Während der Inbetriebnahme- und Servicetätigkeiten sollen jegliche Auffälligkeiten, Änderungen und Verletzungen der IT-Sicherheitsvorgaben identifiziert und gemeldet werden. Folgende Anforderungen sind zu erfüllen:

- Überwachung der Inbetriebnahme- und Servicetätigkeiten auf Unregelmäßigkeiten, dazu zählen:
  - Verlust/Diebstahl/Zerstörung von Hardware und anderem IT-Equipment.
  - Missbrauch von Zugangsdaten wie Benutzername oder Passwort.
  - Verlust oder Kompromittierung von Zugangsdaten (z.B. Passwort wird durch Social Engineering vom Angreifer erbeutet, Passwort Cracking, Passwörter auf unverschlüsselten Datenträgern).
  - Ungewöhnliches Applikationsverhalten oder undefinierte Applikationszustände (z.B. ungewöhnlich hoher Datentransfer, ungewöhnlicher Netzwerkverkehr, Applikation reagiert langsamer als gewöhnlich).
  - Befall von Malware (Virus, Trojaner, Spyware, etc.).
  - Prozessschwäche oder Leistungsminderung (z.B. fehlende Datensicherung; Datenverlust nach Change/Migration).
  - Unautorisierter Zutritt zum Anlagenbereich bzw. -komponenten, sowie unautorisierter Zugriff auf Anlagenkomponenten.

- Der Lieferant muss eine erkannte Verletzung der IT-Sicherheitsvorgaben umgehend an eine der folgenden Instanzen melden:
  - den zuständigen Projektverantwortlichen
  - die Mailbox: cyber.security@daimler.com

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.6.4	

6.2.3 Umgang mit Speichermedien

Werden während des Aufbaus, Inbetriebnahme und Serviceeinsätze einer Anlage Speichermedien eingesetzt, so müssen diese zusätzlich gesichert werden. Folgende Anforderungen sind zu erfüllen:

- Werden externe Speichermedien (z.B. USB-Sticks) eingesetzt, so sind diese vor dem Einsatz auf Malware zu überprüfen. Dies kann durch folgende Möglichkeiten durchgeführt werden:
  - Überprüfung mit einem Virenscanner auf einem Endgerät, der über tagesaktuelle Signaturen verfügt.
  - Der Scan ist nach anderweitigem Gebrauch des Speichermediums zu wiederholen.
- Die durchgeführte Überprüfung der Speichermedien muss nachgewiesen werden.
- Wird bei der Überprüfung eines Speichermediums Malware gefunden, so muss dies umgehend wie unter 6.2.2 beschrieben an Daimler gemeldet werden.
- Zusätzliche Schutzmechanismen der Speichermedien (z.B. Verschlüsselung) sind basierend auf IT-Security Best Practice (siehe Anhang C) umzusetzen.
- Speichermedien müssen vor unautorisiertem Zugriff, missbräuchlicher Verwendung oder Verfälschung während des Transports geschützt werden.
- Speichermedien müssen, wenn sie nicht mehr benötigt werden, sicher und unter Anwendung formaler Verfahrensanweisungen, basierend auf IT-Security Best Practice, entsorgt werden.
- Werden Speichermedien vor oder nach Abschluss der Arbeiten nicht mehr benötigt, so sind jegliche Daten, die während dem Einsatz gespeichert wurden, sicher, unwiderruflich und dauerhaft zu löschen.

Referenz		IEC 62443-2-4: SP.10.05 RE(2) CSSA 4.2, 9.2-1

6.2.4 Umgang mit Mobiltelefonen/Smartphones

Werden während des Aufbaus, Inbetriebnahme und Serviceeinsätze einer Anlage Mobiltelefone mit Zugriff auf das Daimler WLAN bzw. Internet eingesetzt, so unterliegt der Einsatz dieser, besonderen Regelungen. Diese Regelungen gelten nur, wenn ein mobiles Endgerät z.B. Smartphone mit der Anlage oder einer Anlagenkomponente verbunden wird.

Folgende Anforderungen sind zu erfüllen:

- Der Umgang mit Mobiltelefonen, welche auf das WLAN Netzwerk von Daimler zugreifen (außer Guest-Connect), bzw. Zugriff zu Komponenten in der Anlage haben, muss nach Best Practice IT-Sicherheit Guidelines[1] erfolgen. Dies inkludiert zumindest folgende Punkte:
    - Einhaltung der IT-Sicherheit Vorgaben.
    - Die Mobiltelefone müssen mit einer PIN gesperrt sein. Diese ist nach IT-Security Best Practice zu erstellen (z.B. keine einfache Kombination wie „1234“).
    - Der Einsatz von unerlaubter, potenziell bösartiger Software auf den Mobiltelefonen ist nicht gestattet.
    - Der Zugriff auf unbekannte, potenziell bösartige, Daten und Webseiten außerhalb des Daimler Netzwerks ist verboten.
    - Sämtliche Anlagen-spezifische Daten und Programme auf den Endgeräten sind vor unautorisiertem Zugriff zu schützen.
    - Das mutwillige Verändern des Betriebssystems („Rooten“) ist nicht gestattet.
    - Mobiltelefone dürfen nicht als Speichermedium genutzt werden.

