VDMA

VDMA-Lastenheft

Supply Chain Security

Hinweis

Das Lastenheft wurde im VDMA-Arbeitskreis „Industrial Security“ gemeinsam von Betreibern, Maschinenbauern, Komponentenherstellern und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet.
Die Anforderungen in diesem Dokument sind weder vollumfassend noch verpflichtend.
Betreibern soll dieses Dokument die Möglichkeit geben, die richtigen Anforderungen hinsichtlich der Cybersecurity bei der Beschaffung von Maschinen und Anlagen zu formulieren.
Herstellern von Maschinen oder Anlagen soll dieses Dokument die Möglichkeit geben, mit einem standardisierten Lastenheft gleichförmige Anforderungen zu erhalten.

Beides dient zur Vereinfachung des Einkaufsprozesses, ohne die Anforderungen an Cybersecurity unnötig zu reduzieren.

Das vorliegende Dokument bildet im ersten Schritt die Mindestanforderungen der Security auf Basis der Norm IEC 62443 für Maschinen, Anlagen und Dienstleistungen ab. Auf dieser Grundlage können zukünftig weitere Gesetzesvorgaben einfach abgebildet oder ergänzt werden, zum Beispiel aus dem Cyber Resilience Act (CRA), der Funkanlagenrichtlinie (RED) oder nationalen Gesetzen auf Basis der NIS2-Richtlinie.

Dieses Lastenheft soll mittelfristig in ein zweisprachiges VDMA-Einheitsblatt überführt werden. Sollten Sie hierzu an der Mitarbeit Interesse haben, melden Sie sich gerne beim VDMA.

Steffen Zimmermann
Leiter Competence Center Industrial Security

Telefon: +49 69 6603-1978
E-Mail: Steffen.Zimmermann@vdma.org

© VDMA 2023

VDMA
Lyoner Str. 18
60528 Frankfurt am Main

www.vdma.org

Stand: 09.01.2023

Inhaltsverzeichnis

1. Einleitung

Dieses Lastenheft ist eine „Cyber Security Requirement Specification“ (CSRS) und beschreibt das Umfeld des Betreibers, in welchem eine konkrete, angefragte Anlage oder Maschine betrieben werden soll, sowie die daraus resultierenden Cybersecurity-Anforderungen des Betreibers. Anforderungen an die funktionale Sicherheit sind nicht Teil des Dokumentes.
Die CSRS-SI (System Integrator) wird zwischen Betreiber (Kunde) und Integrator (Auftragnehmer) ausgehandelt, d.h. der Integrator erstellt, basierend auf den Anforderungen des Betreibers in dem vorliegenden Lastenheft ein Angebot.
Der Integrator kann aber auch offenlegen, dass einzelne Anforderungen nicht erfüllt werden können. Ggf. kann es notwendig sein Rückfragen zu stellen, um die Situation im Gesamtkontext bewerten zu können.

Dieses Lastenheft ist als Template zu verstehen und umfasst mögliche Anforderungs-Formulierungen, die sich aus den Mindestempfehlungen des VDMA ableiten. Diese sind anhand eines risikobasierten Ansatzes zu überprüfen und ggf. anzupassen und zu ergänzen.

Das Lastenheft sollte immer im individuellen Kontext der bestimmungsgemäßen Verwendung auf Adaptierbarkeit geprüft werden. Bei der Abstimmung des Betreibers mit dem Integrator ist zudem darauf zu achten, dass rechtliche umzusetzende Vorgaben des Arbeitsschutzes, der Maschinensicherheit und des Datenschutzes eingehalten werden und zukünftige Vorgaben zur Cybersicherheit gemäß nationaler Vorschriften, Maschinenverordnung, Delegierten Rechtsakt zur Funkanlagenrichtlinie oder Cyber Resilience Act beachtet werden müssen.

2. Betreiber und dessen Betriebsumgebung

In diesem Kapitel beschreibt der Betreiber die Betriebsumgebung der Maschine oder Anlage und stellt kaufmännische Anforderungen an den Integrator.

2.1. Physikalischer Schutz des Betreibers

In diesem Kapitel beschreibt der Betreiber allgemein den Einsatzbereich in seiner Fertigung oder des Werksgeländes. Dieses dient dem Integrator bei der Auslegung des Security Konzepts (der Maschine, der Anlage, des Systems).

_____
_____
_____

2.2. Betreibernetzwerk

In diesem Kapitel beschreibt der Betreiber seine Netzwerk–Infrastruktur und gibt Auskunft zur Anbindung an überlagerten Systemen (SCADA, MES, Leitstände, Fernzugriffslösung, Verzeichnisdienst, Zeitserver ...).

_____
_____
_____
_____

☐ Verzeichnisdienst vorhanden. Variante: _____
☐ NTP-Server vorhanden.

2.3. Cybersecurity-Services

In diesem Kapitel beschreibt der Betreiber die Anbindung an Cybersecurity-Services seiner Infrastruktur (EPP-systeme, SIEM, IDS, IPS, ...).

_____
_____
_____

2.4. Kaufmännische Anforderungen

Hier sind kaufmännische Aspekte zu beschreiben, die in diesem Zusammenhang einzuhalten sind (Service Agreement, Trainings, Delivery Agreements, ...)

_____
_____
_____
_____

3. Security Anforderungen an den Integrator

Folgende organisatorischen Anforderungen gelten an die Entwicklungsumgebung des Integrators.
Die einzelnen Anforderungen sind mit einer eindeutigen Referenz-ID versehen. Auf diese Weise kann einfach darauf verwiesen werden. Im Kapitel 7 'Referenzliste' werden die einzelnen Anforderungen in Verbindung zu den Mindestanforderungen und den dort adressierten Standards hergestellt.

3.1. Tabellarische Forderungsübersicht

In Tabellarischer Auflistung werden Referenz-ID, Forderung/Lasten und Abstimmungsbereich dem Integrator übermittelt. Folgend exemplarisch die Überschrift jeder Tabelle.

ID	Forderung / Last	NA

3.1.1. ID

Die ID setzen sich wie folgt zusammen (Beispiel: CSRS-SI-GOV-1):

- Der erste Teil «CSRS-SI» stellt den Bezug zu diesem Dokument für die CSRS zwischen Betreiber und Integrator her. Die Abkürzung steht für «Cyber Security Requirement Specification – System Integrator».
- Zweiter Teil bezieht sich auf den Bereich der Anforderungen, z.B. GOV für „Governance". Diese orientieren sich an den Bereich aus den Mindestanforderungen und der Struktur in diesem Dokument.
- Dritter Teil ist eine fortlaufende Nummer.

