Zertifizierungsprogramm

für Produkte und Prozesse

CERTIFER Deutschland GmbH
Zertifizierungsstelle
Adam-Klein-Str. 26
D-90429 Nürnberg

Telefon: +49 911 520992-0
Fax: +49 911 520992-10

VA_650_150
Version VA: 1.3

Inhaltsverzeichnis

1. ALLGEMEINES

1.2 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AD	Allgemeine Dokumentation
AGB	Allgemeine Geschäftsbedingungen
FB	Formblatt
QM	Qualitätsmanagement
VA	Verfahrensanweisung
VL	Vorlage
ZE	Zertifizierungsstelle

1.3 Begriffe

Den Geltungsbereich der Zertifizierungsstelle definieren die Normen DIN EN ISO/IEC 17065 und DIN EN ISO/IEC 17067 Begriffe, welche u. a. detailliert in Kapitel 3 des Zertifizierungsstellenhandbuchs VA_650_050 aufgeführt werden.

2 ANGABEN ZUM ZERTIFIZIERUNGSPROGRAMM

2.1 Anwendungsbereich

Dieses Dokument beschreibt den Prozessablauf und das Vorgehen für die **„Konformitätsbewertung im Bereich der Informationssicherheit/Cyber-Security“** durch die CERTIFER Zertifizierungsstelle und ist nur zur eigenen Verwendung bestimmt.

Das Zertifizierungsprogramm umfasst die Normen DIN EN IEC 62433-4-1 und DIN EN IEC 62433-4-2.

Somit gilt das Zertifizierungsprogramm zum Nachweis der Anforderungserfüllung an den Lebenszyklus für eine sichere Produktentwicklung sowie zum Nachweis der technischen Sicherheitsanforderungen an Produkte industrieller Automatisierungssysteme.

Zusätzlich zum vorliegenden Zertifizierungsprogramm sind folgende Dokumente bei der Durchführung von Konformitätsprüfungen zu beachten:

- Qualitätsmanagementhandbuch von CERTIFER Deutschland
- Zertifizierungsstellenhandbuch für Prozesse VA_650_050
- Zertifizierungsvereinbarung für Prozesszertifizierung ZE_650_050

Die Zertifizierung erfolgt anhand der vom Antragsteller gelieferten Nachweisdokumente und Audits.

2.2 Programmeigner

Programmeigner für dieses Zertifizierungsprogramm ist die

CERTIFER Zertifizierungsstelle

Adam-Klein-Str. 26

D-90429 Nürnberg

2.3 Zugang zum Programm

Dieses Zertifizierungsprogramm steht auf der Homepage von CERTIFER, im Bereich der Zertifizierungsstelle von CERIFER Deutschland, zur Verfügung und gibt Informationen über die angewendeten Verfahren und zu beachtenden Regeln für die Akteure, die in den Zertifizierungsprozess eingebunden sind.

2.4 Anforderungen für die Anwendung des Programms

2.4.1 Produktanforderungen

Grundlage für die Prozesszertifizierung ist die Norm DIN EN/IEC 62443-4-1. Diese Norm enthält sämtliche Anforderungen, die ein Prozess für die Zertifizierung erfüllen muss.

Grundlage für die Produktzertifizierung ist die Norm DIN EN/IEC 62443-4-2. Diese Norm enthält sämtliche Anforderungen, die ein Produkt für die Zertifizierung erfüllen muss.

2.4.2 Anforderungen an den Kunden

Der Kunde muss ein implementiertes (Qualitäts-)Managementsystem oder sonstige entsprechende Tätigkeiten zur Prozesslenkung besitzen, um nachweisen zu können, dass alle Anforderungen auch in der Anwendung dauerhaft erfüllt werden.

Der Umgang mit Werbematerialien sowie alle weiteren Aufgaben und Pflichten des Kunden bzgl. des Zertifizierungsprozesses sind der Zertifizierungsvereinbarung (ZE_650_050) zu entnehmen.

Die Zertifizierungsvereinbarung ist zusätzlich zu den AGB fester Bestandteil des Vertrages, der für die Zertifizierung zwischen Kunde (Antragsteller) und Zertifizierungsstelle geschlossen wird.

2.4.3 Anforderungen an die Zertifizierungsstelle

Die Erfüllung der Anforderungen an die Zertifizierungsstelle hinsichtlich Unparteilichkeit, Diskriminierungsfreiheit, Vertraulichkeit, Kompetenz und Ressourcenplanung ist dem Zertifizierungsstellenhandbuch VA_650_050 zu entnehmen.