- Werden Mobiltelefone als Hotspot (WLAN für externe Geräte) eingesetzt, gelten alle IT-Sicherheitsanforderungen der Punkte 6.2.1 und 6.2.2. Darüber hinaus werden folgende Anforderungen gestellt:
    - Über den Hotspot darf keine Verbindung in das Daimler Anlagennetzwerk hergestellt werden oder möglich sein.
    - Die Sicherheitsmechanismen müssen den Best Practice IT-Sicherheitsstandrads (siehe Anhang C) entsprechen: Als WLAN Verschlüsselung ist mindestens WPA2 einzusetzen. Das Passwort ist sicher zu wählen, siehe Daimler Passwortvorgabe bzw. IT-Security Best Practice (siehe Anhang C).
    - Ein bewusster und sicherer Einsatz des Hotspots, sowie Zugriff auf das Internet wird vorausgesetzt.
    - Mobiltelefone sind vor dem Einsatz auf Malware zu überprüfen. Dies kann durch einen aktuellen Virenscanner auf dem Endgerät erfolgen. Dieser Scan ist nach anderweitigem Gebrauch des Mobiltelefons zu wiederholen.
- Zusätzliche Schutzmechanismen (z.B. Verschlüsselung) sind basierend auf IT-Security Best Practice (siehe Anhang C) umzusetzen.
- Werden Mobiltelefone vor oder nach Abschluss der Arbeiten nicht mehr benötigt, so sind jegliche Daten, die während dem Einsatz gespeichert wurden, sicher, unwiderruflich und dauerhaft zu löschen.

Referenz		IEC 62443-2-4: SP.10.05 RE(2) CSSA 3.3

[1] Siehe Anhang C

6.3 Anlagendokumentation und Konfigurationsmanagement

MBN 9666-1 (Kapitel: Dokumentation) ist zu beachten.

Die Anlage ist dokumentiert zu übergeben. Dies bedeutet, dass die in den nachfolgenden Unterkapiteln genannten Dokumente zu erstellen und an Daimler zu übergeben sind.

6.3.1 Betriebshandbuch für Informationssicherheit (BHB InfoSec)

Das BHB InfoSec kann als separates Dokument oder als Bestandteil der normalen Betriebsdokumentation erstellt werden. Es muss Informationen zu folgenden Themen enthalten:

- Interne Architektur der Software und Hardware
- Kernfunktionen der Anlage und ihrer Komponenten
- Bedrohungsanalyse
- Übersicht bekannter Schwachstellen bewertet nach CVSS mindestens Version 3
- Verwendete Hard- und Software inklusive der eingesetzten Bibliotheken
- Schnittstellendokumentation
- Systemanforderungen und Rahmenbedingungen
- Ggf. bekannte Probleme und Schwachstellen inklusive der von Daimler genehmigten Ausnahmen

Ein Template für ein Betriebshandbuch für Informationssicherheit ist im Anhang A enthalten. Existieren Teile des Betriebshandbuches für Informationssicherheit bereits in anderen Dokumenten, kann auf diese verwiesen werden.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.8.1	

6.3.2 Asset Dokumentation

Es müssen alle wesentlichen Komponenten der Anlage dokumentiert sein. Dies sind mindestens alle Komponenten, die für die Kommunikation genutzt werden, die Daten der Anlage verarbeiten und alle Komponenten, die eine wesentliche Funktion (Zweckerfüllung, Safety und Informationssicherheit) innerhalb der Anlage ausführen. Folgende Anforderungen sind zu erfüllen:

- Die Erfassung der Daten muss in den Werkzeugen von Daimler (Asset-Datenbank) oder in einem von Daimler vorgegebenen Format erfolgen. Die jeweiligen Werkzeuge sind in den spezifischen Anforderungen definiert.
- Die Asset-Dokumentation muss zumindest folgende Informationen beinhalten:
    - Gerätename
    - MAC Adresse
    - IP Adresse & Adressierung (DCP, DHCP, STATIC)
    - Geräteklasse
    - Gerätetyp
    - Subnetzmaske
    - Router Eintrag (Gateway)
    - Bestellnummer
    - Seriennummer
    - FW-Version / Betriebssystem Versionen
    - Hardware Revision

Spezifische Anforderungen
2.3.1. Mercedes-Benz Aufbau
2.3.1. Mercedes-Benz Powertrain

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.8.3	

6.3.3 Dokumentation Kommunikationsbeziehungen

Zum Schutz der Produktionsanlagen werden seitens Daimler Hardware Firewalls eingesetzt. Für die Kommunikation innerhalb der Anlage und zu Systemen außerhalb der Anlage müssen daher die Kommunikationsbeziehungen vor Inbetriebnahme als Kommunikationsmatrix dokumentiert werden. Nicht dokumentierte Kommunikationsbeziehungen werden seitens Daimler nicht freigeschalten.

