Qualitätssicherungsstandard zur Entwicklung von Elektronik und Software durch Lieferanten
Quality assurance standard for the development of electronic components and software by suppliers

MTQ 5013

Englische Fassung ab Seite 10 / English version from page 10

Ersatz für
Ausgabe 08.2020

Inhaltsverzeichnis Seite

1	Anwendungsbereich	2
2	Normative Verweisung	2
3	Allgemeine Prozessvorgaben	2
4	Projektplanung, Projektverfolgung	3
5	Entwicklungsprozess	4
5.1	Anforderungsmanagement	4
5.2	Entwicklung	4
5.3	Review und Test	5
6	Unterstützungsprozesse	6
6.1	Änderungsmanagement	6
6.2	Konfigurationsmanagement	6
6.3	Qualitätssicherung	7
7	Safety und Security	7
7.1	Anforderungen mit funktionaler Sicherheit	7
7.2	Anforderungen an die Produkt-Cybersicherheit	7
8	Wartung und Serienbetreuung	8
9	Anhang	8
9.1	Abkürzungsverzeichnis	8
9.2	Dokumentenliste	8

Fortsetzung Seite 2 bis 18
Continued on pages 2 to 18

Fachbereich: Specialist department:	Redaktionell geprüft: Editorially checked by:	Freigegeben: Approved by:	ICS-Nr. ICS-No.
T. Daniel, TRY	A. Nitschke-Werner, TQCD	M. Katzschke, TQCD	03.100.10, 03.120.10, 31.190, 35.020, 35.080

Rolls-Royce Solutions GmbH
Für diese Werknorm behalten wir uns alle Rechte vor
All rights reserved for this Factory standard
Exportkontrollrelevanz: nicht gelistet / Export control relevance: not listed

1 Anwendungsbereich

Dieser Standard beschreibt grundlegende Anforderungen, die für die Entwicklung RRS-spezifischer Elektronik- und Softwareprodukte durch Lieferanten (nachfolgend Auftragnehmer genannt) sowie die Modifizierung von Elektronik- und Software-Produkten des Lieferanten durch den Lieferanten im Auftrag der RRS anzuwenden sind. Dieser Standard findet auch bei RRS-spezifischer Modifikation bereits vorhandener Produkte und Software Anwendung, bzw. bei sogenannten Baukastensystemen. Anteile, die nicht speziell für RRS entwickelt wurden, sind insofern zu berücksichtigen, dass zum Projektende eine geschlossene Nachweiskette vorliegt. Siehe hierzu auch Kapitel 5.3 Review und Test.

Zur Verfügung gestellte Informationen und Anforderungen bzw. ausgetauschte Informationen sind vertraulich zu behandeln und unterliegen der Geheimhaltung. Liegt kein NDA vor, so müssen entsprechende Vereinbarungen zwischen Auftragnehmer und Auftraggeber getroffen werden.

Falls der Lieferant eigene Regelungen implementiert hat, die den gleichen Zweck erfüllen wie die in diesem Dokument beschriebenen, so ist es möglich auch diese anzuwenden.
Abweichende Regelungen zu diesem Dokument bedürfen allerdings gesonderter Vereinbarung zwischen Auftragnehmer und RRS (nachfolgende Auftraggeber genannt) vor Beauftragung.

Der Daten- und Informationsaustausch kann exportrechtlichen Grundsätzen unterliegen. Hier besteht Informationspflicht durch den Auftragnehmer .

2 Normative Verweisung

Soweit projektspezifisch nichts anderes vorgegeben finden insbesondere folgende Normen / Standards branchenspezifisch Anwendung:

- DIN EN 50716 (Anwendung Rail)
- DIN EN 50129 (Anwendung Rail)
- DIN EN 61508 (generell, funktionale Sicherheit)
- EN ISO 13849 (generell, funktionale Sicherheit (Maschinenrichtlinie)
- IEC 62443
- IEC60092 (Anwendung Marine)
- IACS UR E5, E8, E10, E11, E13, E16 ,E17, E18, E19, E20, E22, E23, E25, E26, E27 (Anwendung Marine)
- CMMI for development, V2.0 (Reifegradmodell Entwicklungsprozess)
- ISO 15288/12207 (generell)
- ISO/IEC 250xx (Normenreihe, generell)
- ISO/IEC 2700x (Normenreihe, IT-Sicherheit)
- Stand der Technik

Entwicklungsumfänge für die Anwendung Marine müssen konform zu den Regularien der Klassifikationsgesellschaften sein. Details (wie z. B. anzuwendende Rules, Klassifikationsgesellschaft, Software Conformity Assessment) müssen mit dem Auftraggeber abgestimmt werden.

Normvorgaben und Standards aus Anforderungsdokumenten werden vom Auftragnehmer auf Aktualität geprüft.

3 Allgemeine Prozessvorgaben

Der Auftragnehmer pflegt im Rahmen seines Qualitätsmanagementsystems (ISO9001 gemäß MTQ5003 oder vergleichbar) einen dokumentierten Entwicklungsprozess, der bei der Entwicklung der zu liefernden Produkte angewendet wird.

Die Prozesssicherheit der Entwicklungstätigkeiten sollte durch geeignete Werkzeuge unterstützt werden.
Der Entwicklungsprozess des Auftragnehmers muss alle notwendigen Rollen, Entwicklungsschritte und Arbeitsprodukte/Dokumente gemäß den Anforderungen des Einsatzmarktes / der Domäne (z.B. Bahn, Marine, Genset, ...) oder falls kein spezifischer Einsatzmarkt spezifiziert ist, nach dem Stand der Technik anfordern.
Dazu sind auch domänenspezifische Standards heranzuziehen.