3.1.2. Forderung / Last

Aufgeführte Forderungen und Lasten des Betreibers befinden sich in der Tabelle unter der entsprechenden Überschrift. Des Weiteren sind hier auch die Abnahmekriterien der Forderung oder Last aufgeführt.

3.1.3. Akzeptanz durch Integrator

Die dritte Spalte dient dem Austausch zwischen Integrator und Betreiber.
Dieses enthält die Auswahlkriterien | YES | NO | NA.

YES Der Integrator stimmt der Forderung zu.
NO Der Integrator lehnt die Forderung ab.
NA Der Integrator hat hier Handlungsbedarf, kann noch nicht zusagen oder muss sich mit dem Betreiber abstimmen.

3.2. Organisatorisches

3.2.1. Compliance (GOV)

In diesen Anforderungen werden allgemeine Anforderungen zu Security-Prozessen und dem Betrieb des Lieferanten abgefragt. Diese sollen dem Betreiber ein Vertrauen in die Entwicklungsprozesse und dem Betrieb des Lieferanten geben. Zum einem dient dazu die Lieferantenselbstbewertung dem allgemeinen Vergleich verschiedener Integratoren, zum anderem dienen diese spezifischen Anforderungen dazu, dedizierte Anforderungen zu platzieren.

ID	Forderung / Last	□
CSRS-SI-GOV-1	Security-Richtlinien und Prozesse müssen im Unternehmen (des Lieferanten) formuliert, dokumentiert und angewandt werden (z.B. schlanke Policy bis hin zum umfassenden ISMS). **Abnahmekriterium:** Nachweis erfolgt mittels Bestätigung durch den Lieferanten (z.B. mittels der Lieferantenselbstauskunft).	NA
CSRS-SI-GOV-2	Die Security-Richtlinien müssen anwendbar sein auf folgende Bereiche: • interne Office-IT (inkl. Service-Rechner) • Produktentwicklung / Engineering (z.B. Quality-Gates) • Produktion • externe Dienstleister (z.B. Leistungsbeschreibungen) **Abnahmekriterium:** Der Nachweis erfolgt mittels Bestätigung durch den Lieferanten und deckt die aufgeführten Bereiche ab (Nachweis erfolgt z.B. mittels Lieferantenselbstauskunft, Vertragsbedingungen mit Lieferanten, Prozessnachweise, ...).	NA

3.2.2. Asset-Management (AMS)

Die Anforderungen zum Asset-Management dienen dem späteren Betrieb der OT-Komponenten. Dazu werden die erhobenen Komponenten in eine Inventarisierung des Betreibers übergeben und dienen dem Risikomanagement, sowie der Mitigation von Risiken des Betreibers.

ID	Forderung / Last	□
CSRS-SI-AMS-1	Der Integrator verpflichtet sich, die nötige technische Dokumentation aller in einer Maschine verbauten IT-Komponenten durchzuführen. Dabei sind in erster Linie die Assets aufzulisten, die über das Ethernet direkt oder indirekt erreicht werden können. Minimal müssen folgende Informationen per OT-Komponente erfasst werden: • IP-Adresse • MAC-Adresse • Betriebssystem / Firmware-Version • Hersteller der Komponente • Herstellerbezeichnung • Applikation + Softwareversion • Security-Fähigkeiten **Abnahmekriterium:** Der Nachweis erfolgt minimal mittels beigestellter Dokumentation in tabellarischer Form und ggf. mit entsprechenden weiterführenden Referenzen auf beigelegter Herstellerdokumentation durch den Lieferanten.	NA
CSRS-SI-AMS-2	Der Integrator verpflichtet sich, die Komponenten der Maschine in maschinenlesbar Form beizustellen. Diese muss als Liste aller Komponenten pro Maschine erfolgen. **Abnahmekriterium:** Der Nachweis erfolgt mittels beigestellter Liste in tabellarischer Form durch den Lieferanten. (z.B. im Dateiformat *.csv; *.xlsx) Die erfassten Kriterien müssen dabei in einzelnen Spalten separiert sein.	NA

3.2.3. Risikomanagement (SRM)

Ziel des Risikomanagements ist es, mitigierende Maßnahmen einzufordern oder diese durch den Integrator identifizieren zu lassen, damit dieser mitigierende Maßnahmen einleiten kann.

ID	Forderung / Last	□
CSRS-SI-SRM-1	Der Integrator verpflichtet sich, die ihm übergebenen relevanten Teile des Sicherheitskonzeptes des Betreibers zu beachten. Dieses ist in der risikobasierten Planung von Securitymaßnahmen für die Maschinen und Anlagen zu berücksichtigen. **Abnahmekriterium:** Bestätigung der Übergabe der relevanten Teile des Sicherheitskonzept des Betreibers durch den Integrator (z.B. in den Einkaufskriterien, Mail an Betreiber, ...)	NA
CSRS-SI-SRM-2	Der Integrator stellt sicher, dass Informationssicherheitsrisiken, die bis zur Inbetriebnahme der Maschine beim Betreiber erkannt werden, durch risikomitigierende Maßnahmen behoben werden. Die Festlegung der erforderlichen Maßnahmen (z.B. Systemhärtung zum Schutz der Komponenten) erfolgt bereits ab der Planungsphase neuer Maschinen und gliedert sich, durch Abstimmung, in das Sicherheitskonzept des Betreibers ein. **Abnahmekriterium:** Nachweis der Wirksamkeit (z.B. durch einen Penetration Test / Audit) der risikomitigierenden Maßnahmen (z.B. Segmentierung, Firewallsettings, Konfiguration) und Dokumentation in der Betriebsanleitung. Dies muss in der Betriebsanleitung (das Sicherheitskonzept der Maschine) dokumentiert werden.	NA

3.3. Sicherheitskonzept (SIK)

Das Sicherheitskonzept dient zur Abstimmung über die Implementierung von Security-Maßnahmen zwischen Betreiber und Integrator. Die Abstimmung dient der Erhöhung und Ausprägung der Maßnahmen.