Die Dokumentation muss mindestens folgende Informationen enthalten:

Quelle	Name Quellsystem	Name des Quellsystems
	Quelladresse IP	IP-Adresse des Quellsystems
	Quelladresse DNS	DNS-Name des Quellsystems
Ziel	Name Zielsystem	Name des Zielsystems
	Zieladresse IP	IP-Adresse des Zielsystems
	Zieladresse DNS	DNS-Name des Zielsystems
Dienst	Dienst	Welcher Dienst wird genutzt z.B. Web Service
	Protokoll	Eingesetztes Kommunikationsprotokoll z.B. https
	Port	Eingesetzte Ports z.B. TCP 443
Zusätzliche Angaben	Applikation	Für welche Applikation wird die Kommunikation benötigt z.B. Auftragssteuerung
	Beschreibung	Aussagekräftige Beschreibung für was die Kommunikation benötigt wird
	Weitere Informationen	Ggf. weitere Angaben

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.8.4	IEC 62443-2-4: SP.03.09 BR

6.3.4 Dokumentation Anlagennetzwerk als Netzwerkplan

Die Kommunikation innerhalb der Anlage und zu Systemen außerhalb der Anlage muss als grafischer Netzwerkplan dokumentiert werden. Die Übersicht aller Kommunikationsteilnehmer und der physischen und logischen Kommunikationsverbindungen soll dokumentiert werden. Folgende Anforderungen sind zu erfüllen:

- Im Netzwerkplan ist der aktuelle Ist-Zustand des Netzwerkes der Anlage festzuhalten. Die Dokumentation hat in übersichtlicher Weise und vollständig zu erfolgen.
- Erfolgt die Dokumentation nicht direkt in den von Daimler bereitgestellten Werkzeugen, ist Art und Umfang der Dokumentation mit dem Verantwortlichen für Informationssicherheit oder dem Projektverantwortlichen von Daimler abzustimmen.

Spezifische Anforderungen
2.3.3. Mercedes-Benz Aufbau

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.8.4	

6.4 Netzwerk- und Kommunikationssicherheit

6.4.1 Netzwerksicherheit LAN

Das Netzwerk, das den Produktionsprozess direkt unterstützt, muss bei der Planung, dem Aufbau und beim Betrieb von Produktionszellen folgende Anforderungen erfüllen:

- Diagnosefunktionen sind laut Daimler Vorgabe zu implementieren, siehe spezifische Anforderungen.
- Unterschiedliche Sicherheitslevel innerhalb der Anlage sind durch eine geeignete Segmentierung zu realisieren. Die umzusetzende Netzwerkarchitektur wird von Daimler vorgegeben und muss nach der Umsetzung von Daimler abgenommen werden.
- Die Kommunikationsbeziehungen müssen definiert und dokumentiert sein. (siehe 6.3.2)
    - Die Kommunikation muss auf das Notwendigste beschränkt werden.
    - Die Kommunikationsbeziehungen müssen bei Inbetriebnahme auf Plausibilität überprüft werden.
- Der Einsatz von abweichenden Maßnahmen ist erst nach Überprüfung und Freigabe durch Daimler erlaubt. Die Maßnahmen müssen einen gleichwertigen oder besseren Schutzlevel für Informationssicherheit nachweisen können.
- Eine direkte Anbindung der Anlage an das Internet ist nicht zulässig. Der Zugriff auf das Internet darf ausschließlich nach Genehmigung durch Daimler über den Internet-Proxy / das DCN von Daimler zu erfolgen. Eine dauerhafte Anbindung an das Internet darf keine Voraussetzung für den regulären Betrieb der Anlage sein.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.5.3, 5.5.4	IEC 62443-3-3: SR 5.1 CSSA 3.1

6.4.1.1 Anlagennetzwerk

Die umzusetzenden Netzwerkkonzepte werden seitens Daimler vorgegeben. Folgende Anforderungen sind zu erfüllen:

- Der Aufbau, die Einrichtung, sowie die Absicherung der Netzwerkübergabepunkte an das Daimler Netzwerk, sind durch Daimler Guidelines vorgegeben. Für spezielle Anforderungen der Teilbereiche, siehe spezifische Anforderungen.
- Kommen lokale Anlagenfirewalls zum Einsatz erfolgt Lieferung und Montage der Firewall über den Auftragnehmer. Parametrierung wird bauseits vom technischen Betreiber durchgeführt. Die Dokumentation der Kommunikationsbeziehungen muss vom Auftragnehmer erstellt werden, siehe Kapitel 6.3.2.

Spezifische Anforderungen
2.4.1.1. Mercedes-Benz Powertrain

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.5	

6.4.1.2 Integration in das Common Network und zentrale Security Systeme

Die Integration in das Daimlernetzwerk muss nach der durch Daimler bereitgestellten Guideline erfolgen.

- Die Integration erfolgt über Daimler bereitgestellte Netzwerkübergabepunkte (RJ45 Dose, LWL-Spleißbox). Ein entsprechender Platzvorhalt im Schaltschrank/Netzwerkschrank ist vom Auftragnehmer vorzusehen. Die eingesetzte Netzwerktechnik ist basierend auf der Guideline zu implementieren.
- Die von Daimler geforderten Komponenten der Anlage müssen an die zentralen Systeme von Daimler angebunden werden. Die von Daimler dafür bereitgestellten Systeme müssen verwendet werden. Details sind mit dem Daimler-Verantwortlichen des Bereiches für Informationssicherheit abzustimmen.
- Die Vorgehensweise zur Umsetzung ist in einem Daimler internen Planungs- und Aufbauprozess beschrieben.
- Sicherheitsrelevante Informationen müssen über Standardschnittstellen (z. B. Syslog, XML usw.) verfügbar, herstellerunabhängig auswertbar und frei nutzbar sein.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.5.2	IEC 62443-2-4: SP.03.02 BR + RE(1) + RE(2)

6.4.2 Netzwerksicherheit WLAN

Sollte der Einsatz von WLAN aus produktionstechnischen Gründen notwendig sein, so muss der Einsatz durch Daimler genehmigt und freigegeben werden. Für den Einsatz von WLAN dürfen nur durch Daimler freigegebene Komponenten eingesetzt werden. WLAN kommt nur dann zum Einsatz, wenn die Mobilität der Endgeräte zwingend erforderlich und mit wesentlichen Vorteilen verbunden ist.