Falls notwendig und vereinbart wird der Auftragnehmer zusätzliche Arbeitsprodukte/ Dokumente erzeugen, um die Anforderungen an den Entwicklungsprozess aus diesem Dokument zu erreichen (Konsistenzprüfung Prozess- und Planungsdokumente, Einhaltung von Normen und Standards).

Der dokumentierte Entwicklungsprozess enthält auch Regelungen zu Änderungsmanagement, Konfigurationsmanagement und Qualitätssicherung (siehe Kapitel 6 Unterstützungsprozesse).

4 Projektplanung, Projektverfolgung

Der Auftragnehmer benennt Ansprechpartner für den Auftraggeber: Projektverantwortlicher und Qualitätssicherer, ggf. weitere Ansprechpartner. Ein Single Point of Contact ist zu bevorzugen.

Auf Basis der vom Auftraggeber übergebenen Anforderungen führt der Auftragnehmer vor Beauftragung eine Aufwandsschätzung durch, erstellt einen groben Projektterminplan und hält die zur Auftragsbearbeitung notwendigen Ressourcen vor (Personal, Tools, Lizenzen, Infrastruktur usw.).
Der Projektterminplan muss zur Projektverfolgung entsprechende Meilensteine enthalten.

Nach Beauftragung muss der Projektterminplan konkretisiert und detailliert werden.
Der Projektterminplan muss mit dem Auftraggeber abgestimmt werden.

Im Rahmen der Beauftragung wird zwischen Auftragnehmer und Auftraggeber eine Lieferantenschnittstellenvereinbarung abgestimmt. Über diese wird geregelt, von welcher Partei welches Arbeitsprodukt erzeugt wird, wie es ausgetauscht und abgenommen wird.

Zur regelmäßigen Abstimmung, zur Projektkontrolle bzw. zur Fortschrittskontrolle muss eine regelmäßige Abstimmung zwischen Auftragnehmer und Auftraggeber etabliert werden.
Das daraus resultierende Reporting und der Berichtsweg müssen definiert werden.

Das Reporting muss zu folgendem eine Aussage treffen:
- Einhaltung des vereinbarten Aufwandes (nur bei Dienstleistungsverträgen)
- Erreichung von Meilensteinen
- Sicherstellung der Qualität
- Arbeitsfortschritt in unterschiedlichen Projektphasen
- Fortschritt Testausführung
- Fortschritt Fehlerabarbeitung
- Projektrisiken und Maßnahmen zur Risikominderung

Die Aussage kann z. B. durch Definition und Berichten geeigneter Kennzahlen (Metriken) erfolgen.
Das Berichten relevanter Metriken orientiert sich an der jeweiligen Projektphase.

Während der Projektlaufzeit betreibt der Auftragnehmer ein angemessenes Risikomanagement und informiert den Auftraggeber über projektgefährdende Risiken.

Agile Zusammenarbeitsmodelle, z. B. SCRUM, können Anwendung finden.

Der Auftraggeber behält sich vor, erfolgskritische Prozesse gesondert zu überwachen. Die Entscheidung, was ein erfolgskritischer Prozess ist, kann im Laufe des Projekts festgelegt werden.

5 Entwicklungsprozess

5.1 Anforderungsmanagement

Die Anforderungen des Auftraggebers werden vom Auftragnehmer inhaltlich geprüft. Die anzuwendenden Prüfkriterien sind mindestens:

- Verständlichkeit,
- Widerspruchsfreiheit,
- Eindeutigkeit,
- Angemessenheit des Umfangs,
- Korrektheit des Inhalts,
- Testbarkeit.

Auf Basis der vom Auftraggeber übergebenen Anforderungen erstellt der Auftragnehmer ein Pflichtenheft (oder ein vergleichbares Dokument, welchen einen Pflichtenheft-Charakter hat).
Das Pflichtenheft muss mindestens die folgenden Beschreibungen beinhalten:

- Zielbestimmung
- Geplante Betriebsbedingungen
- Produktübersicht
- Liste der Produktfunktionen
- Qualitätsanforderungen
- Nichtfunktionale Anforderungen
- Notwendige technische Produktumgebung und Schnittstellen
- Hardware, Software

Das Pflichtenheft muss mit dem Auftraggeber abgestimmt werden.
Bei kleineren Gewerken kann das Pflichtenheft auch zusammen mit dem Auftraggeber erstellt werden. Das Vorgehen muss zwischen Auftragnehmer und Auftraggeber abgestimmt werden.

Die Anforderungen des Auftraggebers müssen geeignet verwaltet werden. Ein Schutz vor unberechtigter Änderung ist vorzusehen.

5.2 Entwicklung

Die Reife des Entwicklungsprozesses muss vor Auftragsvergabe nachgewiesen werden. Der Auftragnehmer kann die Nachweise wahlweise insbesondere wie folgt erbringen:

- detaillierter Bericht über ein durchgeführtes CMMI Appraisal bis Maturity Level 2,
- detaillierter Bericht über ein AutomotiveSpice Assessment HIS Scope,
- ein detaillierter Bericht bzgl. der Einhaltung der Prozessanforderungen im Rahmen der domänenspezifischen Prüfung der funktionalen Sicherheit
- ein RRS Lieferantenaudit mit Fokus Entwicklung
- für Cyber Security ein Audit nach IEC 62443-4-1,
- externe Audits durch Kunden aus vergleichbaren Industrien
- Zertifizierungen des Unternehmens durch Standards wie z. B. DIN EN ISO 9100, IRIS, ISO 13485, KTA-IAEA-Zulassung

Dieses Liste ist nicht abschließend. Der Lieferant kann die Reife seines Entwicklungsprozesses auch durch andere, geeignete Nachweise führen. Diese bedürfen jedoch der Abstimmung mit dem Auftraggeber.