ID	Forderung / Last	□
CSRS-SI-SIK-1	Der Integrator verpflichtet sich, basierend auf dem mit dem Betreiber abgestimmten Verwendungszweck (Intended Use) und dem übergeordneten Sicherheitskonzept des Betreibers, ein angepasstes Sicherheitskonzept für die Maschine zu erstellen. Dieses enthält die implementierten technischen Maßnahmen, sowie die durch den Betreiber umzusetzenden notwendigen technischen und organisatorischen Maßnahmen. Das Sicherheitskonzept muss regelmäßig bis zur Übergabe an den Betreiber basierend auf dem Risikomanagement angepasst werden. **Abnahmekriterium:** Ein dokumentiertes Sicherheitskonzept für die Maschine mit Beschreibung der Maßnahmen und Nachweisen deren Wirksamkeit, sowie seitens des Betreibers umzusetzenden weitere Maßnahmen.	NA
CSRS-SI-SIK-2	Der Integrator weist die Umsetzung des Sicherheitskonzeptes durch eine geeignete Dokumentation nach. Diese umfasst mindestens die implementierten Maßnahmen, Schnittstellen zu übergeordneten Themen aus dem Sicherheitskonzept des Betreibers und der verbleibenden Risiken. **Abnahmekriterium:** Übergabe eines dokumentierten Sicherheitskonzepts an den Betreiber je Maschine.	NA
CSRS-SI-SIK-3	Der Integrator unterstützt die Durchführung zyklischer Überprüfungen der Informationssicherheit der Maschine durch Bereitstellung von Informationen, Ressourcen und notwendigen Zeitfenstern (z. B. monatliche Schwachstellenaudits (Vulnerability-Scans), eine jährliche Risikobewertung, Freigabeprüfungen zu Meilensteinen wie SOP oder bei Netzkopplung usw.). **Abnahmekriterium** Unterstützungserklärung des Betreibers im Betrieb durch Wartungs- oder Instandhaltungsverträge.	NA

3.3.1. Engineering Prozess (SCS)

Die Anforderungen zum Engineering Prozess dienen dazu, eine sichere Umgebung im Rahmen der Entwicklung zu gewährleisten. Es soll damit ein gewisser Qualitäts- und Sicherheitsstandard erreicht werden, um Fehler und Schwachstellen frühzeitig zu vermeiden.

ID	Forderung / Last	□
CSRS-SI-SCS-1	Der Integrator verpflichtet sich, die Risikobetrachtung des Betreibers bei der Umsetzung im Securitykonzept der Maschine oder Anlage zu beachten (High-Level-Risikoanalyse). **Abnahmekriterium:** Nachweis, dass Bestandteile der Betreiberrisikoanalyse übernommen und die aufgeführten Risiken behandelt wurden.	NA
CSRS-SI-SCS-2	Der Integrator verpflichtet sich, für den Engineeringprozess eine sichere Umgebung für die System-Integration zu betreiben. Dazu gehören Regelungen für den Zutritt zu Entwicklungsbereichen, für die Speicherung und die Verarbeitung von Entwicklungsdaten. Des Weiteren verpflichtet er sich, Vorgaben zur sicheren Entwicklung (sog. Secure Development Lifecycle) implementiert zu haben, um (typische) Schwachstellen bei der Entwicklung zu vermeiden und keine undokumentierten Funktionen zu integrieren. **Abnahmekriterium:** Der Integrator bestätigt, ein Sicherheitsmanagement für die Umgebung der System-Integration zu betreiben. Zudem bestätigt er die Erfüllung eines Secure Development Lifecycles mit Verweis auf entsprechende Vorgaben und Vorgehensweisen, ggf. durch Zertifikat/Drittstellenprüfung.	NA
CSRS-SI-SCS-3	Der Integrator verpflichtet sich, den bestimmungsgemäßen Gebrauch (Intended Use) zu dokumentieren, um den Security-Status der Maschine/Anlage aufrechtzuerhalten. **Abnahmekriterium:** Der Integrator liefert, im Rahmen der Dokumentation, Hinweise zum Einsatz der Maschine. Dies enthält Hinweise • zur Integration der Maschine in die Infrastruktur des Betreibers, • zu Aufgaben und Pflichten des Betreibers und • zur Aufrechterhaltung der Security (z.B. Updates).	NA
CSRS-SI-SCS-4	Der Integrator verpflichtet sich, die Anforderungen des Betreibers in den Abnahmeprozess aufzunehmen und unterstützt den Abnahmeprozess. **Abnahmekriterium:**	NA

	Der Integrator bestätigt die Einhaltung der Anforderungen und verweist auf andere Nachweise (z.B. andere Anforderungen, Prüfprotokolle, usw.).	
CSRS-SI-SCS-5	Der Integrator verpflichtet sich, Serviceverträge zu Security Anforderungen (wie z.B. Schwachstellen-Management, Fernzugriff, Monitoring, ...) anzubieten oder alternative Dienstleister auszuweisen. Externe - Dienstleister müssen zusichern, dass ihre Rechner in diesem Zusammenhang verwaltet sind (aktuelles Betriebssystem, Virenscanner mit aktuellen Signaturen). **Abnahmekriterium:** Ausweisen von Serviceverträgen für z.B. Schwachstellen- / Patch-Management, Fernzugriff, Monitoring, Virenscan, LifeCycle-Management, ...	NA
CSRS-SI-SCS-6	Der Integrator verpflichtet sich, die aktuelle Konfiguration der Maschine und Systeme an den Betreiber zu übergeben und die Einrichtung zu dokumentieren, um die Konfiguration nach einem Incident wiederherstellen zu können. **Abnahmekriterium:** Es liegen zu allen relevanten Komponenten, die notwendigen Konfigurationen, Steuerungsprogramme, usw. in digitaler Form vor.	NA

3.3.2. Schwachstellen-Management (VUL)

ID	Forderung / Last	□
CSRS-SI-VUL-1	Der Integrator verpflichtet sich, selbständig die bekannten Kanäle (z.B. Hersteller Newsfeed, CERT@VDE, CISA, BSI, Mailverteiler, ...) für die Veröffentlichung von Schwachstellen und Sicherheitslücken in der von Ihm eingesetzten Software- und IT-Komponenten zu überwachen (Security Monitoring) und hinsichtlich der Auswirkungen zu bewerten. **Abnahmekriterium:** Nachweis erfolgt mittels Bestätigung.	NA
CSRS-SI-VUL-2	Der Integrator verpflichtet sich, mindestens alle relevanten Informationen, bekannte Schwachstellen und Herstellerhinweise zu jeglicher in den Maschinen oder Anlagen eingesetzten Hard- und Software unverzüglich an den Betreiber weiterzugeben. **Abnahmekriterium:** Der Nachweis erfolgt mittels Bestätigung zur Lieferung der relevanten Informationen und der Information über die Verteilung der Informationen.	NA
CSRS-SI-VUL-3	Der Integrator verpflichtet sich, die Meldungen zu Schwachstellen in einem maschinenlesbaren und automatisiert auswertbaren Format (z.B. CSAF) bereitzustellen. **Abnahmekriterium:** Der Nachweis erfolgt durch Übergabe von Informationen zum Bezug und der Dokumentation des Formats.	NA
CSRS-SI-VUL-4	Der Integrator verpflichtet sich (nach der Inbetriebnahme) kritische Schwachstellen der erstellten Maschine/Anlage (z.B. CVSS-Score > 9) zu jeglicher eingesetzten Hard- und Software unverzüglich an den Betreiber weiterzugeben. **Abnahmekriterium:** Der Integrator bestätigt, dass er die ihm zur Verfügung stehenden Informationen und Handlungsempfehlungen rechtzeitig an den Betreiber weitergibt.	NA
CSRS-SI-VUL-5	Der Integrator verpflichtet sich, einen Kontakt und Prozess zur Entgegennahme und Bearbeitung von Schwachstellenmeldungen bereitzustellen. **Abnahmekriterium:** Der Nachweis erfolgt durch Bestätigung durch den Integrator und Benennen der Kontaktdaten.	NA