Es werden zwei Arten von WLANs bei Daimler eingesetzt. Abhängig davon wird die WLAN-Infrastruktur geplant.

- IT-WLAN (Nachrichtentechnik): Für genehmigte Anwendungsfälle sollte primär das bestehende Daimler IT-WLAN verwendet werden. Dabei muss die WLAN-Infrastruktur nicht eigens geplant werden.
- Anlagen-WLAN (Layer2-Kommunikation): Wird ein spezifisches Anlagen-WLAN benötigt, so muss die erforderliche WLAN-Infrastruktur mit ITI/GN (Netzwerkplanung des Auftragsgebers) geplant werden.
- Wird Wireless LAN, unabhängig der Art, eingesetzt, so sind folgende Anforderungen zu erfüllen:
    - Der gesamte Aufbau des WLAN Netzes (Erlaubte Frequenzen, SSIDs) muss basierend auf der Daimler WLAN Guideline (GWSA) erfolgen. Der Einsatz von abweichenden Parametrierungen, Technologien oder Funktionen ist nicht gestattet.
    - Der Lieferant muss spezifische Protokolle und andere detaillierte Informationen dokumentieren, die für die Kommunikation von drahtlosen Geräten mit dem Steuerungsnetzwerk erforderlich sind, einschließlich anderer drahtloser Geräte, die mit den vom Lieferanten gelieferten Geräten kommunizieren können.
    - Der Lieferant muss dokumentieren, dass Sicherheitsmechanismen und -protokolle eingesetzt werden. Diese müssen nach Best Practice IT-Sicherheitsstandards (siehe Anhang C) erfolgen (keine unverschlüsselte WLAN Kommunikation oder unsichere Protokolle wie WEP, WPS).

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.7.1, 5.7.4	IEC 62443-2-4: SP.04.01 BR, SP.04.02 BR+RE(1), SP.04.03 BR

6.4.3 Absicherung von Funktechnologien

Zusätzliche Funkprotokolle (z.B. ZigBee, LTE/UMTS/GSM, BLE, LoRaWAN) bieten aufgrund ihrer physischen Ausbreitung eine potentielle Angriffsoberfläche und müssen daher abgesichert werden. Für den Einsatz von Funktechnologien dürfen nur durch Daimler freigegebene Komponenten eingesetzt werden und nach Daimler Vorgaben konfiguriert werden (GWSA). Werden Funktechnologien genutzt, müssen diese inklusive ihrer Use Cases (Inhalt der Datenübertragung) vollständig dokumentiert sein. Bei der Verwendung von Wireless-Technik zur Datenübertragung ist grundsätzlich ein sicheres Transportprotokoll einzusetzen. Daten, die aufgrund von Anforderungen an die Integrität zu schützen sind, müssen durch geeignete Verfahren geschützt werden (z. B. Verschlüsselung, sowie kryptographisch gestützte Authentisierung und Integritätsprüfung).

Folgende Anforderungen sind zu erfüllen:

- Der Lieferant muss spezifische Protokolle und andere detaillierte Informationen dokumentieren, die für die Kommunikation von drahtlosen Geräten mit dem Steuerungsnetzwerk erforderlich sind, einschließlich anderer drahtloser Geräte, die mit den vom Lieferanten gelieferten Geräten kommunizieren können.
- Der Lieferant muss den Verwendungszweck, technische Eigenschaften und Einsatzmöglichkeiten der drahtlosen Geräte dokumentieren.
- Der Lieferant muss die Leistungs- und Frequenzanforderungen der drahtlosen Geräte dokumentieren.
- Die eingesetzten Funktechnologien und die zugehörigen Geräte müssen den Standardanforderungen für Betrieb und Sicherheit entsprechen, die in den geltenden Drahtlosstandards oder -spezifikationen festgelegt sind. Der Einsatz ist zu dokumentieren.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.7.1, 5.7.4	IEC 62443-2-4: SP.04.01 BR, SP.04.02 BR+RE(1), SP.04.03 BR, CSSA 6

6.4.4 (Fern-) Wartung

Es darf nur die durch Daimler freigegebenen (Fern-) Wartungslösung eingesetzt werden. Der Einsatz von alternativen Applikationen ist nicht gestattet. Folgende Anforderungen sind zu erfüllen:

- (Fern-) Wartungszugänge müssen zu jedem Zeitpunkt ausschließlich unter der Kontrolle von Daimler liegen.
- Permanente Zugänge sind zu vermeiden und nur in von Daimler genehmigten Fällen zulässig. Ohne eine detaillierte Risikoabschätzung und Maßnahmen die einen ungewollten Datenabfluss verhindern, sind solche Verbindungen unzulässig.
- Die Initiierung der Fernwartung erfolgt durch Daimler, hierfür erfolgt die Freigabe der Fernwartung innerhalb eines Freigabeprozesses. Der Freigabeprozess muss auch einen Notfallprozess beinhalten.
- Der Fernwartungszugriff muss entweder dem 4-Augen-Prinzip unterliegen oder über personalisierte Accounts erfolgen.
- (Fern-) Wartungszugänge müssen überwacht, protokolliert und dokumentiert werden. Erfolgt die Freigabe seitens Daimler ohne individuelle Freigabe je Fernwartung, sind zyklische Fernwartungszugriffe besonders zu überwachen und zu kontrollieren.
- Eine direkte Verbindung zwischen (Fern-) Wartungssystem und Anlage muss vermieden werden. Ein direkter Zugriff auf die Anlage ist nur im Notfall erlaubt und muss dokumentiert werden.
- Der Lieferant muss gewährleisten, dass auf den gelieferten PCs das von Daimler freigegebene Fernwartungstool installiert werden kann.