Die Vorgehensweise bzw. der Nachweis der Erfüllung der Anforderungen bei der Einbindung von internen sowie vertraglich gebundenen externen Personen ist ebenfalls dem Zertifizierungsstellenhandbuch VA_650_050 zu entnehmen.

2.5 Aufrechterhaltung und Verbesserung des Programms

Die Zertifizierungsstelle ergreift folgende Maßnahmen zur Aufrechterhaltung und Verbesserungen des Zertifizierungsprogrammes:

- Rückmeldungen von Kunden oder anderen Prozessteilnehmern zum Prozessablauf werden über das Formblatt FB_99 (zum Beispiel nach Zertifikatsausstellung) sowie durch regelmäßige Befragungen aufgenommen.
- Es finden in regelmäßigen Abständen interne Audits der Zertifizierungsstelle statt.

- Die Gültigkeit der Normen und normativer Dokumente wird in regelmäßigen Abständen und mindestens bei Beginn eines Zertifizierungsprozesses im Rahmen der Erstellung oder Prüfung des Nachweisplans überprüft.
- Die Ergebnisse aus Befragungen und internen Audits werden evaluiert und unter Beteiligung der Leitung der Zertifizierungsstelle oder durch die Leitung selbst werden entsprechende Maßnahmen beschlossen, die zeitnah in das Zertifizierungsprogramm eingearbeitet werden.

3 DURCHFÜHRUNG DER KONFORMITÄTSPRÜFUNG

3.1 Allgemeines

Die Durchführung der Konformitätsprüfung erfolgt nach dem Zertifizierungsprogramm, welches in diesem Dokument beschrieben wird.

Die Prüfgrundlage für den zu zertifizierenden Prozess richtet sich nach DIN EN IEC 62443-4-1.

Die Prüfgrundlage für das zu zertifizierende Produkt richtet sich nach DIN EN IEC 62443-4-2.

3.2 Antrag

Der Kunde (Antragsteller) stellt bei der Zertifizierungsstelle einen Antrag auf Zertifizierung bzw. Konformitätsbewertung nach den oben genannten Normen.

Das Antragsformular ZE_650_150 wird dem Kunden als Anlage zum Angebot zur Verfügung gestellt.

Folgende Angaben müssen in dem Antrag enthalten sein:

- Benennung des Prozesses und weitere wichtige Informationen diesbezüglich,
- Benennung des Produktes und weitere wichtige Informationen diesbezüglich,
- Benennung des Kunden und weitere wichtige Informationen diesbezüglich,
- Art der Konformitätsbewertung,
- Regelwerke und Normen, nach denen der Prozess bzw. das Produkt zertifiziert werden soll,
- ausgegliederte Prozesse, falls relevant,
- weitere relevante Informationen bzgl. des Zertifizierungsprozesses.

Die für die Bewertung der Erfüllung der Anforderungen benötigten Nachweisdokumente werden vom Antragsteller in einem Nachweisplan erfasst und zur Verfügung gestellt (siehe hierzu auch die Zertifizierungsvereinbarung ZE_650_050).

Der Antragsteller ist dafür verantwortlich, den Bewertungsstandard verbunden mit den spezifischen Sicherheitsanforderungen zu identifizieren und zu benennen, die im Rahmen der Zertifizierung zu bewerten sind. Der Antragsteller hat die Anforderungen, die von der Bewertung ausgenommen werden sollen, explizit auszuweisen.

3.3 Antragsbewertung

Die Zertifizierungsstelle muss die Angaben, die in der Anfrage enthalten sind, bewerten, um sicherzustellen, dass:

- die Informationen über den Kunden und den Prozess ausreichend für die Durchführung des Zertifizierungsprozesses sind;
- alle bekannten Differenzen im Verständnis zwischen der Zertifizierungsstelle und dem Kunden geklärt werden, einschließlich der Vereinbarung bezüglich der Normen oder der normativen Dokumente;
- der Geltungsbereich der angestrebten Zertifizierung festgelegt ist;
- die Mittel zur Durchführung aller Evaluierungstätigkeiten verfügbar sind (siehe FB_99 ausgestellt bei der Angebotserstellung);
- die Zertifizierungsstelle über die Kompetenz und die Fähigkeit verfügt, die Zertifizierungstätigkeiten durchzuführen (siehe FB_99 ausgestellt bei der Angebotserstellung);
- ein Antrag auf Produktzertifizierung nach DIN EN IEC 62433-4-2 vorliegt, zusätzlich ist zu prüfen, ob ein Nachweis über die Einhaltung der Anforderungen an einen sicheren Produktentwicklungszyklus des zu zertifizierenden Produktes nach DIN EN IEC 62443-4-1 vorliegt.

