

Vorgabedokument der Bundesdruckerei Gruppe

Konzept: Lastenheft Maschinensysteme-Maschinen-IT

Revisions-Nummer: 5.0

Inhaltsverzeichnis

1.	Sprachreglung Anforderungen	2
2.	Bewertung der Anforderungen durch den Lieferanten	2
3.	Anforderungen	3
3.1	Informationssicherheit allgemein	3
3.2	Infrastruktur	4
3.3	Hardware für technische Anlagen	4
3.4	Software für technische Anlagen	5
3.5	Lieferungen (Software, Firmware, u. ä.)	7
3.6	Lizenzen	7
3.7	Dokumentation	8
4.	Glossar	9

1. Sprachreglung Anforderungen

Bei der Beschreibung von Anforderungen für technische Systeme sind bestimmten Formulierungen und Schlüsselwörtern besondere Bedeutungen beizumessen. Die Festlegungen basieren auf den Regelungen in RFC 2119, die relevanten Schlüsselwörter wurden ins Deutsche übersetzt, das englische Originalwort ist jeweils in Klammern genannt.

Die Schlüsselwörter MUSS (MUST), DARF NICHT (MUST NOT), ERFORDERLICH (REQUIRED), SOLL (SHALL), SOLL NICHT (SHALL NOT), SOLLTE (SHOULD), SOLLTE NICHT (SHOULD NOT), EMPFOHLEN (RECOMMENDED), DARF (MAY) und OPTIONAL (OPTIONAL), welche im Rahmen der Anforderungsbeschreibung genutzt werden sollen, sind so zu interpretieren und zu verwenden, wie in RFC 2119¹ definiert.

2. Bewertung der Anforderungen durch den Lieferanten

Neben der Dokumentation zu Details und Ausprägungen der konkreten Umsetzung, wird vom Lieferanten zu jeder Anforderung eine Aussage erwartet in der Form: „*wird erfüllt*“, „*wird nicht erfüllt*“, „*wird erfüllt bis <Datumsangabe DD.MM.YYYY>*“ und „*nicht zutreffend*“.

¹ <http://www.ietf.org/rfc/rfc2119.txt>

3. Anforderungen

In den folgenden Absätzen sind die Anforderungen formuliert, die sich an den Auftragnehmer richten. Zur besseren Lesbarkeit wurden die Anforderungen deshalb nicht so formuliert, dass jedes Mal „der Auftragnehmer“ beschrieben wird. Anforderungen, die der Auftraggeber erfüllen muss, sind explizit mit dem Hinweis auf die BDr formuliert.

3.1 Informationssicherheit allgemein

Die BDr ist nach ISO 27001 zertifiziert. Darüber hinaus arbeitet die BDr auf Grund hoheitlicher Aufträge nach BSI IT-Grundschutz. Ziel ist es, die stete Verfügbarkeit, Integrität und Vertraulichkeit von Geschäftsprozessen, Informationen und Daten zu gewährleisten.

ITS-1	Die anwendbaren Maßnahmen aus den BSI IT-Grundschutz-Katalogen für IT-Systeme in der Version zum Zeitpunkt des Vertragsabschlusses MUSS vom Auftragnehmer umgesetzt werden respektive durch die BDr auf den gelieferten Komponenten umsetzbar sein. Dies ist zu bestätigen und Bestandteil der Lieferung.
ITS-2	Die Verwendung von lokalen Passwörtern DARF NICHT im Klartext erfolgen. Beispielsweise ist eine Verschlüsselung oder ein Hash zu wählen.
ITS-3	Die Vorgaben des BSI IT-Grundschutz zu Authentifizierung und Verschlüsselung MUSS eingehalten werden.
ITS-4	Um Verfügbarkeit, Integrität und Vertraulichkeit der Geschäftsprozesse der BDr zu gewährleisten, MUSS Sicherheitslücken behoben werden können.
ITS-5	Die Funktionsfähigkeit der gelieferten Komponenten MUSS nach Sicherheitsupdates gewährleistet sein.
ITS-6	Es MUSS der BDr ermöglicht werden, Schutz vor Schadsoftware auf allen Systemen zu installieren.
ITS-7	Hard- und Software MUSS mit aktivem zentral verwalteten Virens Scanner uneingeschränkt funktional sein.