Spezifische Anforderungen
2.4.4. SPPA Mercedes-Benz Powertrain

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.5.5	IEC 62443-2-4: SP.07.01-SP.07.04, CSSA 8.1

6.4.5 IoT und Cloud Technologien

Moderne IoT-Lösungen müssen besonders abgesichert werden. Darunter fallen vernetzte Komponenten, die untereinander, mit anderen Anlagen oder dem Internet kommunizieren und Informationen austauschen können. Die hierfür notwendigen Maßnahmen müssen über eine Bedrohungsanalyse hergeleitet und von Daimler genehmigt werden.

Die Nutzung von Cloud-Services muss Daimler mitgeteilt und im Vorfeld durch den Informationssicherheits-Verantwortlichen des Werkes von Daimler genehmigt werden. Für die Genehmigung durch Daimler ist ein Nachweis über die Absicherung des Cloud-Services, basierend auf den Best Practice IT-Sicherheitsstandrads (siehe Anhang C), vorzulegen oder eine Bedrohungsanalyse durchzuführen.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.7.2, 5.7.3	

6.5 Schutz von Endgeräten

6.5.1 Sichere Konfiguration

Unter einer sicheren Konfiguration wird verstanden, dass nur benötigte Dienste, Funktionen und Schnittstellen aktiv sind und dass die gängigen Best Practice-Empfehlungen umgesetzt sind. Die Daimler Vorgaben für die Konfiguration von Komponenten ist einzuhalten.

Folgende Anforderungen sind für die bei Daimler zum Einsatz kommenden Systeme zu erfüllen:

- Nicht benötigte Software und Funktionen sollen entfernt oder deaktiviert und dokumentiert werden. Dies umfasst unter anderem:
    - Nicht verwendete Netzwerk- und Kommunikationsprotokolle
    - Nicht verwendete Verwaltungsprogramme, Diagnose-, Netzwerk- und Systemverwaltungsfunktionen
    - Sicherungen von Dateien, Datenbanken und Programmen, die nur während der Systementwicklung verwendet werden
    - Gerätetreiber für Produktkomponenten, die nicht beschafft wurden
    - Nicht verwendete Daten und Konfigurationsdateien

- Ist der Lieferant einer Produktsoftware gleichzeitig auch der Hersteller, soll dieser eine Dokumentation der Software des Produkts, dies inkludiert Skripte, Laufzeitkonfigurationsdateien und -interpreter, Datenbanken und jegliche Software, erstellen. Diese soll Versionen, Revisionen und Patch Levels beinhalten. Die Dokumentation muss alle Ports und autorisierten Dienste enthalten, die für den normalen Betrieb, den Notfallbetrieb oder die Fehlerbehebung erforderlich sind.
- Die Anbindung an ein Security Monitoring System, muss nach Daimler Vorgaben möglich sein.
- Der Lieferant soll alle Dienste und/oder Ports am Produkt nach Daimler Vorgabe konfigurieren. Bei fehlender oder allgemeiner Vorgabe sollen alle Dienste und/oder Ports, welche nicht für den normalen Betrieb, den Notfallbetrieb oder die Fehlerbehebung erforderlich sind, deaktiviert werden. Dies inkludiert logische Kommunikations-Ports und physische Schnittstellen. Der Lieferant muss eine Dokumentation aller Ports, Anschlüsse und Schnittstellen bereitstellen.
- Neben der sicheren und robusten Übergabe der Anlage muss die Aufrechterhaltung des sicheren und robusten Zustands möglich sein. Hierfür hat der Lieferant darzustellen, wie und durch wen die Anlage bei neu entdeckten Schwachstellen wieder auf das notwendige Sicherheitsniveau gebracht werden kann. Ebenfalls haben der Lieferant zu erklären, dass Daimler bei Ausbleiben geeigneter Maßnahmen eigene Maßnahmen umsetzen darf, um die Sicherheit der Anlage und der angeschlossenen Systeme sicherzustellen, ohne dass hieraus Nachteile für Daimler entstehen (insbesondere Garantieverlust). Der Lieferant hat aufzuzeigen und zu begründen, welche Systeme der Anlage nicht verändert oder ausgetauscht werden dürfen.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.3.5, 5.4.1	CSSA 4

6.5.2 Zugriffschutz und User-Management

Benutzerkonten und Berechtigungen, die für die Anlage genutzt werden, müssen im Sinne einer sicheren Konfiguration folgende Anforderungen erfüllen:

Standard- Passwörter und User

- Keine Nutzung von hartcodierten Passwörtern.
- Keine Nutzung von Default Usern oder Passwörtern.
- Alle Benutzer und Passwörter müssen dokumentiert und änderbar sein. Der Lieferant muss alle vorhandenen Benutzer und die zugehörigen Passwörter für das beschaffte Produkt dokumentieren und an Daimler übergeben. Die Übergabe ist nachzuweisen.
- Der Lieferant muss alle Standardpasswörter für das nach Daimler Vorgabe beschaffte Produkt ändern. Alle Standardpasswörter müssen auf sichere, den Daimler Passwort Policy entsprechenden Passwörtern geändert werden und an Daimler übergeben werden.