CSRS-SI-VUL-6	Der Integrator verpflichtet sich, eine Festlegung des freigegebenen Softwarestandes ("Baseline") zu treffen, welche bei der Konstruktion der Maschine oder Anlage berücksichtigt wurde. **Abnahmekriterium:** Der Nachweis einer Baseline in Form von Softwareversionen in Bezug auf die verwendeten Komponenten wird erbracht.	NA

3.3.3. Service-Management (SSM)

Die Forderungen des Service-Managements dienen dazu, die Services abzufragen, die von Integratoren angeboten werden, um das Security-Level der Maschine, Anlage oder des Systems aufrechtzuhalten.

ID	Forderung / Last	□
CSRS-SI-SSM-1	Der Integrator weist nach, welche Security Services zur Unterstützung angeboten werden können. Diese Dienstleistungen können ggf. auch durch Partnerunternehmen angeboten werden (z.B. im Rahmen einer internen oder externen Serviceleistung). Security-Services sind z.B. Patchmanagement, Fernzugriff zu Wartungszwecken oder Netzwerk-Monitoring. Security-Services können im Rahmen von separaten Serviceverträgen angeboten werden. **Abnahmekriterium:** Angebot von verschiedenen Services, incl. eines vereinbarten Service Level Agreement (SLA) zum Vertrag.	NA

3.3.4. Life-Cycle-Management (LCS)

Im Life-Cycle-Management werden die Rahmenbedingungen festgehalten, die sich auf den geforderten Service des Anlagen- und Maschinenbauers beziehen.

ID	Forderung / Last	□
CSRS-SI-LCS-1	Der Integrator verpflichtet sich, mit dem Betreiber vertraglich zu vereinbaren, welche Service-Bedingungen an seine Maschinen und Anlagen geknüpft sind und wann dieser Service endet. **Abnahmekriterium:** Vertragliche Festlegung im Kaufvertrag.	NA

3.3.5. Training (TRA)

Security-Trainings müssen regelmäßig stattfinden und sicherstellen, dass Mitarbeiter und Manager über das notwendige Wissen verfügen, um im Rahmen ihrer täglichen Arbeit einen sicheren Lebenszyklus der Anlage und der Systeme zu gewährleisten. Dies ist insbesondere auch dann notwendig, wenn andere Personengruppen Tätigkeiten übernehmen (z.B. im Rahmen der Inbetriebnahme muss der Anlagen- und Maschinenbauer die Mitarbeiter des Betreibers angemessen schulen).

ID	Forderung / Last	□
CSRS-SI-TRA-1	Der Integrator weist nach, dass alle seine Mitarbeiter (Manager, interne Mitarbeiter und externe DL), die mit der Produkterstellung (während der Konzeption, Entwicklung, Integration und Inbetriebnahme) beauftragt sind, regelmäßig Security-Trainings absolvieren. Diese Security-Trainings müssen einerseits allgemeines Wissen sowie auch spezielles tätigkeitsbezogenes Wissen vermitteln. **Abnahmekriterium:** Jährliche Verpflichtungserklärung durch den Mitarbeiter.	NA
CSRS-SI-TRA-2	Im Rahmen der Inbetriebnahme unterweist der Integrator die Mitarbeiter des Betreibers im Umgang mit allen notwendigen Security-Themen hinsichtlich der Anlage bzw. Maschine. **Abnahmekriterium:** Nachweis der Unterweisung des Servicepersonals.	NA
CSRS-SI-TRA-3	Der Betreiber unterweist die Mitarbeiter des Integrators hinsichtlich der bei ihm geltenden Security-Anforderungen. Der Integrator verpflichtet sich, bei einem Wechsel von Mitarbeitern diese erneut zu unterweisen. **Abnahmekriterium:** Nachweis der Unterweisung des Servicepersonals.	NA

3.3.6. Information Security Incident Management (IIM)

Das Incident-Management umfasst den gesamten organisatorischen und technischen Prozess als Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen. Das Spektrum möglicher Vorfälle reicht dabei von technischen Problemen und Schwachstellen bis hin zu konkreten Cyber-Angriffen auf Maschinen- oder Netzinfrastruktur.

ID	Forderung / Last	□
CSRS-SI-IIM-1	Der Integrator verpflichtet sich, alle ihm bekannten Vorfälle (Incidents) in seinen betroffenen Produkten unverzüglich an den Betreiber zu melden. Notwendige Sofortmaßnahmen zur Eindämmung oder Schadensbegrenzung des Vorfalls müssen dem Betreiber zeitnah aufgezeigt werden. Der Integrator verpflichtet sich, alle notwendigen Maßnahmen zur Eindämmung und Behandlung des Vorfalles zu unterstützen und angemessene Maßnahmen zu erarbeiten oder zu empfehlen (z. B. Patchen, Netzwerktrennung). **Abnahmekriterium:** Vertragliche Verpflichtung des Integrators mit dem Betreiber.	NA

3.4. Technische Anforderungen

3.4.1. Infrastruktur (INF)

Die technischen Anforderungen an die Betreiberinfrastruktur zur Aufrechterhaltung des Sicherheitsniveaus der Maschine, Anlage oder des Systems.

ID	Forderung / Last	□
CSRS-SI-INF-1	Der Integrator verpflichtet sich, seine Mitarbeiter zu unterweisen, dass sie sich in den Räumlichkeiten des Betreibers nur in den zugewiesenen Bereichen aufhalten. **Abnahmekriterium:** Der Nachweis von der Unterweisung im Rahmen des Auftrags.	NA
CSRS-SI-INF-2	Der Integrator verpflichtet sich, einen Abgleich mit der Betreiber-Infrastruktur durchzuführen, um die benötigten Verbindungen zu ermitteln (z.B. Anbindung vom MES Server, Patch Server, Backup Server, ...). **Abnahmekriterium:** Der Nachweis von der Anbindung an die erforderlichen Dienste des Betreibers.	NA
CSRS-SI-INF-3	Der Integrator verpflichtet sich, das Maschinen-/Anlagenetz vom Netz des Betreibers zu trennen und nur notwendige Zugriffe zu ermöglichen. **Abnahmekriterium:** Der Nachweis des ordnungsgemäßen Netzwerkzugriffs auf die notwendigen Dienste des Betreibers (incl. Dokumentation / Protokollierung der Abnahmeergebnisses (SAT)).	NA

3.4.2. Authentifizierung (UAC)

Die technischen Anforderungen, die ein Integrator und der Betreiber erfüllen müssen, um das Sicherheitsniveau der Maschine, Anlage oder des Systems zu erhalten.