3.2 Infrastruktur

Folgend wird die Anbindung der Peripherie der technischen Anlage an die BDr-Infrastruktur symbolisch dargestellt.

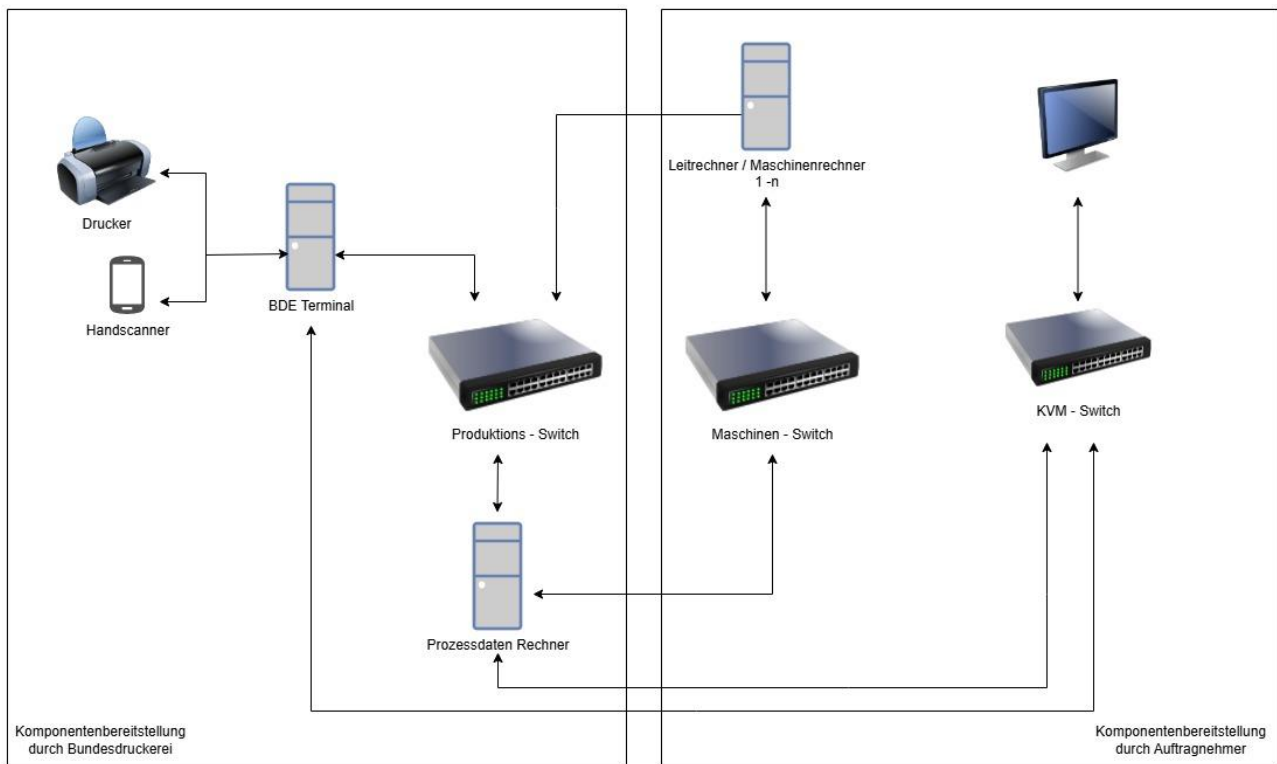


Abbildung 1

IF-1	Die BDr MUSS das BDE und deren Peripherie, sowie einen Produktions-Switch zur Anbindung der Maschine an das Produktionsnetz zur Verfügung stellen.
IF-2	Es MUSS für die Komponenten der BDr (siehe Abbildung 1) in der Anlage räumlich Platz vorgehalten werden. (Prod-Switch 1HE 19“, BDE + OPCUA ein Ablagefach, Drucker, Handscanner)
IF-3	Es MUSS für die Komponenten der BDr in der Anlage elektrische Anschlüsse vorgehalten werden.
IF-4	Der Produktions-Switch MUSS dauerhaft (auch bei ausgeschalteter Maschine) bestromt werden.
IF-5	Die Verdrahtung für die Komponenten der BDr KANN anschlussfertig in der Anlage geliefert werden.
IF-6	Die BDr MUSS dem Lieferanten die Datenblätter für die benötigten BDr-Komponenten (siehe Abbildung 1) auf Nachfrage bereitstellen.
IF-7	OPTIONAL stellt die BDr den Auftragnehmer einen MES-Simulator für die Entwicklung der Leitrechnerschnittstelle zur Verfügung.