User-Management

- Es muss ein User-Management innerhalb der Anlage und deren Applikationen vorhanden sein.
- Benutzerkonten sollen über ein Berechtigungsmanagement verwaltet werden können. Im Idealfall ist dies das Daimler Active Directory.
- Die Nutzung einer starken Authentifizierung für administrative Zugriffe oder bei Zugriffen von außerhalb des anlageninternen Netzwerks ist sicherzustellen.
- Die Trennung von administrativen und produktiv genutzten Berechtigungen muss möglich sein.
- Lokale Gruppen-Accounts mit Autologin dürfen niemals administrative Berechtigungen haben.
- Bei Gruppen-Accounts für administrative Tätigkeiten oder schreibende Zugriffe muss eine Authentifizierung erfolgen und eine Dokumentation an Daimler übergeben werden.
- Zugriffsrechte sind nach dem Least Privilege Prinzip zu vergeben (nur die benötigten Berechtigungen, die für den Zweck notwenig sind)

Log-on Funktionalitäten

- Die Implementierung von Verfahren, die eine einfache Nutzung der Anlage ermöglichen, ohne auf Sicherheit zu verzichten (z. B. Single Sign-on – SSO), sollte möglich sein.
- Sobald die Autologon-Funktonalität aktiviert wird, d.h. keine interaktive Anmeldung möglich ist, muss das User-Interface auf die Anwendung bzw. den Produktionsprozess beschränkt werden, sodass kein Zugriff auf das Betriebssystem möglich ist.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.2, 5.3.1	CSSA 7.1

6.5.3 Malware Schutz

Zum Schutz der Rechnersysteme in der Produktionswelt vor dem Befall durch Malware ist auf jedem System im Produktionsumfeld zwingend der Einsatz einer Antivirus-Software oder eine mit Daimler abgestimmte alternative Maßnahme vorgeschrieben.

Der Lieferant hat den Einsatz der von Daimler vorgeschriebenen Antiviren- oder Härtungs-Software zu ermöglichen. Ist keine dieser Lösungen einsetzbar, muss dies schriftlich begründet und eine Alternativlösung mit Daimler abgestimmt werden.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.4.2	

6.5.3.1 Antivirenschutz

Es ist der bei Daimler standardmäßig verwendete Malwareschutz, für alle Windows-basierten Rechner der Produktionsanlagen, mit aktueller Daimler-Konfiguration einzusetzen.

- Ist der Betrieb des Daimler standardmäßig verwendete Malwareschutzes nicht möglich, ist mit Daimler eine mindestens gleichwertige Alternative abzustimmen und umzusetzen.
- Die Vorgehensweise zur Umsetzung ist in einem Daimler internen Planungs- und Aufbauprozess beschrieben.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.4.2.1	

6.5.3.2 System Härtung

Als zusätzliche oder alternative Malware-Sicherheitsmaßnahme für Systeme wird die Systemhärtung eingesetzt. Folgende Anforderungen sind zu erfüllen:

- Es sind die von Daimler standardmäßig verwendete Systemhärtungs-Lösung und die entsprechend definierten Policies einzusetzen.
    - Der Einsatz der Systemhärtung ist nach Daimlervorgaben umzusetzen. Die Vorgehensweise ist in einem daimlerinternen Planungs- und Aufbauprozess beschrieben.
    - Der Integrator hat sicherzustellen, dass diese Systeme nach der Installation einwandfrei funktionieren.
    - Der Lieferant bzw. Integrator haben sicherzustellen, dass die eingesetzte System Hardening-Policy die Funktionalität des Systems nicht funktionskritisch beeinträchtigt. Notwendige Änderungen sind schriftlich bei Daimler zu begründen und durch Daimler freizugeben.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.4.2.2	

6.5.4 Schwachstellen und Patch Management

- Es ist sicherzustellen, dass die Anlage in das Schwachstellen- und Patch-Management von Daimler integriert werden kann.
- Das Patch Management, sowie die Anbindung an die Daimler Systeme für Updates muss nach Daimler Vorgabe erfolgen. Hierzu ist auf die bei Daimler standardmäßig verwendeten Schwachstellen- und Patch Management-Systeme zurückzugreifen.
- Es ist sicherzustellen, dass alle vernetzten Komponenten der Anlage im Rahmen der Netzkopplung sowie regelmäßig während der Nutzung mittels eines Schwachstellenscans auf vorhandene Schwachstellen überprüft werden können. Der Scan muss innerhalb von maximal 5 Tagen nach der Netzkopplung durchgeführt werden. Des Weiteren muss die Möglichkeit gegeben sein, regelmäßige Schwachstellenscans durchführen zu können.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.6.5	CSSA 5

6.5.5 Netzwerkkomponenten

Für Netzwerkkomponenten gelten alle anwendbaren Anforderungen aus Kapitel 6.5.1. Folgende zusätzliche Anforderungen sind zu erfüllen:

6.5.5.1 Schnittstellensicherheit

- Es müssen allgemeine oder spezifische Daimler-Vorgaben für die Konfiguration von Schnittstellen vorhanden und implementiert sein. Sind diese nicht vorhanden, müssen mindestens die Anforderungen der Best Practice IT-Security Guidelines auf anwendbare Netzwerkkomponenten implementiert werden:
    - Die Netzwerkkomponenten müssen nicht benötigte und unsichere Protokolle wie FTP, Telnet oder SNMP v1/v2 deaktivieren.
    - Falls Netzwerkgeräte andere Protokolle, als die zur Datenübertragung benötigten erlauben, müssen diese ebenfalls deaktiviert werden.
    - Wird die Übertragung mittels Funkverbindung nicht genutzt, muss diese Funktionalität deaktiviert werden.
    - Alle physischen Geräteschnittstellen der Netzwerkkomponenten die aktiv sind, d.h. einen Zugriff ermöglichen, müssen in der Projekt- oder Systemdokumentation dargestellt werden.
    - Alle physischen Geräteschnittstellen, die nicht für den Betrieb bzw. den Wartungsfall benötigt werden (z.B. lokale serielle Konsole, proprietäre Punkt-zu-Punkt Verbindungen), sollten nach der Inbetriebnahme deaktiviert werden und nur bei Bedarf wieder aktiviert werden können.
    - Der Fernzugriff auf die Netzwerkkomponenten darf nur über sichere Protokolle (z.B. SSH, HTTPS) vorgenommen werden. Unsichere Klartextfernwartungsprotokolle (z.B. Telnet, http) müssen deaktiviert werden.

6.5.5.2 Zugriffsschutz für Netzwerkkomponenten

- Der Zugriffsschutz für Netzwerkkomponenten soll nach Daimlervorgaben umgesetzt werden.
- Der Einbau der Netzwerkkomponenten hat, wenn möglich, nicht frei zugänglich zu erfolgen. Nur die für den normalen Betrieb notwendigen Schnittstellen dürfen frei zugänglich sein.
- Für die Authentifizierung an den Netzwerkkomponenten müssen die vorhandenen Standardpasswörter geändert und stattdessen sichere, der Daimler Passwort Policy entsprechenden, Passwörter verwendet werden. Zusätzlich muss die Anzahl an nicht erfolgreichen Anmeldeversuchen eingeschränkt werden. Bei einer Überschreitung der festgelegten Anzahl an Anmeldeversuchen kann je nach Kritikalität der Zugriff für den Benutzer gesperrt werden oder eine Benachrichtigung an den zuständigen Sicherheitsverantwortlichen gesendet werden.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.4.3	

6.5.6 Non-Windows Systeme

Für Non-Windows Systeme gelten alle anwendbaren Anforderungen aus Kapitel 6.5.1. Folgende zusätzliche Anforderungen sind zu erfüllen:

- Die einzusetzende Firmware-Version und Konfiguration der Non-Windows Systeme hat nach Daimlervorgaben zu erfolgen. Wird während dem Anlagenbau eine neue Firmware einer Komponente durch den Hersteller veröffentlicht, muss der Lieferant den Einsatz dieser Firmware mit Daimler abstimmen.
- Nicht benötigte Funktionen (Services, Dienste) sind zu deaktivieren und zu dokumentieren.
- Der Einbau der Komponenten hat, wenn möglich, nicht frei zugänglich zu erfolgen. Nur die für den normalen Betrieb notwendigen Schnittstellen dürfen frei zugänglich sein.
- Wo technisch unterstützt soll der Integrator auch auf Industriekomponenten vorhandene spezifische Härtungsmaßnahmen/Sicherheitsfunktionen aktivieren, z.B. Schutzstufenpasswort.

6.5.7 Windows Systeme

Für Windows Systeme gelten alle anwendbaren Anforderungen aus Kapitel 6.5.1. Darüber hinaus sind alle Systeme grundsätzlich gehärtet zu betreiben, siehe Kapitel 6.5.3 und 6.5.4. Die dafür notwendigen Voraussetzungen müssen durch den Lieferanten geschaffen werden. Für Windows Systeme sind folgende zusätzliche Anforderungen zu erfüllen.

6.5.7.1 Industrie-PCs (Blue PC)

Komponenten

Es dürfen ausschließlich durch Daimler freigegebene Komponenten, siehe Kapitel 6.1.2, eingesetzt werden.

Betriebssystem

Der Standard-Produktions-PC ist der „Blue PC“ mit der aktuellen von Daimler freigegebenen Betriebssystemversion. Die aktuell freigegebene Betriebssystemversion ist vor Auftragsvergabe beim Standortverantwortlichen zu erfragen.

6.5.7.2 Nachweis der Softwarelauffähigkeit auf Blue PCs

Die Lauffähigkeit von Anwendersoftware muss auf der Hardwareplattform, sowie der Software (z.B. Betriebssystem) nachgewiesen werden. Folgende Anforderungen sind zu erfüllen:

- Die Anwendersoftware muss mit der aktuellen von Daimler freigegebenen Betriebssystemversion kompatibel sein. Die aktuell freigegebene Betriebssystemversion ist beim Projektverantwortlichen zu erfragen.
- Die Anwendersoftware muss eine Kompatibilität mit folgenden Komponenten nachweisen:
    - Datenbanken
    - Applikationen inkl. Middleware (z. B. Java)
    - Hardware und Peripherie
- Kann eine Unterstützung bzw. Kompatibilität der Anwendersoftware nicht garantiert werden, sind geeignete Maßnahmen aufzuzeigen, die einen sicheren und robusten Betrieb über die gesamte geplante Laufzeit der Anlage ermöglichen.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.6.2	

6.5.7.3 Korrekte Funktionsweise der Software auf der Hardwareplattform

Die Auswahl der Hardwareplattform hat basierend auf den von Daimler vorgegebenen Komponenten zu erfolgen. Folgende Anforderungen sind zu erfüllen:

- Der Lieferant muss sicherstellen, dass die von Daimler vorgeschriebene Software (Betriebssysteme, Applikationen) auf der ausgewählten Plattform lauffähig ist.
- Sollten jegliche Abweichungen bzw. Minderung der Leistung der Software festgestellt werden, muss dies an Daimler gemeldet werden und eine mögliche Hardwarelösung ermittelt werden.