Die Anforderungen des Auftraggebers werden im Entwicklungsprozess in Arbeitsprodukte überführt.
Ein dem aktuellen Industriestandard entsprechendes Vorgehensmodell nach Stand der Technik ist anzuwenden.

Der Auftragnehmer muss anhand von konkreten Entwicklungsdokumenten nachweisen, wie er das Produkt entwickelt oder ändert, insbesondere Anforderungen, Realisierung, Test, Traceability.
Zu den Entwicklungsdokumenten zählen:

- (Software-)Entwurfsdokumente
- Architekturdokumente
- (Modul-)Designdokumente

Die Softwarearchitektur muss die Schnittstellen des Softwaresystems mit der Umgebung vollständig abbilden.
Die Schnittstellen für jedes Strukturelement müssen beschrieben sein.

Wichtige Designentscheidungen müssen dokumentiert werden (u. a. Begründungen, Abwägungen, warum das Design so gewählt wurde und nicht anders). Dies unterstützt eine konsistente Umsetzung und reduziert Fehlinterpretationen.

Die Programmiersprache muss so ausgewählt werden, dass sie für den Zweck geeignet ist.
RRS empfiehlt die Anwendung von etablierten Codier-Richtlinien (z. B. MISRA-C, EN 61131, EN 61131-3).
Bei modellbasierter Entwicklung sollte äquivalent dazu ein Standard angezogen werden.

Generell ist das Softwaresystem so zu gestalten, dass Softwarekomponenten einfach integriert werden können. Gleiches gilt für das Zusammenspiel aus Betriebssystem und SW-Versionen.
Integrationsschritte sind geeignet zu testen.

Die Entwicklung muss grundsätzlich mit geeigneten Werkzeugen erfolgen.
Die eingesetzten Tools mit ihrer jeweiligen Version und Einstellung sind im Projekt zu dokumentieren.
Bei Änderungen sind die Auswirkungen zu prüfen.

Branchenspezifische Standards können eine gesonderte Tool-Qualifizierung fordern.
Vor Einsatz eines Werkzeugs ist abzuprüfen, ob eine Qualifizierung des Tools erforderlich ist.
RRS ist über das Ergebnis der Tool-Qualifizierung zu informieren.

Besteht die Notwendigkeit, im Projekt ein SW-Tool zu entwickeln, so müssen die Anforderungen an das Tool die Randbedingungen des Projekts abbilden.
Vor Freigabe ist das entwickelte Tool geeignet zu testen.
Schulungsmaßnahmen für Anwender sind vorzusehen, die zugehörige Benutzerdokumentation muss vorhanden und freigegeben sein.
Die Rechte an diesem SW-Tool sind zwischen Auftragnehmer und Auftraggeber zu klären.
Besteht für das SW-Tool die Notwendigkeit einer Toolqualifizierung, so ist diese entsprechend durchzuführen.

5.3 Review und Test

Der Auftragnehmer hat eine dokumentierte Review- und Teststrategie für sein Produkt und wendet diese an.
Angewendete Review- und Testmethoden sind dokumentiert.

Die Teststrategie beschreibt auch, wie mit gefundenen Fehlern umgegangen wird.
Reviews werden nach dem 4 Augen Prinzip und ansonsten nach domänenspezifisch Regeln durchgeführt.
Reviews werden nachvollziehbar dokumentiert.

Der Auftragnehmer weist nach, dass die an das Produkt gestellten Anforderungen vollständig getestet werden.
Dazu werden Testprotokolle, Review-Protokolle und Berichte über Abweichungen dem Auftraggeber zur Verfügung gestellt.
Ist ein vollständiger Test nicht möglich, so sind alternative Nachweise (z. B. Analysen) zu liefern.

Der Auftragnehmer sollte Tests auf verschiedenen Testebenen durchführen. Domänenspezifische Testmethoden sind zu verwenden.
Die Testmethoden sollten die Standards nach ISTQB beinhalten, insbesondere Grenzwertanalyse, Äquivalenzklassen, Negativtest, Robustheitstest.

Für Softwaretests wird eine dokumentierte Testabdeckung gefordert, die mindestens C0 entspricht.
Tests werden von unabhängigem Personal durchgeführt. Dies bedeutet zumindest, dass der Test nicht von der Person durchgeführt wird, die die Entwicklung durchgeführt hat. Ansonsten gelten domänenspezifische Regeln.
Der Auftragnehmer sollte statische Analysen und Code Reviews auf das Produkt durchführen.
Der Auftragnehmer stellt sicher, dass alle Tests reproduzierbar sind und nachvollziehbar dokumentiert werden.
Die verwendete Testumgebung ist vollständig beschrieben und ist unter Versionskontrolle.

Auf Wunsch von RRS werden aktuelle Testberichte passend zum gelieferten Produkt geliefert, die folgendes erkennen lassen:
- die Testerfüllung
- die Testabdeckung
- die Testbewertung inkl. kritischer Fehler
- die Identifikation des getesteten Produktes.

Auf Wunsch von RRS werden aktuelle Freigabeberichte/Freigabemitteilungen passend zum gelieferten Produkt geliefert.
Die Lieferung erfolgt jeweils gemäß der Lieferantenschnittstellenvereinbarung.