3.3 Hardware für technische Anlagen

HW-1	Der Maschinenrechner MUSS integraler Bestandteil der Konstruktion der technischen Anlage sein.
HW-2	Der bevorzugte Hardwarelieferant der Maschinenrechner SOLL die FA. Spectra GmbH & CO. KG sein.
HW-3	Die Hardwareauswahl des benötigten Maschinenrechners und deren Formfaktor SOLL mit Zustimmung der BDr erfolgen.
HW-4	Zur Reduzierung der Variantenvielfalt der Maschinenrechner in der technischen Anlage, SOLL die Verwendung identischer Hardware erfolgen.
HW-5	Bei der Beauftragung anzuschaffender baugleicher technischer Anlagen oder Arbeitsplätzen mit Stückzahl ≥ 2 , MUSS die Verwendung typengleicher Maschinenrechner erfolgen.

HW-6	Es MUSS ein zusätzlicher, nicht montierter Satz Maschinenrechner nach Abschluss des FAT, der BDr übergeben werden. Spätestens jedoch 4 Wochen vor dem SAT. Dieser Satz Maschinenrechner bildet die Menge an Maschinenrechner ab, die zum Zeitpunkt des SAT in der Maschine erforderlich sind. Dieser Satz Maschinenrechner ist zur Bereitstellung des produktiven Festplattensatzes zwingend erforderlich und Bestandteil der Lieferung.
HW-7	Die Hardware MUSS durch den Lieferanten beigelegt und verbaut werden.
HW-8	Die Komponenten MUSS für den Einsatz im industriellen Umfeld vorgesehen sein.
HW-9	Maschinenrechner und deren Peripherie MUSS für Belastungen und unterbrechungsfreien Dauerbetrieb ausgelegt sein.
HW-10	Bei der Integration von Maschinenrechnern innerhalb geschlossener Systeme, MUSS die mittlere Raumlufttemperatur von $\leq 40^{\circ}\text{C}$ eingehalten werden.
HW-11	Für alle Maschinenrechner MUSS eine unterbrechungsfreie Stromversorgung (USV) vorgehalten werden, diese ist Bestandteil der Maschinenlieferung.
HW-12	Die Laufzeit der USV MUSS so ausgelegt sein, dass alle angeschlossenen Maschinenrechner ihre Anwendungen schließen können und den Prozess „Windows herunterfahren“ abgeschlossen haben.
HW-13	Die USV MUSS eine Leistungserweiterung von 20% erfüllen. Der Prozentsatz ist demnach das Maß der Überdimensionierung.
HW-14	Der Maschinenrechner MUSS ein Intel-RAID basiertes Managementsystem nutzen und MUSS mindestens RAID 1 erfüllen.
HW-15	Der Maschinenrechner MUSS mit 2,5 Zoll SATA Festplatten ausgestattet werden.
HW-16	Es MUSS je HDD ein 2,5 Zoll SATA -Festplattenwechselrahmen zum Einsatz kommen.
HW-17	Der Zugang zu den Festplattenwechselrahmen MUSS ohne Montagetätigkeiten und Werkzeug einfach erreichbar sein.
HW-18	Es MUSS ein Festplattensatz pro RAID-Verbund bereitgestellt werden, diese sind Bestandteil der Lieferung.
HW-19	Bei Einsatz von SSD MUSS diese eine TBW von ≥ 3000 (3 Petabytes) verwendet werden.
HW-20	Der Zugang zu allen IT-Komponenten MUSS für eine nicht elektrotechnisch unterwiesenen Person, also dem elektrotechnischen Laien, zulässig sein.
HW-21	Die Erreichbarkeit der Maschinenrechner und deren Schnittstellen MUSS ohne Montagetätigkeiten, von der Vorder- sowie Rückseite leicht zugänglich sein.
HW-22	Bei Einsatz eines KVM MUSS ein zusätzlicher Anschluss für das BDE vorgehalten werden.
HW-23	Es SOLL ein KVM der Firma ATEN genutzt werden.
HW-24	Der Maschinenrechner MUSS über eine exklusive RJ-45 (1000 Mbit/s) Netzwerkschnittstelle zur Anbindung an die BDr betriebene IT-Infrastruktur verfügen.
HW-25	Der Maschinenrechner MUSS für den Einsatz in Test- und Produktivumgebung einen von der BDr definierten Hostname und IP-Adresse erhalten können.