ID	Forderung / Last	□
CSRS-SI-UAC-1	Der Integrator verpflichtet sich, geeignete Rollen und Benutzergruppen zu definieren und technisch zwingend umzusetzen, die abhängig von den Umgebungsrisiken sind (z.B. spezielle Authentifizierung und Autorisierung für Konfigurationsänderungen, Softwareänderungen, etc.). **Abnahmekriterium:** Der Nachweis von der Umsetzung des Rollen- und Rechtekonzepts durch die Abnahme-Testergebnisse.	NA
CSRS-SI-UAC-2	Der Integrator verpflichtet sich, bei der Inbetriebnahme individuelle Passwörter gemäß dem Rollen- und Rechte-Konzept zu verwenden. Alle temporären und unnötigen Benutzerkonten müssen bei der Inbetriebnahme gelöscht werden. **Abnahmekriterium:** Der Nachweis von der Umsetzung des Rollen- und Rechtekonzepts durch die Abnahme-Testergebnisse.	NA
CSRS-SI-UAC-3	Der Integrator verpflichtet sich, die Maschinen nur über die Benutzer- oder Gruppenkonten zu bedienen und das Administratorkonto während des normalen Betriebs nicht zu verwenden. **Abnahmekriterium:** Der Integrator verpflichtet sich, während der normalen Betriebsbedingungen gemäß des Rollen- und Rechtekonzepts, Benutzerkonten mit eingeschränkten Funktionen anzulegen.	NA

3.4.3. Netzwerksicherheit (NCC)

Die technischen Anforderungen an die Netzwerksicherheit dienen dazu, das Sicherheitsniveau der Maschine, des Geräts oder des Systems aufrecht zu halten.

ID	Forderung / Last	□
CSRS-SI-NCC-1	Der Integrator verpflichtet sich, das Safety-Netz vom Produktionsnetz zu trennen. Dies kann durch Netzwerksegmentierung oder logische Trennung erfolgen. **Abnahmekriterium:** Der Nachweis erfolgt durch Netzwerkarchitekturdiagramm oder Design-Dokumente.	NA
CSRS-SI-NCC-2	Der Integrator verpflichtet sich, das Echtzeitnetz ("Feldebene") und die Produktionsnetze nicht direkt zu verbinden. Das Echtzeitnetz und die Produktionsnetze müssen durch eine physikalische Schnittstelle getrennt sein. **Abnahmekriterium:** Der Nachweis erfolgt durch das Netzwerkarchitekturdiagramm oder Design-Dokumente.	NA

3.4.4. Systemhärtung (CHA)

Für einen sicheren Betrieb ist es wichtig, bestimmte Maßnahmen zur Systemhärtung zu ergreifen, um einen reibungslosen Ablauf der Produktion zu gewährleisten und Angriffsfläche zu reduzieren.

ID	Forderung / Last	□
CSRS-SI-CHA-1	Der Integrator verpflichtet sich, aktuelle Security Patches vor der Inbetriebnahme auf den zugehörigen Komponenten zu installieren. Der Integrator sollte keine veralteten Betriebssysteme verwenden, die von den Betriebssystem-Herstellern nicht mehr unterstützt werden. **Abnahmekriterium:** Der Nachweis erfolgt über die Dokumentation der installierten Firm- und Software, sowie deren Versionen in den Assetlisten oder der SBOM.	NA
CSRS-SI-CHA-2	Der Integrator verpflichtet sich, grundlegende Systemhärtung und von Komponentenherstellern empfohlene Maßnahmen durchzuführen: wie z. B. die Deaktivierung ungenutzter USB-Anschlüsse und die Deaktivierung unnötiger Dienste. **Abnahmekriterium:** Der Nachweis erfolgt durch Bestätigung durch den Integrator.	NA
CSRS-SI-CHA-3	Der Integrator verpflichtet sich, die vom Komponentenhersteller empfohlenen Härtungsmaßnahmen umzusetzen. **Abnahmekriterium:** Der Nachweis erfolgt durch Bestätigung durch den Integrator.	NA

3.4.5. Systemwiederherstellung (AVA)

Die Anforderungen dienen der Wiederherstellung des Systems nach einer Katastrophe oder einem Zwischenfall. Dies ist wichtig, um einen reibungslosen Geschäftsbetrieb ohne Unterbrechungen zu gewährleisten.

ID	Forderung / Last	□
CSRS-SI-AVA-1	Der Integrator verpflichtet sich, die erforderlichen Schritte zur Durchführung von Backups zu dokumentieren und ggf. das Personal zu schulen und darüber hinaus nach der End-Abnahme ein Backup zu erstellen. **Abnahmekriterium:** Der Nachweis erfolgt über die Dokumentation und ggf. der Durchführung der Schulung. Zudem ist ein Nachweis zu erbringen das ein Backup erstellt wurde und zur Verfügung steht.	NA
CSRS-SI-AVA-2	Der Integrator verpflichtet sich, die Möglichkeit zur Wiederherstellung der Werkseinstellungen zu dokumentieren und zu testen. **Abnahmekriterium:** Der Nachweis erfolgt durch eine Wiederherstellung an einem zufällig ausgewählten Asset.	NA

3.4.6. Fernzugriff (NRA)

Unter Fernzugriff versteht man den räumlich getrennten Zugriff auf die Maschine, Anlage, IT- oder OT-Komponenten durch eine Person (Techniker intern oder extern), welche nicht physisch an der Maschine agiert. Um die Maschine und deren Einzelkomponenten beispielsweise im Fehlerfall einer Diagnose oder Wartung aus der Ferne unterziehen zu können, ist es daher notwendig, einen Fernzugriff einzurichten. Die folgenden Anforderungen dienen dazu, einen entsprechenden Service angeboten zu bekommen.