Zu definierten Zeitpunkten, spätestens jedoch am Ende des Projekts übergibt der Auftragnehmer soweit nicht anders vertraglich vereinbart an den Auftraggeber
- die ausführbare Software (Executable),
- den Quellcode,
- die Testdokumentation,
- die Dokumentation der Software inklusive Änderungsdokumentation, Schnittstellendokumentationen, Installations- und/oder Integrationsbeschreibungen.

Falls vorhanden müssen abgeleitete Anforderungen ebenfalls übergeben werden.

Gesonderte Nachweise (z. B. zur funktionalen Sicherheit, IT Sicherheit, Datenschutz oder ähnlichem) werden projektspezifisch vereinbart und ebenfalls zum definierten Zeitpunkt übergeben.

6 Unterstützungsprozesse

6.1 Änderungsmanagement

Der Auftragnehmer muss für Änderungen an seinen Produkten ein strukturiertes Änderungsmanagement betreiben, dass entsprechend dem Entwicklungsprozess Entwicklungsschritte und Arbeitsprodukte in gleicher Reife nachvollziehbar erzeugt.
Änderungen müssen nachvollziehbar dokumentiert werden.
Auf Wunsch von RRS liefert der Auftragnehmer die Änderungshistorie mit detaillierten Änderungen des Produktes.
Ein toolgestütztes Vorgehen wird empfohlen.

Werden von Seiten Auftraggeber Änderungen an Anforderungen vorgenommen, so sind diese durch den Auftragnehmer zu bewerten und Auswirkungen transparent aufzuzeigen.
Gleiches gilt für Änderungen, welche die Zusammenarbeit betreffen.
Änderungen an den Anforderungen müssen rückverfolgbar sein.

6.2 Konfigurationsmanagement

Zur Gewährleistung der Wiederauffindbarkeit und um die Integrität der Arbeitsprodukte sicherzustellen, richtet der Auftragnehmer ein geeignetes Vorgehen zur Identifikation und Steuerung von Produkt- und Projektdokumenten ein (Konfigurationsmanagement).
Ein toolgestütztes Vorgehen wird empfohlen.
Das Konfigurationsmanagement muss über die Projektlaufzeit aufrechterhalten und soweit nicht anders vertraglich vereinbart im Wartungsfall fortgesetzt werden. Die Daten müssen im Rahmen der Liefer-Gewährleistungs- und Ersatzteilverpflichtung (somit über die Projektlaufzeit hinaus) zugänglich sein.

Die Arbeitsprodukte sind vor unberechtigter Änderung und Verlust zu schützen.
Eine entsprechende Datensicherung ist vorzusehen, zu planen und regelmäßig auszuführen (Backupstrategie).

Lieferungen des Auftragnehmers werden in einer geprüften Lieferbaseline zusammengefasst.

6.3 Qualitätssicherung

Der Auftragnehmer stellt mit einer kontinuierlichen, geplanten Qualitätssicherung sicher, dass der definierte Entwicklungs- sowie Änderungsprozess eingehalten wird und dass Abweichungen von diesem Prozess transparent berichtet und behoben werden.
Qualitätssicherung wird über die Projektlaufzeit aufrechterhalten.

Auf Wunsch von RRS stellt der Auftragnehmer aktuelle Qualitätssicherungsberichte zum Produkt zur Verfügung, aus denen die Qualitätssicherungsaktivitäten sowie der Qualitätsstatus der Prozesseinhaltung ersichtlich ist. Berichtsintervalle und Inhalte sind bei Bedarf mit den Projektverantwortlichen abzustimmen.

RRS behält sich vor, auch eigene QS-Reviews und Audits durchzuführen. Die Durchführung erfolgt bei Bedarf oder regelmäßig (vergleiche 4 Projektplanung, Projektverfolgung, erfolgskritische Prozesse) gemäß RRS-Prozess bzw. domänenspezifischen Standards.

7 Safety und Security

7.1 Anforderungen mit funktionaler Sicherheit

Werden sicherheitsrelevante Funktionen durch das Produkt des Auftragnehmers realisiert, so sind durch den Auftragnehmer die zusätzlich Anforderungen an Produktsicherheit und Funktionale Sicherheit zu erfüllen, die sich aus relevanten Standards ergeben.
Insbesondere muss der Auftragnehmer für sein Produkt eine Gefahren- und Risikoanalyse durchführen.

Gefährdungen, die von dem Produkt ausgehen und Gefährdungen, die von dem Produkt gemindert werden, werden zu definierten Zeitpunkten, jedoch spätestens am Projektende an den Auftraggeber übergeben.

7.2 Anforderungen an die Produkt-Cybersicherheit

Die Anforderungen an die Produkt-Cybersicherheit richten sich nach der Qualitätsnorm MTQ 5014 (Produkt-Cybersicherheitsbedingungen für Lieferanten). Diese ist in der jeweils gültigen Fassung anzuwenden.

Für die Umsetzung der Anforderungen der Produkt-Cybersicherheit gewährleistet der Auftragnehmer, dass sein Produkt nach einem anerkannten Standard der IT oder OT-Sicherheit, z.B. IEC 62443-4-1 entwickelt und hergestellt wird, wobei ein strukturierter, sicherer Entwicklungsprozess einschließlich Konfigurationsmanagement und Qualitätssicherung zugrunde gelegt wird.

Produkt-Cybersicherheitsrisiken wurden durch den Auftragnehmer bei der Planung, Entwicklung und Herstellung des Vertragsproduktes berücksichtigt, das zu liefernde Produkt muss compliant zum EU Cyber Resilience Act sein.