3.4 Software für technische Anlagen

SW-1	Als Betriebssystem für alle Rechner im Bundesdruckerei internen Netz (Test- und Produktionszustand) MUSS Windows 11 Enterprise LTSC 64 Bit verwendet werden. Verweis auf Li-6 Hinweis: Als Betriebssystem für die zugehörigen SPS SOLL Windows 11 Enterprise LTSC 64 Bit verwendet werden.
SW-2	Alle zur technischen Anlage gehörige Software MUSS passend für dieses Betriebssystem gewählt bzw. entwickelt werden.
SW-3	Werden auf den Maschinenrechner RDBMS verwendet, SOLL PostgreSQL genutzt werden. Die Verwendung von Oracle Datenbanken oder Microsoft SQL Server MUSS die Zustimmung der BDr erhalten.
SW-4	Andere Persistenz-Verfahren MUSS die Zustimmung der BDr erhalten.
SW-5	Die Installationen von Softwarekomponenten MUSS unter den Programmverzeichnissen von Microsoft erfolgen. Abweichungen hiervon benötigen die Zustimmung der BDr.
SW-6	Die Softwarekomponente DARF NICHT Schreibrechte auf Systemverzeichnisse von Windows zur Ausführung benötigen (Programmverzeichnisse, Windowsverzeichnis, etc.).
SW-7	In der BDr existieren strenge Richtlinien zur Sicherheit von IT-Systemen. Das Betriebssystem und die Softwareinstallation werden bei der BDr einer Härtung unterzogen. Die volle Funktion der Software MUSS in diesem gehärteten Umfeld gegeben sein.
SW-8	Zur Einrichtung der Software im gehärteten Umfeld MUSS Unterstützung in den Räumlichkeiten der BDr geleistet werden.

SW-9	ID- und Access-Management inkl. Rollen, notwendige Rechte MUSS durch den Auftragnehmer exakt spezifiziert werden.
SW-10	Zur Benutzer- bzw. Rollenverwaltung MUSS die gelieferte Software über eine Active-Directory-Anbindung verfügen.
SW-11	Eine Benutzerverwaltung der gelieferten Software, DARF NICHT ausschließlich lokal stattfinden.
SW-12	Die mit der Anlage gelieferte Software DARF NICHT die Rechte eines Benutzers mit Administratorrechten erfordern.
SW-13	Der Maschinenrechner MUSS als Mitglied eines Active Directory zentral verwaltbar sein.
SW-14	Die Protokollierung/Logging MUSS konfigurierbar gestaltet werden.
SW-15	Diese Konfigurationsparameter MÜSSEN mindestens sein: Loglevel, Speicherort, Größe, Aufbewahrungsdauer, Log-Rotation.
SW-16	Die Protokollierung/Logging im höchsten Level (bzw. Trace) DARF schutzbedürftige (z.B. personenbezogene Daten, Passwort, Schlüssel, etc.) Daten enthalten.
SW-17	Die Protokollierung/Logging im Loglevel < Trace, MUSS eine Protokollierung ohne schutzbedürftige Daten erfolgen.
SW-18	Die Protokollierung/Logging MUSS in Textform erfolgen.

3.5 Lieferungen (Software, Firmware, u. ä.)

Softwarelieferungen an die BDr unterliegen den Vorgaben des Configuration Managements. Die nachfolgende Abbildung beschreibt den einzuhaltenden Workflow einer Softwarelieferung.