ID	Forderung / Last	□
CSRS-SI-NRA-1	Die vorhandene Fernwartungslösung ist zu nutzen. (Siehe dazu *Dokumentation xyz.doc*) Ein Fernzugriff wird bei dieser Maschine / Anlage benötigt. Die Verbindung muss von der Fertigungsstätte aufgebaut werden. Es ist dabei nur eine verschlüsselte Verbindung auf ein Rendezvous – Server erlaubt. **Abnahmekriterium:** Nachweis der eingerichteten und verwendeten Technologie (z.B. verschlüsselte Verbindung bis zu einer Security-Netzwerkkomponente). Bedienelement für User in der Fertigungsstätte zur Herstellung der Verbindung und Signalisierung, dass eine Verbindung aufgebaut wurde.	NA
CSRS-SI-NRA-2	Der Fernzugriff darf nur auf IT-/OT-Komponenten der Maschine/Anlage erfolgen, die für die Remote-Verbindung notwendig oder vorgesehen sind. Mittels Risikoanalyse ist nachzuweisen, auf welche Systeme oder Komponenten zugegriffen werden darf, ohne dass eine Gefahr für Mitarbeiter an der Maschine durch den Fernzugriff besteht. **Abnahmekriterium:** Nachweis der verfügbaren IT-/OT-Komponenten und Ausschluss von Safetykomponenten (außer explizit von Betreiber bestätigt).	NA
CSRS-SI-NRA-3	Fernzugriffe sind explizit technisch und/oder organisatorisch von Betreiberseite freigegeben. **Abnahmekriterium:** Einhaltung der Fernzugriffsberechtigung durch den Betreiber.	NA
CSRS-SI-NRA-4	Der Fernzugriff auf das ausgewählte System muss protokolliert werden. Dieses beschreibt den Nutzer, Datum, Dauer, IT-/OT-Komponente auf die zugegriffen wurde, die Tätigkeit des Fern-Zugreifenden und des Auftraggebers. **Abnahmekriterium:**	NA

	Protokollnachweis durch das Fernwartungssystem mit entsprechenden Einträgen zum Nutzer, Datum, Dauer, Komponente, Tätigkeit, Auftraggeber.	
CSRS-SI-NRA-5	Bei der Auswahl von Fernwartungslösungen müssen diese nach dem Stand der Technik und vorhandenen Good Practices berücksichtigt werden, z.B. nach BSI, VDMA «Sichere Fernwartung». **Abnahmekriterium:** Nachweis des Abgleichs mit Good Practices (z.B. des BSI).	NA

3.4.7. Sonstiges

Dieser Abschnitt dient zur Definition eigener Forderungen, die über das standardisierte Lastenheft hinausgehen.

ID	Forderung / Last	☐
SON	Der Integrator verpflichtet sich, eine Geheimhaltungserklärung zu unterzeichnen. **Abnahmekriterium:** Geheimhaltungsvereinbarung ist abgestimmt und unterzeichnet.	NA
		NA
		NA
		NA
		NA
		NA
		NA

4. Abnahmebedingungen

Dieser Abschnitt dient zur Formulierung zusätzlicher Anforderungen an die Protokollierung und Dokumentation. Darüber hinaus sollten die mit dem Integrator vereinbarten Gewährleistungszeiträume festgehalten werden.

5. Dokumentation

Die Dokumentation muss alle Informationen der OT-Komponenten, zum bestimmungsgemäßen Gebrauch der Maschine / Anlage und zur Aufrechterhaltung des Security Status enthalten.
In den Abnahmekriterien wird Bezug auf die Dokumentationsanforderungen genommen.

6. Glossar

AMS	Asset Management Shopfloor
AVA	Availability
CERT	Computer Emergency Response Team
CHA	Component Hardening
CSRS	Cyber Security Requirement Specification
CVSS	Common Vulnerability Scoring System
GOV	Governance
IIM	Information Security Incident Management
INF	Infrastruktur
LCS	Life Cycle Security
LSA	Lieferantenselbstauskunft
NCC	Network – Conduit Communication
NRA	Network – Remote Access
SCS	Supply Chain Security
SI	System Integrator
SIK	Sicherheitskonzept
SMM	Service Management
SON	Sonstiges
SRM	Shopfloor Risk Management
TRA	Training
VUL	Vulnerability Management

7. Referenzliste

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
CSRS-SI-GOV-1	MR-GOV-1-I	GOV	ORG 1.1 (ORG 1.2) (ORG 1.3) ORG 2.4	SP.01.04 BR SP.01.04 RE (1) SP.01.05 BR SP.01.06 BR SP.01.07 BR			
CSRS-SI-GOV-2	MR-GOV-2-I	GOV	ORG 1.1				
CSRS-SI-AMS-1	MR-AMS-1-I	AMS	CM1.1 CM1.2 CM1.3 NET1.2 COMP3.3	SP.06.01 SP.06.02 BR SP.06.03 BR SP.03.02 RE(2) SP.06.03 RE(1) SP.11.06 RE(3)	SR 7.6 SR 7.6 RE 1 SR 7.8		
CSRS-SI-AMS-2	MR-AMS-2-I						
CSRS-SI-SRM-1	MR-SRM-1-I	SRM	ORG2.1 COMP3.5	SP.11.02 RE(2)		SM-11	
CSRS-SI-SRM-2	MR-SRM-2-I	SRM	ORG 2.1	SP.02.01 BR SP.03.01 BR SP.03.01 RE(1) SP.03.01 RE(2)		SM-11	
CSRS-SI-SIK-1	MR-SIK-1-I MR-SIK-3-I		COMP 3.4	SP.11.06 RE(1)		SD-1	
CSRS-SI-SIK-2	MR-SIK-1-I MR-SIK-2-I		COMP 3.4	SP.11.06 RE(1)		SD-2	
CSRS-SI-SIK-3	MR-SIK-3-I		ORG 2.4			SD-2	
CSRS-SI-SCS-1	MR-SCS-2-I		ORG 1.6 ORG 2.3			SM-7 SD-1 SD-2	

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
						SM-6	
CSRS-SI-SCS-2	MR-SCS-2-I		ORG 1.6 ORG 2.3			SM-7 SD-1 SD-2 SM-6	
CSRS-SI-SCS-3	MR-SCS-3-I		ORG 1.6 ORG 2.3			SM-7 SD-1 SD-2 SM-6	
CSRS-SI-SCS-4	MR-SCS-5-I		ORG 1.6 ORG 2.3				
CSRS-SI-SCS-5	MR-SCS-6-I		ORG 1.6 ORG 2.3				
CSRS-SI-SCS-6	MR-SCS-7-I		COMP 1.1 (COMP 3.1) (COMP 3.2) (COMP 3.4) (COMP 3.5)	SP.11.01 BR SP.11.01 RE(1) SP.11.02 BR SP.11.02 RE(1) SP.11.02 RE(2) SP.11.03 BR SP.11.04 BR SP.11.05 BR SP.11.06 BR SP.11.06 RE(1) SP.11.06 RE(2)	SR 7.7	SR-1	
CSRS-SI-VUL-1	MR- VUL-1-I	VUL	EVENT 1.9				
CSRS-SI-VUL-2	MR- VUL-1-I	VUL	EVENT 1.9				
CSRS-SI-VUL-3	MR- VUL-1-I	VUL	EVENT 1.9				
CSRS-SI- VUL-4	MR- VUL-1-I	VUL	EVENT 1.9			SM-9	
CSRS-SI-VUL-5	MR-VUL-2-I	VUL	EVENT 1.9			DM-1	
CSRS-SI-VUL-6	MR-VUL-3-I					DM-6 SUM-5	
CSRS-SI-SSM-1	MR-SSM-1		COMP 3.1	SP.11.01 BR			