Die folgenden Arbeitsprodukte werden vom Auftragnehmer erstellt und gereviewed geliefert:

- Abgestimmte Security Anforderungen / Security Level
- Threat & Risk Assessment mit für das Produkt zutreffenden Risiken
- Security Konzept inkl. Schlüsselkonzept und Härtungskonzept
- Software Bill of Material (SBOM)
- Funktionale Security Testbericht (siehe Kap. 5.3) mit den Testmethoden aus der IEC 62443-4-1
- Schwachstellenscan /-analysebericht
- Penetrationtestbericht (wenn vereinbart)
- Fertigungskonzept zur sicheren Produktion
- Handbuch mit
    - o dem Verwendungszweck /
    - o essentiellen Funktionen sowie dem vorhersehbaren Fehlgebrauch
    - o Anleitung zur sicheren Einstellung
    - o Anleitung zur sicheren Wartung
- Alle Informationen, die benötigt werden, um die technische Dokumentation im Sinne des EU Cyber Resilience Act zu erfüllen
- Nachweis der essentiellen Anforderungen des EU Cyber Resilience Act Annex I, Teil 1 und Teil 2
- Nachweis der Schadsoftwarefreiheit

8 Wartung und Serienbetreuung

Die längerfristige Wartbarkeit der Software muss sichergestellt werden, soweit eine weitere Pflege der Software in Verantwortung des Auftragnehmers liegt.

9 Anhang

9.1 Abkürzungsverzeichnis

Abkürzung	Bedeutung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMMI	Capability Maturity Model Integration
C0	Anweisungsüberdeckungstest
DIN	Deutsches Institut für Normung
DNV GL	Zusammenschluss aus Det Norske Veritas und Germanischer Lloyd
EN	Europäische Norm
HIS	Herstellerinitiative Software
IEC	International Electrotechnical Commission
ISO	Internationale Organisation für Normung
ISTQB	International Software Testing Qualifications Board
IT	Informationstechnik
MISRA	Motor Industry Software Reliability Association
MISRA-C	Analog MISRA, Definitionen für den Sprachumfang der Programmiersprache C
RRS	RRS Friedrichshafen GmbH

9.2 Dokumentenliste

Die nachfolgende Liste fasst die in dieser Werknorm genannten Dokumente zusammen. Die einzelnen Dokumente können beim Auftragnehmer anders benannt sein.

Dokument	Beschreibung, Inhalt
Anforderungsdokument Lastenheft	Dokumentierte Anforderungen
Prozessbeschreibung	Beschreibung von Prozessen
Gefahren- und Risikoanalyse	Identifiziert Risikominderungsbedarf, der wiederum Anforderungen an das zu entwickelnde Produkt erzeugt
IT-Sicherheitskonzept	Beschreibt Maßnahmen zur Verfolgung der Ziele und Strategien, die in der Leitlinie zur Informationssicherheit beschrieben sind.
Type Approval	Bescheinigung der Typzulassung
Aufwandsschätzung	Abschätzung für die Projektplanung
Projektterminplan	Rahmentermine, Meilensteine, Zeitplanung des Projekts
Lieferantenschnittstellenvereinbarung	Beschreibt die Schnittstelle zwischen Auftragnehmer und Auftraggeber, die auszutauschenden Dokumente und Arbeitsprodukte, die Art des Austauschs und die Abnahme der Dokumente und Arbeitsprodukte
Projektreporting Lieferant	Reporting Projektfortschritt, definierte Kennzahlen, kundenrelevante Informationen, ggf. Unterstützungsbedarf
Pflichtenheft	Konkrete Lösung und Umsetzung zu den Anforderungen des Auftraggebers
Zertifikat	Dokumentation einer Übereinstimmung mit einem Standard oder einer Norm
Auditbericht	Bericht über eine Überprüfung durch eine unabhängige Stelle
Entwicklungsdokumente	Dokumente die im Entwicklungsprozess entstehen. Sie beschreiben das Vorgehen und die Ergebnisse
Entwurfsdokumente	Beschreiben den Entwurf der Lösung

Dokument	**Beschreibung, Inhalt**
Architekturdokumente	Beschreiben die Architektur der Lösung
Designdokumente	Beschreiben das Design der Lösung
Schnittstellenbeschreibungen	Beschreiben die Schnittstellen der Lösung
Reviewstrategie	Beschreiben das Vorgehen bzgl. Reviews.
Teststrategie	Beschreiben das Vorgehen bzgl. Tests
Reviewprotokoll	Dokumentiert ein durchgeführtes Review
Testprotokoll Testbericht Testdokumentation	Dokumentiert die Testausführung mit Ergebnissen, Abweichungen und Begründungen
Freigabe	Attestiert die Freigabe auf Basis von Tests gegen die Anforderungen; Unter Umständen sind Bedingungen an die Freigabe geknüpft, die zwischen Auftraggeber und Auftragnehmer abgestimmt sein müssen.
Dokumentation	Dokumentiert das Entwicklungsergebnis. Dazu gehören unter anderem Schnittstellen, Quellcode, Zeichnungen, Installations- und Integrationsvorgaben, Benutzeranleitungen usw.
QS-Planung	Planung qualitätssichernder Aktivitäten in Zeit und Umfang
QS-Bericht	Bericht über Aktivitäten der Qualitätssicherung, inkl. identifizierter Abweichungen.

Ergänzende Angaben

Frühere Ausgaben

08.2020

Änderungen

- Anpassungen zur Erfüllung des EU Cyber Resilience Act.
- Norm redaktionell überarbeitet

ENDE DER DEUTSCHEN FASSSUNG!