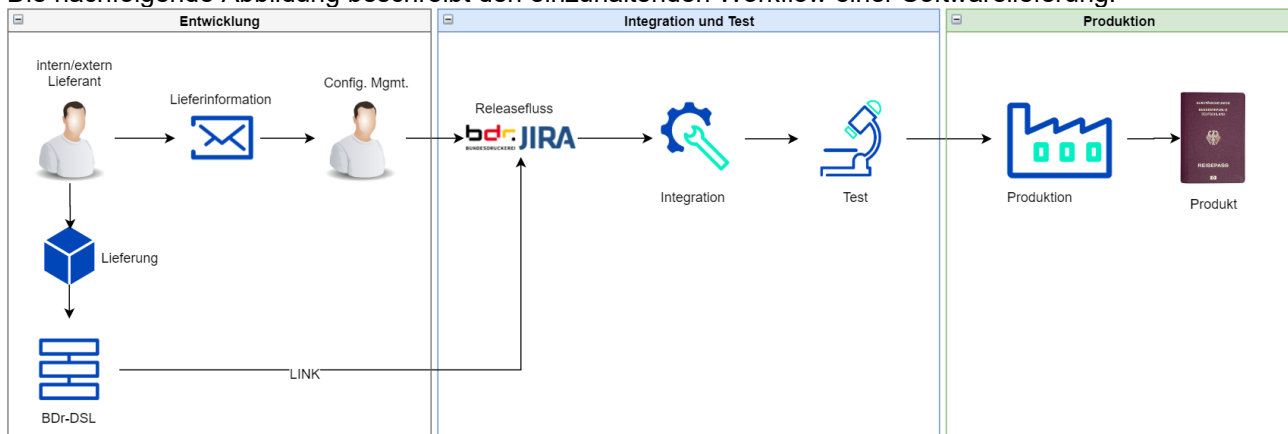


Abbildung 2

CONF-1	Die Softwarelieferung MUSS über den offiziellen Prozess der BDr und DARF NICHT per alternative Wege (z.B. via E-Mail) erfolgen.
CONF-2	Die Vorgaben der Softwarelieferungen MUSS für jeden Softwareliefergegenstand berücksichtigt werden. Beispiele: <ul style="list-style-type: none"> • Updates • Firmware • Treiber • Konfigurationsdateien
CONF-3	Die Softwarelieferung MUSS Releasenotes nach BDr-Vorgabe enthalten.
CONF-4	Die BDr MUSS dem Lieferanten ein Vorlagedokument der Releasenotes auf Anfrage zur Verfügung stellen.
CONF-5	Die Softwarelieferung MUSS versioniert sein.
CONF-6	Die Versionsnummer MUSS eindeutig sein.
CONF-7	Die Versionsnummer einer SW-Komponente DARF NICHT wiederholt genutzt werden.
CONF-8	Die Versionsnummer DARF NICHT Leer- und Sonderzeichen enthalten.
CONF-9	Die Versionsnummer SOLL dreistellig, mit Punkt getrennt sein. Hauptversion, Nebenversion und Revisionsnummer.
CONF-10	Die Softwarelieferung MUSS Installationsanweisungen enthalten.
CONF-11	Die Softwarelieferungen MUSS einzeln installierbar sein.
CONF-12	Die Softwarelieferung DARF NICHT als Image geliefert werden.
CONF-13	Der Installationsvorgang MUSS ohne Internetzugang erfolgen.
CONF-14	Jede für die volle Funktionalität der technischen Anlage benötigte Software MUSS der BDr übergeben werden. Beispielsweise: Treiber, zusätzliche benötigte Software
CONF-15	Auf Anforderung MUSS nach inkrementellen Updates, ein vollständiges Installationspaket, mit integrierten Updates geliefert werden, sodass eine Installation von mehreren, aufbauenden inkrementellen Updates vermieden werden kann.
CONF-16	Bei inkrementellen Lieferungen MUSS ein Rollback-Verfahren beschrieben sein.
CONF-17	Alle benötigten Informationen zur Weiterverwendbarkeit, Anpassungsnotwendigkeiten und Übertragung von Konfigurationsdaten bei einem Releasewechsel MUSS in der Installationsanleitung enthalten sein.