Liegt die Konformitätsbewertung des Prozesses im Tätigkeits- und Zuständigkeitsfeld der Zertifizierungsstelle, kann ein Angebot erstellt werden.

Die Beauftragung wird erst angenommen, wenn auch alle anderen Anforderungen gemäß DIN EN ISO/IEC 17065 erfüllt sind.

Die Zertifizierungsstelle führt schriftliche Aufzeichnungen darüber, ob Zertifizierungen durchgeführt oder abgelehnt werden; die Entscheidung ist zu begründen. Wenn sich die Zertifizierung auf eine bereits bestehende Zertifizierung beruft, muss auf diese in den Aufzeichnungen Bezug genommen werden.

Sollte ein Zertifizierungsverfahren einen Prozess, ein normatives Dokument oder ein Zertifizierungsprogramm beinhalten, mit dem die Zertifizierungsstelle bislang keine Erfahrung hat, wird fallweise von der Zertifizierungsstellenleitung entschieden, wie die weitere Vorgehensweise für dieses Projekt ist.

3.4 Evaluierung und Probenahme

Die Zertifizierungsstelle erstellt und führt einen Plan für die Zertifizierungstätigkeiten, in dem auch die Evaluierungstätigkeiten enthalten sind. Die Zertifizierungsstelle stellt den Inspektoren alle Informationen und Dokumentationen, die für die Durchführung der Evaluierungstätigkeiten notwendig sind, zur Verfügung. Die Zertifizierungsstelle führt die Evaluierungen entweder selbst durch oder bedient sich bereits vorliegender Inspektionsberichte einer Inspektionsstelle.

Die Zertifizierungsstelle behält sich vor, unter der Voraussetzung der Einhaltung der DIN EN ISO/IEC 17065:2012, Kap. 7.4.5, Evaluierungen, die von Kunden oder Laboren vor der Antragsstellung auf Zertifizierung durchgeführt wurden, anzuerkennen. Gleiches gilt für Inspektionsberichte, die von Kunden oder Inspektionsstellen vor der Antragstellung auf Zertifizierung eingereicht wurden.

Die Evaluierungstätigkeiten werden durch einen Lead Inspektor der Zertifizierungsstelle koordiniert. Die Evaluierungstätigkeiten werden von den Inspektoren durchgeführt, und das Ergebnis wird in Inspektionsberichten festgehalten.

Die im Rahmen der Evaluierung durchgeführten Inspektionen richten sich nach der in Verfahrensanweisung VA_750_015 – Einzelnorm beschriebenen Vorgehensweisen der CERTIFER Inspektionsstelle.

3.5 Bewertung

Die Ergebnisse der Evaluierung werden von der Zertifizierungsstelle geprüft und bewertet. Die Bewertung wird stets anhand einer Checkliste von einem Bewerter (Technischer Reviewer) durchgeführt, der nicht in den Evaluierungsprozess einbezogen war.

Empfehlungen für eine Zertifizierungsentscheidung werden ebenfalls in der Checkliste dokumentiert, sofern die Bewertung und Zertifizierungsentscheidung nicht gleichzeitig durch dieselbe Person erfolgen.

Eine abgeschlossene Bewertung muss nicht zwangsläufig ein positives Ergebnis zur Folge haben. Werden nicht alle Anforderungen durch den Kunden nachgewiesen, wird keine Empfehlung zur Ausstellung eines Zertifikats gegeben.

Inhalt der Bewertung nach DIN EN IEC 62443-4-1:

Die Konformitätsbewertung muss eine Aussage zur Normenkonformität des Produktentwicklungszyklus für die im Zertifizierungsantrag genannte(n) Komponente(n) nach den Ansätzen 1-8 sowie zum Reifegrad der Produktentwicklungsorganisation treffen, s.a. Kap 7.2 VA_ 750_015. Die Aussage teilt sich wie untenstehend auf:

1. Aussage zur Normenkonformität der im Antrag genannten Ansätze des Produktentwicklungszyklus.
2. Aussage zum Reifegrad der Produktentwicklungsorganisation für die im Antrag genannten Ansätze.