The *English* version is a translation. In case of dispute the German original will govern.

Replaces
Edition 08.2020

CONTENTS Page

1 Scope ... 11

2 Reference standards ... 11

3 General process requirements ... 11

4 Project planning, project monitoring ... 12

5 Development process ... 13
5.1 Requirement management ... 13
5.2 Development ... 13
5.3 Review and testing ... 14

6 Support processes ... 15
6.1 Change management ... 15
6.2 Configuration management ... 15
6.3 Quality assurance ... 15

7 Safety and security ... 16
7.1 Requirements involving functional safety ... 16
7.2 Requirements for IT security ... 16

8 Maintenance and series development ... 16

9 Annex ... 17
9.1 List of abbreviations ... 17
9.2 List of documents ... 17

1 Scope

This standard describes basic requirements for the development of electronic and software products specifically for RRS by suppliers (hereinafter referred to as the Contractor) and the modification of supplier's own electronic and software products at RRS's request. This standard also applies when modifying existing products and software specifically for RRS, as well as so-called modular systems. Any associated parts which are not developed specifically for RRS shall be duly incorporated such as to complete a closed chain of evidence at project closeout. See section 5.3 Review and testing.

All information and requirements obtained, disclosed or exchanged shall be treated as strictly confidential. In the absence of any NDA, similar arrangements shall be made between Contractor and Customer.

Contractors may also apply their own directives insofar as these duly reflect the content of this document to all intents and purposes.
However, any provisions which deviate from those described in this document shall be subject to separate agreement between the Contractor and RRS (hereinafter referred to as the Customer) prior to order placement.

The exchange of data and information may be subject to the recognized principles of export law. The Contractor shall provide the necessary information in this regard.

2 Reference standards

Unless otherwise agreed to meet project requirements, the following industry-specific norms and standards shall apply in particular:

- DIN EN 50716 (Rail applications)
- DIN EN 50129 (Rail applications)
- DIN EN 61508 (general, functional safety)
- IEC 62443
- EN ISO 13849 (general, functional safety (Machinery Directive))
- IEC60092 (Marine applications)
- IACS UR E5, E8, E10, E11, E13, E16 ,E17, E18, E19, E20, E22, E23, E25, E26, E27 (Marine applications)
- CMMI for development, V2.0 (capability maturity model for the development process)
- ISO 15288/12207 (general)
- ISO/IEC 250xx (series of standards, general)
- ISO/IEC 2700x (series of standards, IT security)
- State of the art

Development scopes for Marine applications shall comply with classification society regulations. Details (e.g. applicable rules, classification society, Software Conformity Assessment) are subject to prior arrangement with the Customer.

The Contractor shall verify that the norms and standards specified in the requirement documents are current.

3 General process requirements

The Contractor shall maintain a documented development process on the basis of his quality management system (ISO9001 as per MTQ5003 or similar) which shall be applied when developing the products included the scope of supply.

The process reliability of the development activities should be assisted by the use of appropriate tools.
The development process of the Contractor shall incorporate all the necessary roles, development steps and work products/documents required by the field of application or domain concerned (e.g. Rail, Marine, Genset, ...) or, in the absence of specific market-sector requirements, established state-of-the-art principles.
Domain-specific standards shall also serve as reference.

Where necessary and subject to agreement, the Contractor shall create additional work products / documents in order to meet the requirements stipulated for the development process in this document (verification of process and planning document consistency, demonstration of compliance with norms and standards).

The documented development process shall also regulate change management, configuration management and quality assurance (see section 6 Support processes).

4 Project planning, project monitoring

The Contractor shall appoint contacts for the Customer: Project Responsible and Quality Assurance Officer, other contacts as necessary. A designated Single Point of Contact is the preferred arrangement.

Prior to order placement, the Contractor shall estimate the effort involved and outline a rough project schedule based on the requirements submitted by the Customer and secure those resources (in terms of personnel, tools, licenses, infrastructure etc.) deemed necessary to process the order.
The project schedule shall include appropriate milestones to facilitate project monitoring.

The project schedule shall be elaborated with detail following order placement.
The project schedule shall be agreed with the Customer.

A Supplier Interface Agreement shall be drawn up between the Contractor and the Customer in the course of order placement. Said agreement shall define the respective responsibilities of the parties for creating the various work products and how these are to be exchanged and accepted.

Routine coordination procedures for purposes of project and progress monitoring shall be established between the Contractor and the Customer.
Subsequent reporting and reporting paths shall be defined.

Status reports shall include:
- Budget compliance (service contracts only)
- Milestone achievement
- Quality assurance
- Work progress in various project phases
- Testing progress
- Troubleshooting progress
- Project risks and risk mitigation measures

Status reports may be based on e.g. defined key figures (metrics) where appropriate.
Reporting on relevant metrics depends on the project phase concerned.

The Contractor shall implement appropriate risk management strategies and inform the Customer of any risks which might jeopardize the project.

Agile collaboration models, e.g. SCRUM may be deployed.

The Customer reserves the right to separately monitor mission-critical processes. Mission-critical processes can be defined over the course of the project.

5 Development process

5.1 Requirement management

The Contractor shall review the content of the requirements stipulated by the Customer. The following criteria shall be verified as a minimum requirement:

- Comprehensibility
- Consistency
- Clarity
- Reasonability of scope
- Correctness of content
- Testability

The Contractor shall draft a functional specification (or similar document having the character of a functional specification) based on the requirements specified by the Customer.
The functional specification shall include the following descriptions as a minimum requirement:

- Objective
- Intended operating conditions
- Product summary
- List of product functionalities
- Quality requirements
- Non-functional requirements
- Technical environment and interfaces required for the product
- Hardware, software

The fine specifications shall be agreed with the Customer.
In the case of less major deliverables, the fine specifications may also be drafted together with the Customer by mutual agreement between Contractor and Customer.