3.6 Lizenzen

Li-1	Lizenzen für jede Hard- und Software MUSS Bestandteil der Lieferung sein.
Li-2	Eine Testlizenz DARF NICHT genutzt werden.
Li-3	Ein Hardwaredongel DARF NICHT genutzt werden.
Li-4	Eine Lizenz mit beschränkter Laufzeit DARF NICHT genutzt werden.
Li-5	Ein Lizenzierungsverfahren das Internetzugang benötigt DARF NICHT genutzt werden.

Li-6	Die Lizenzierung der Betriebssysteminstallationen für die in der BDr vorhandene Test – und Produktivumgebung MUSS durch die BDr erfolgen.
------	---

3.7 Dokumentation

DOC-1	Es MUSS eine Stückliste der IT-Hardwarekomponenten von der technischen Anlage zum SAT vorliegen.
DOC-2	Es MUSS ein Netzplan zum SAT vorliegen, der alle Kommunikationsteilnehmer (aktiv und passiv) aufzeigt.
DOC-3	Die Beschriftung aller Schnittstellenkabel MUSS beidseitig eindeutig vorhanden sein.
DOC-4	Es MUSS ein Schaltplan, der die Verbindung aller Hardwarekomponenten abbildet zum SAT vorliegen.
DOC-5	<p>Die Dokumentation für die verwendeten Softwarekomponenten inkl. Treiber, Komponenten von Drittherstellern, zusätzliche Windowskomponenten etc. MUSS zum SAT vorliegen.</p> <p>Bestandteil der Dokumentation ist:</p> <ul style="list-style-type: none"> • Softwarename • Hersteller • Versionsnummer • Lizenzinfos • Installationspfad • Zugriffsrechte auf sämtlich benötigte Verzeichnisse • Verwendete Kommunikationsprotokolle (TCP/IP, UDP) und die dazugehörenden Portnummern
DOC-6	<p>Es MUSS ein Administrationshandbuch zum SAT vorliegen.</p> <p>Bestandteil dieser Dokumentation ist:</p> <ul style="list-style-type: none"> • Installationsanleitungen • Bedienerhandbücher • Verwendete Hardware aller Komponenten, inkl. der von Drittherstellern (z. B. Kameras, Scanner, Drucker, Vision-Systeme, Schnittstellenkarten, Hubs, usw.). Deren herstellerspezifischen Versionen sowie der Typbezeichnungen.
DOC-7	Die Dokumentation MUSS in digitaler Fassung im PDF/A Format übergeben werden

4. Glossar

Akronym	Erklärung
BDr	Bundesdruckerei GmbH
Maschinenrechner	Formuliert alle Rechner (mit Abgrenzung zur SPS) und deren benötigte angeschlossene Peripherie, die für den angedachten Fertigungsprozess bzw. Arbeitsgang benötigt werden. Diese können innerhalb oder außerhalb von Maschinen bereitgestellt werden.
SPS	Speicherprogrammierbare Steuerung
EOSL	End of Service Life: Ab diesem Datum unterstützt ein Hersteller ein Produkt (z. B. Software) nicht mehr; es werden auch keine Sicherheitsupdates mehr herausgebracht; Ersatzteile sind nicht mehr lieferbar etc.
RDBMS	Relationales Datenbankmanagementsystem
Checkmk	Software für das Monitoring von IT-Infrastruktur
GenuBox	Hardwarekomponente zur Netzwerk-Transportverschlüsselung
BDE	BetriebsDatenErfassung Rechner mit Benutzerschnittstelle zur Anlagenspezifischen MES-Auftragsverwaltung
MES	Manufacturing Execution System - Produktionsleitsystem
FAT	Factory Acceptance Test – Werksabnahme des Produktes beim Hersteller
SAT	Site Acceptance Test – Abnahme des Produktes beim Kunden
technische Anlage	Formuliert ein Produkt aus dem Anlagenbau
SSD	Solid State Drive
TBW	Terabytes written – Datenmenge, die ohne Ausfall garantiert auf eine SSD geschrieben werden kann.