6.6 Schutz von Daten und Verschlüsselung

Vertraulich oder geheim eingestufte Daten müssen bei der Speicherung und Übertragung verschlüsselt werden. Hierbei sind folgende Anforderungen zu erfüllen:

- Einsatz aktueller Protokolle und Verschlüsselungsverfahren
- Nutzung von etablierten und öffentlichen Verfahren (z. B. AES oder Public-Key-/Privat-Key-Verfahren)
- Alle Verfahren müssen dokumentiert werden.
- Die verwendeten Passwörter und Zertifikate (Schlüssel) sind auf einem sicheren Weg an Daimler zu übergeben.

Wenn Daten darüber hinaus einen außergewöhnlichen Schutzbedarf aufweisen (z.B. aufgrund von Datenschutz- oder Integritätsschutzanforderungen), können weitere Maßnahmen zum Schutz dieser Daten vorgeschrieben werden.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.7	

6.7 Backup und Wiederherstellung

Bei der Übergabe der Anlage an Daimler muss ein Backup aller Systeme, dass die Anlage im übergebenen und abgenommenen Zustand widerspiegelt und es ermöglicht diesen Zustand jederzeit wiederherzustellen, vorhanden sein. Dies gilt auch für die Wiederherstellung auf neuer Hardware. Dieses Backup muss neben allen Daten auch eine detaillierte, schrittweise Anleitung für das Einspielen des Backups enthalten.

Referenz	MBN 9666-9 Ausgabe 2019-09: 5.3.3	

Anhang A **(normativ)**
Betriebshandbuch Informationssicherheit

Im Betriebshandbuch für Informationssicherheit müssen alle notwendigen Informationen für einen sicheren und robusten Betreib der Anlage zusammengefasst werden. Es kann als separates Dokument oder als Teil eines umfassenden Betriebshandbuches konzipiert werden. Folgende Informationen müssen detailliert enthalten sein:

Systemdaten und Kontaktpersonen

- Name, IP's, DNS

Software- und Hardwarearchitektur

- Details zu Hard-und Software
  - Versionsstände
  - Supportende

Kernfunktionen der Anlage und ihrer Komponenten

- Beschreibung der Kernfunktionen und der notwendigen Kernkomponenten inkl. grafischer Darstellung.

Schnittstellen

- Datenaustausch

Netzwerkkommunikation

- Verbindungsdaten: IP-Adressen, Ports, Firewallregeln

Systemanforderungen und Rahmenbedingungen

- Anbindung an weitere Systeme

Bekannte Probleme und Schwachstellen

Notfallprozess

- Meldewege und Eskalation
- Krisenstab
- Verteilung der Rollen während eines Notfalls
- Weitere Dokumentation/Informationen
- Anlaufplan nach SLAs

Ausfallszenarien

- Voraussetzungen für diese Szenarien
- Sofortmaßnamen
- Einrichtung des Notbetriebs
- Änderungen an Arbeitsabläufen im Notbetrieb
- Rückführung in den Regelbetrieb
- Nacharbeiten

Dienstleisterkontakte

Glossar

Anhang B **(informativ) Abkürzungsverzeichnis**

Abkürzung	Bedeutung
BLE	Bluetooth Low Energy
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protokoll
IT	Informationstechnik
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media-Access-Control
MBN	Mercedes Benz Norm
PLC	Programmable Logic Controller
SNMP	Simple Network Management Protocol
SPS	Speicherprogrammierbare Steuerung
SSH	Secure Shell
SSID	Service Set Identifier
SSO	Single Sign-on
TCP	Transmission Control Protocol
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Anhang C **(informativ)**
Literaturhinweise

C.1 **Internationale Normen**

ISO/IEC 27000-Familie

Dieses Dokument bietet einen Überblick über die ISO/IEC 27000-Familie von Informationssicherheits-Managementsystemen, die aus miteinander in Beziehung stehenden Normen und Richtlinien besteht, die bereits veröffentlicht wurden oder in Entwicklung sind.

ISO 27001

Dieses Dokument enthält die ISO-Standards der Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems im Kontext der Organisation.

ISO 27002

Dieses Dokument beschreibt die Durchführung und Überprüfung der Informationssicherheitsmaßnahmen.

C.2 **Weitere Literatur**

BDEW Whitepaper

Das BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V.) Whitepaper definiert grundsätzliche Sicherheitsanforderungen für Steuerungs- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung und gibt Ausführungshinweise zu deren Umsetzung.

National Information Security Technology Standard Specification

Diese Webseite enthält eine Sammlung nationaler Informationssicherheitsstandards, die vom National Information Security Standards Technical Committee formuliert wurden. Diese Standards umfassen Informationssicherheitsmanagement, Informationssicherheitsbewertung, Authentifizierung und Autorisierung, usw.

SANS Security Policy Resource

Diese Ressourcen werden vom SANS Institute für die schnelle Entwicklung und Implementierung von Informationssicherheitsrichtlinien veröffentlicht.