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
			COMP 3.2	SP.11.01 RE(1) SP.11.02 BR SP.11.02 RE(1) SP.11.03 BR SP.11.04 BR SP.11.05 BR SP.11.06 BR SP.11.06 RE(2)			
CSRS-SI-LCS-1	MR-LCS-1-I		ORG 1.4 ORG 1.5	SP.01.01 BR SP.01.01 RE(1)		SM-4	
CSRS-SI-LCS-2	-			SP.01.02 BR SP.01.02 RE(1)			
CSRS-SI-TRA-1	MR-TRA-1-I		ORG 1.4 ORG 1.5	SP.01.01 BR SP.01.01 RE(1)		SM-4	
CSRS-SI-TRA-2	MR-TRA-2-I			SP.01.02 BR SP.01.02 RE(1)			
CSRS-SI-TRA-3	MR-TRA-3-I MR-TRA-3-O						
CSRS-SI-IIM-1	MR-IIM-1-I		DATA 1.5 AVAIL 1.1 AVAIL 2.1 AVAIL 2.2 AVAIL 2.3 AVAIL 2.4 AVAIL 2.5	SP.12.01 BR SP.12.02 BR SP.12.03 BR SP.12.04 BR SP.12.05 BR SP.12.06 BR SP.12.07 BR SP.12.08 BR SP.12.09 BR	SR 3.7 SR 7.3 SR 7.3 RE(1) SR 7.3 RE(2) SR 7.4		
CSRS-SI-INF-1	MR-INF-1-O		ORG 3.1				
CSRS-SI-INF-2	MR-INF-2-O		NET 1.10	NET 1.10	SR 2.11 SR 2.11 RE(1) SR 2.11 RE(2)		
CSRS-SI-INF-3	MR-INF-3-O		NET 1.1	SP.03.02 BR	SR 1.13		

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
			NET 1.4 NET 1.5 NET 1.6	SP.03.02 RE(2) SP.03.03 RE(1) SP.03.07 BR	SR 1.13 RE(1) SR 5.1 SR 5.1 RE(1) SR 5.1 RE(2) SR 5.1 RE(3) SR 5.2 SR 5.2 RE(1) SR 5.2 RE(2) SR 5.2 RE(3) SR 5.4		
CSRS-SI-UAC-1 CSRS-SI-UAC-2	MR-UAC-1-I MR-UAC-2-I						CR 1.1 CR 1.3 CR 1.7
CSRS-SI-UAC-3	MR-UAC-3-I		USER 1.1 USER 1.2 USER 1.3 USER 1.4 USER 1.5 USER 1.8 USER 1.10 USER 1.11 USER 2.1	SP.09.01 BR SP.09.02 BR SP.09.02 RE(1) SP.09.02 RE(2) SP.09.02 RE(3) SP.09.02 RE(4) SP.09.03 BR SP.09.04 BR SP.09.04 RE(1) SP.09.05 BR SP.09.06 BR SP.09.06 RE(1) SP.09.07 BR SP.09.08 BR SP.09.08 RE(1)	SR 1.01 SR 1.01 RE(1) SR 1.02 SR 1.02 RE(1) SR 1.03 SR 1.03 RE(1) SR 1.04 SR 1.05 SR 1.06 SR 1.06 RE(1) SR 1.07 SR 1.07 RE(1 & 2) SR 2.01 SR 2.01 RE(1 & 2) SR 2.03 SR 2.03 RE(1) SR 2.04 SR 2.04 RE(1) SR 6.1		CCSC-3

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
CSRS-SI-NCC-1	MR-NCC-1-I		NET 1.3	SP.05.01 BR SP.05.02 BR SP.05.03 BR SP.05.04 BR SP.05.05 BR SP.05.05 RE(1) SP.05.06 BR			
CSRS-SI-NCC-2	MR-NCC-2-I		NET 1.4		SR 5.2 RE(2)		
CSRS-SI-CHA-1	MR-CHA-1-I		COMP 1.1		SR 7.7	SM-11	
CSRS-SI-CHA-2	MR-CHA-2-I MR-CHA-3-I		COMP 1.1		SR 7.7		CR 7.7 SG-2 SR-1
CSRS-SI-AVA-1	MR-AVA-1-I		DATA 1.5 AVAIL 1.1 AVAIL 2.1 AVAIL 2.2 AVAIL 2.3 AVAIL 2.4 AVAIL 2.5	SP.12.01 BR SP.12.02 BR SP.12.03 BR SP.12.04 BR SP.12.05 BR SP.12.06 BR SP.12.07 BR SP.12.08 BR SP.12.09 BR	SR 3.7 SR 7.3 SR 7.3 RE(1) SR 7.3 RE(2) SR 7.4		CR 7.3
CSRS-SI-AVA-2	MR-AVA-1-I		DATA 1.5 AVAIL 1.1 AVAIL 2.1 AVAIL 2.2 AVAIL 2.3 AVAIL 2.4 AVAIL 2.5	SP.12.01 BR SP.12.02 BR SP.12.03 BR SP.12.04 BR SP.12.05 BR SP.12.06 BR SP.12.07 BR SP.12.08 BR SP.12.09 BR	SR 3.7 SR 7.3 SR 7.3 RE(1) SR 7.3 RE(2) SR 7.4		CR 7.3
CSRS-SI-AVA-3	MR-AVA-2-I						CR 7.3
CSRS-SI-NRA-1	MR-NRA-1-I		NET 3.2				

ID	Mindestanforderungen	VDMA-LSA	IEC 62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
CSRS-SI-NRA-2	MR-NRA-2-I		NET 3.1 NET 3.2				
CSRS-SI-NRA-3	MR-NRA-3-O MR-NRA-3-I		NET 3.2				
CSRS-SI-NRA-4	MR-NRA-4-I		NET 3.2				
CSRS-SI-NRA-5	MR-NRA-5-I		NET 3.2				