Customer requirements shall be handled appropriately at all times including provisions to preclude unauthorized changes.

5.2 Development

The maturity of the development process shall be duly demonstrated prior to order placement. The Contractor may provide objective evidence particularly in the forms listed below at his discretion:

- Detailed report of a CMMI Appraisal conducted up to Maturity Level 2
- Detailed report of an AutomotiveSpice Assessment HIS Scope
- Detailed report on compliance with process requirements based on domain-specific verification of functional safety
- An RRS supplier audit centered on development activities
- for Cyber Security an Audit according to IEC 62443-4-1,
- External audits conducted by clients from similar sectors of industry
- Certification of the enterprise to certain standards e.g. DIN EN ISO 9100, IRIS, ISO 13485, KTA-IAEA approval

This list is not intended to be exhaustive. The Contractor may also provide other appropriate evidence to demonstrate the maturity of his development process by agreement with the Customer.

The requirements of the Customer are incorporated in work products over the course of the development process.
A state-of-the-art procedure model corresponding to the latest industrial standards shall be applied.

Based on existing development documents, the Contractor shall demonstrate how the product is developed or modified, focusing particularly on requirements, realization, testing and traceability.
Development documents shall include, but not be limited to:

- (Software) design documents
- Architecture documents
- (Module) design documents

The software architecture shall comprehensively portray the interfaces of the software system with its environment.
The interfaces of each structural element shall be described.

Significant decisions affecting design shall be duly documented (including considerations and justification of why a particular design was favored over another). This facilitates a consistent approach to implementation and reduces the potential for misinterpretation.

The programming language chosen shall be fit for purpose.
RRS recommends using established coding standards (e.g. MISRA-C, EN 61131, EN 61131-3).
An equivalent standard should be applied in the case of model-based development.

The software system shall be generally designed such as to facilitate the integration of software components. The same applies to interaction between the operating system and software versions.
Integration measures shall be appropriately tested.

Appropriate tools shall be used throughout development without exception.
Tools used, including details of their respective versions and settings, shall be documented accordingly in the project.
The impact of any changes shall be duly appraised.

Industry-specific standards may require separate tool qualification.
The need for tool qualification shall be verified prior to its deployment.
RRS shall be notified of the results of tool qualification.

Should the project entail the development of a SW tool, its requirements shall reflect the boundary conditions of the project.
The developed tool shall be appropriately tested prior to release.
User training shall be provided and relevant user documentation released.
All rights related to this software tool shall be clarified by mutual agreement between the Contractor and the Customer.
Tool qualification shall be conducted accordingly as and when necessary.

5.3 Review and testing

The Contractor has a documented review and test strategy in place for his product which shall be duly applied.
Those review and test methods actually used shall be documented.

The test strategy shall also describe the handling of any nonconformities it reveals.
The two-person rule shall apply and any other domain-specific regulations when conducting reviews.
Reviews shall be documented to assure transparency.

The Contractor shall demonstrate that the requirements made of the product are comprehensively tested.
Test protocols, review protocols and nonconformity reports shall be submitted to the Customer for this purpose.
Alternative evidence (e.g. analyses) shall be provided if full-scale testing is unfeasible.

The Contractor should conduct tests on various levels. Domain-specific test methods shall be used.
Test methods should include ISTQB standards particularly boundary value analysis, equivalence classes, negative testing, robustness testing.

Documented test coverage to C0 is the minimum requirement for software testing.
Tests shall be conducted by independent personnel. This means that the person conducting testing and the person who developed the product are at least not one and the same person. Domain-specific regulations shall apply otherwise.
The Contractor should subject the product to static analyses and code reviews.
The Contractor shall ensure that all tests are reproducible and are documented to assure transparency.
The test environment shall be described in full detail and placed under version control.

The latest test reports relating to the delivered product shall be submitted upon Customer request to confirm:

- Test compliance
- Test coverage
- Test evaluation incl. critical nonconformities
- Identification of the tested product.

The latest release reports/notes relating to the delivered product shall be submitted upon Customer request.
Deliveries shall comply with the Supplier Interface Agreement.

Unless otherwise stipulated, the Contractor shall hand over the following at the defined dates, or by project closeout at the latest

- The executable software
- The source code
- The test documentation
- The software documentation including revision documentation, interface documentation, installation and/or integration descriptions.

Any derived requirements shall also be submitted.

Any additional evidence (e.g. of functional safety, IT security, data protection, etc.) subject to project-specific agreement shall also be handed over at the agreed time.

6 Support processes

6.1 Change management

The Contractor shall implement structured change management to demonstrably create development steps and work products of equal maturity when making any alterations to his product.
Changes shall be documented to assure transparency.
The Contractor shall submit the change history detailing all changes made to the product upon Customer request .
A tool-based approach is recommended.

The Contractor shall evaluate any changes made to the requirements made by the Customer and clearly demonstrate any impact these may have.
The same applies to any changes affecting collaboration.
Any changes made to the requirements shall be traceable.

6.2 Configuration management

The Contractor shall establish a suitable procedure for the identification and control of product and project documents (configuration management) to ensure the retrievability and integrity of the work products.
A tool-based approach is recommended.
Configuration management shall be maintained throughout the duration of the project and, unless otherwise contractually agreed, shall be continued in case of maintenance. Data shall be accessible within the scope of the delivery, warranty and spare parts obligations (thus beyond the duration of the project).