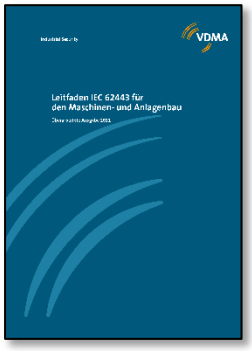
8. Arbeitshilfen des VDMA zu Industrial Security

VDMA Publikation "Sichere Fernwartung im Maschinen- und Anlagenbau"
Sprache: Deutsch
Preis: kostenfrei, nur für Mitglieder

Beispiele von Fernwartungsarchitekturen zeigen auf, wie der Maschinen- und Anlagenbau einen sicheren Service aus der Ferne gewährleisten kann.
https://www.vdma.org/viewer/-/v2article/render/45231112

VDMA Mindestempfehlungen zu Security in der Supply Chain
Sprache: Deutsch
Preis: kostenfrei

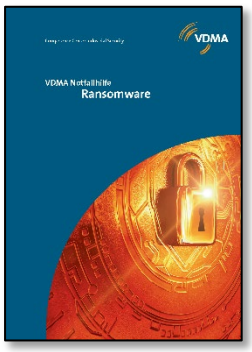
Mindestempfehlungen für Maschinen- und Anlagenbauer zu technischen, organisatorischen und prozessualen Anforderungen bei der Umsetzung von Security für Produkte und Prozesse.
Auf Anfrage bei Frau Biljana Gabric erhältlich:
biljana.gabric@vdma.org



VDMA Leitfaden IEC 62443 für den Maschinen- und Anlagenbau
Sprache: Deutsch, Englisch
Preis: 50 Euro für Nicht-Mitglieder, kostenfrei für Mitglieder

Beschreibung eines Weges durch die IEC 62443, als Integrator einer Maschine nach Security-Level 2, inkl. Beispielen nach 62443-3-3.

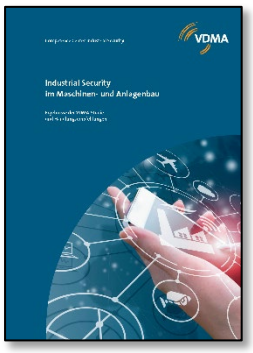
https://www.vdmashop.de/executive-briefings/informatik-und-technik/482/leitfaden-iec-62443-fuer-den-maschinen-und-anlagenbau?number=&c=23



VDMA Notfallhilfe Ransomware
Sprache: Deutsch, Englisch
Preis: kostenfrei

Unterstützung, Handlungsempfehlung bei einer Infektion mit Ransomware, Kontaktstellen bei Behörden und Dienstleistern. Liste von Indikatoren für eine Infektion und Maßnahmen.

https://www.vdma.org/viewer/-/v2article/render/1295961



VDMA Studie „Industrial Security“
Sprache: Deutsch, Englisch
Preis: kostenfrei

Status Quo der Industrial Security im Maschinen- und Anlagenbau, Ergebnisse der Umfrage, Maßnahmen und Handlungsempfehlungen.

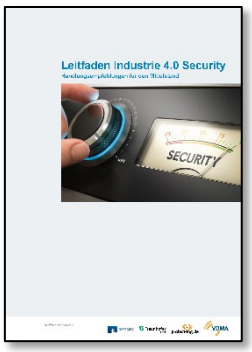
https://www.vdma.org/viewer/-/v2article/render/11923532

VDMA Positionspapier „Cybersecurity: Betreiber- und Arbeitgeberpflichten im Sinne gemeinsamer Anstrengungen“
Sprache: Deutsch
Preis: kostenfrei

Formulierung der VDMA Position zu Cybersecurity-Pflichten im täglichen Anlagenbetrieb.
Auf Anfrage bei Frau Biljana Gabric erhältlich:
biljana.gabric@vdma.org

VSMA Muster IT-Notfallplan
Sprache: Deutsch
Preis: kostenfrei auf Anfrage bei VSMA

Der Muster IT-Notfallplan dient der Unterstützung, nach einer massiven Beeinträchtigung des betrieblichen Ablaufs aufgrund von nicht funktionierender IT-Infrastruktur, schnellstmöglich wieder in einen geordneten IT-Betrieb zurückzufinden.
https://unternehmen-cybersicherheit.de



VDMA Leitfaden „Industrie 4.0 Security“
Sprache: Deutsch, Englisch
Preis: kostenfrei

83 Handlungsempfehlungen in 17 Bereichen für die sichere und dauerhaft zuverlässige Vernetzung von Maschinen und Anlagen.

https://industrialsecurity.vdma.org/viewer/-/v2article/render/26240836

9. Redaktion

An der Erstellung des Lastenhefts waren folgende Personen aus dem Arbeitskreis „Industrial Security“ des VDMA sowie weitere externe Fachexperten beteiligt. Das Redaktionsteam bedankt sich ausdrücklich für die gute Zusammenarbeit von BSI, VDMA und ZVEI.

Sascha Bihler	Endress+Hauser Process Solutions AG
Jens Cordt	BSI – Bundesamt für Sicherheit in der Informationstechnik
Bernd Gehring	J.M. Voith SE & Co. KG
Arne Grandt	GEA Group AG
Martin Holtmannspoetter	Robert Bosch GmbH
Marcel Hug	ZVEI e. V.
Jan Ole Jensen	Volkswagen AG
Jens Kluge	BSI – Bundesamt für Sicherheit in der Informationstechnik
Maximilian Korff	Siemens AG
Thomas Lantermann	Mitsubishi Electric Europe B.V.
Jochen Müller	Bizerba SE & Co. KG
Sebastian Nikelski	Volkswagen AG
Matthias Schmidt	ifm electronic GmbH
Wolfgang Stadler	Sick AG
Rainer Traub	Balluff GmbH
Gunther Vaßen	ifm electronic GmbH
Alexander Wahl	Festo SE & Co. KG
Bernd-Ulrich Wittwer	Weidmüller Interface GmbH & Co. KG
Klaus Ziegler	Bosch Rexroth AG
Steffen Zimmermann	VDMA e. V.

10. Impressum

VDMA
Lyoner Str. 18
60528 Frankfurt am Main
E-Mail: informatik@vdma.org
Internet: www.vdma.org

Erscheinungsjahr
2023

Copyright
VDMA

Bildnachweis
VDMA

Grafiken
VDMA

Hinweis
Die Verbreitung, Vervielfältigung und öffentliche Wiedergabe dieser Publikation bedarf der Zustimmung des VDMA.

VDMA
Abteilung Informatik
Lyoner Str. 18
60528 Frankfurt am Main
Telefon +49 69 6603-0
E-Mail informatik@vdma.org
Internet www.vdma.org

www.vdma.org/cybersecurity