Work products shall be duly protected to prevent unauthorized change and loss.
An appropriate data backup strategy shall be conceived, planned and implemented at regular intervals.

Contractor deliveries shall be summarized in a verified delivery baseline.

6.3 Quality assurance

By means of continuous, planned quality assurance, the Contractor shall ensure compliance with the defined development and change process and that any deviations from this process are transparently reported and duly remedied.
Quality assurance shall be maintained throughout the duration of the project.

Upon Customer request, the Contractor shall provide up-to-date quality assurance reports on the product demonstrating quality assurance activities and the process compliance quality status. Reporting intervals and content shall be arranged with the parties responsible for the project as necessary.

The Customer reserves the right to conduct his own QA reviews and audits as necessary or at routine intervals (cf. section 4 Project planning, project monitoring, Mission-critical processes) in accordance with RRS process or domain-specific standards.

7 Safety and security

7.1 Requirements involving functional safety

Should his product implement safety-critical functions, the Contractor shall meet all additional product and functional safety requirements pursuant to the relevant standards.
The Contractor shall in particular conduct a hazard and risk analysis for his product.

The Customer shall receive due notification of any hazards emanating from and/or mitigated by the product at defined points in time, but no later than at project closeout.

7.2 Requirements for IT security

Product cybersecurity requirements are based on the MTQ 5014 quality standard (Product Cybersecurity Conditions for Suppliers). This is to be applied in the current version.

For the implementation of product cybersecurity requirements, the Contractor shall ensure that its product is developed and manufactured in accordance with a recognized standard of IT or OT security, e.g. IEC 62443-4-1, based on a structured, secure development process including configuration management and quality assurance.

Product cybersecurity risks have been taken into account by the contractor in the planning, development and manufacture of the contract product, and the product to be delivered must be compliant with the EU Cyber Resilience Act.

The following work products will be prepared and reviewed by the contractor:

- Agreed security requirements / security level
- Threat & Risk Assessment with risks applicable to the product
- Security concept incl. key concept and hardening concept
- Software Bill of Material (SBOM)
- Functional security test report (see chapter 5.3) with the test methods from IEC 62443-4-1
- Vulnerability Scan/Analysis Report
- Penetration test report (if agreed)
- Manufacturing concept for secure production
- Manual with
    - the intended use /
    - essential functions as well as foreseeable misuse
    - Secure Configuration Guide
    - Secure Maintenance Guide
- All the information needed to comply with the technical documentation as defined by the EU Cyber Resilience Act
- Proof of essential requirements of the EU Cyber Resilience Act Annex I, Part 1 and Part 2
- Proof of malware-free software

8 Maintenance and series development

Long-term software maintainability shall be assured where responsibility for ongoing software maintenance lies with the Contractor.

9 Annex

9.1 List of abbreviations

Abbreviation	Meaning
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for IT Security)
CMMI	Capability Maturity Model Integration
C0	Structural test coverage
DIN	Deutsches Institut für Normung (German National Standards Institute)
DNV GL	Amalgamation of Det Norske Veritas and Germanischer Lloyd
EN	European Norm/Standard
HIS	Herstellerinitiative Software (OEM Software Initiative)
IEC	International Electrotechnical Commission
ISO	International Standard Organisation
ISTQB	International Software Testing Qualifications Board
IT	Information Technology
MISRA	Motor Industry Software Reliability Association
MISRA-C	As for MISRA, definition of language scope for programming language C
RRS	RRS Friedrichshafen GmbH

9.2 List of documents

An overview of the documents referenced in this factory standard is provided below. The Contractor may use different terms for some of these publications.

Document	Description, content
Requirement document Concept specifications	Documented requirements
Process description	Description of the processes
Hazard and risk analysis	Identifies any need for risk mitigation which in turn creates requirements for the product under development
IT safety concept	Describes measures to pursue the goals and strategies described in the information security policy.
Type approval certificate	Certificate confirming type approval
Effort estimation	Estimate for project planning
Project schedule	General target dates, milestones, project time schedule
Supplier Interface Agreement	Describes the interface between Contractor and Customer, documents and work products to be exchanged, the means of exchange and acceptance of documents and work products
Project reporting – Supplier	Project progress reporting, defined metrics, customer information, need for assistance where necessary
Functional/fine specifications	Solution for and implementation of Customer's requirements in concrete terms
Certificate	Document confirming conformance with a standard or norm
Audit report	Report of an inspection by an independent body
Development documents	Documents created over the course of the development process describing the approach and results
Concept documents	Describe the concept of the solution
Architecture documents	Describe the architecture of the solution
Design documents	Describe the design of the solution
Interface descriptions	Describe the interfaces of the solution
Review strategy	Describe the review procedure.
Test strategy	Describe the testing procedure
Review protocol	Documents a completed review

Document	**Description, content**
Test protocol Test report Test documentation	Document testing and results, deviations and justification
Release	Confirms approval based on testing against requirements; certain conditions agreed between the Customer and the Contractor may be linked to release.
Documentation	Documents the results of the development. May include interfaces, source code, drawings, installation and integration requirements, user manuals, etc.
QA plan	Planning of quality assurance activities including schedule and scope
QA report	Report on quality assurance activities, incl. established nonconformities.

Supplementary Information

Previous editions

08.2020

Changes

- Adaptions for the fulfilment of the EU Cyber-Resilience Act
- Standard editorially revised