Inhalt der Bewertung nach DIN EN IEC 62443-4-2:

Die Konformitätsbewertung muss eine Aussage über die Einhaltung der technischen Anforderungen nach Bewertungsnorm für die erreichbaren Security Level 1 – 4 treffen. Zu bewerten sind für die jeweiligen SL-C 1 bis SL-C 4 die damit verbundenen Anforderungen gemäß Kapitel 5 — 15 der Bewertungsnorm unter Berücksichtigung der Gerätekategorien. Ausgleichsmaßnahmen gemäß Kapitel 4 sind ebenfalls zu betrachten. Für die jeweiligen Anforderungen ist ein Bewertungsergebnis bzw. „Nicht zutreffend“ auszuweisen, falls der Antragsteller die Anforderung aus dem Zertifizierungsumfang explizit ausgeschlossen hat.

3.6 Zertifizierungsentscheidung

Für die Zertifizierungsentscheidung ist allein die Zertifizierungsstelle verantwortlich und behält das alleinige Recht darüber. Die Person, die die Zertifizierungsentscheidung trifft, darf nicht am Evaluierungsprozess beteiligt gewesen sein.

Die Entscheidung über die Zertifizierung erfolgt auf Basis des Antrags auf Zertifizierung, der Ergebnisse aus der Evaluierung und Bewertung einschließlich der Empfehlung zur Zertifizierungsentscheidung und wird in einer Checkliste dokumentiert.

Nach Prüfung der Unterlagen auf Vollständigkeit, Plausibilität und Erfüllung aller Zertifizierungsanforderungen entscheidet der Entscheider über die Zertifizierung und veranlasst ggf. die Ausstellung des Zertifikates.

Die Zertifizierungsentscheidung wird dem Kunden schriftlich mitgeteilt. Wird die Zertifizierung ausgesprochen, erhält der Kunde das Zertifikat. Kann die Zertifizierung nicht erteilt werden, wird dies unter Benennung der Gründe dem Kunden ebenfalls schriftlich mitgeteilt.

3.7 Zertifizierungsdokumentation

Die Zertifizierungsstelle stellt dem Kunden eine formelle Zertifizierungsdokumentation in Form eines Zertifikates zur Verfügung, das mindestens folgende Elemente enthält:

- Name und Anschrift der Zertifizierungsstelle
- Datum der Zertifizierung
- Zertifikatsnummer
- Name und Anschrift des Kunden

- Geltungsbereich der Zertifizierung (Rollen, Objektklassen, Produkte oder Produktgruppen)[1]
- Ergebnis der Bewertung (Ansätze, Reifegrad, Erfüllung der technischen Anforderungen)
- Verweis auf den zugrundeliegenden Anhang
- Einsatzbedingungen und -beschränkungen
- Zeitraum oder Ablaufdatum der Zertifizierung
- Signatur und Unterschrift der Zertifizierungsstelle

Das Zertifikat wird nur ausgestellt, wenn

1. die Zertifizierungsvereinbarung akzeptiert wurde,
2. alle Zertifizierungsanforderungen erfüllt sind.

Der Umgang und die Nutzung von Zertifikaten sind der Zertifizierungsvereinbarung ZE_650_050 zu entnehmen.

3.8 Verzeichnis zertifizierter Prozesse

Alle zertifizierten Prozesse werden unter Nennung des Prozesses/Produkts und der Standorte des Kunden und des angewandten Regelwerkes, nach denen die Konformität zertifiziert wurde, in FB_82 aufgeführt. Außerdem wird der Zeitpunkt des Ablaufs des Zertifikates sowie sonstige relevante Daten mit aufgenommen.

Auf Anfrage können Ausschnitte des Verzeichnisses durch die Zertifizierungsstellenleitung veröffentlicht werden.

3.9 Überwachung

Die regelmäßige Überwachung des Prozesses wird in dreijährigen Intervallen festgelegt und schließt die Überwachung ein, um die weitere Gültigkeit des Nachweises der Anforderungen sicherzustellen (siehe DIN EN ISO/IEC 17065, Kap. 7.9.4.).

Um die Konformität zur Bewertungsnorm innerhalb des Überwachungsintervalls zu gewährleisten, hat der Antragsteller eine jährliche Konformitätserklärung ab Datum der Zertifikatserteilung vorzulegen.

---

[1] **Siehe 71 SD 2 09 | Revision 1.0 | 05.03.2018 – Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/ Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443**

3.10 Umgang mit Nichtkonformitäten, Änderungen, Zurückziehung der Zertifizierung

Neue aufsichtsrechtliche Erkenntnisse zu einem zertifizierten Prozess können zu einer Änderung der Zertifizierung führen. Wenn Gefahr im Verzug ist, erlischt das Zertifikat automatisch und unmittelbar. Sind entsprechende Maßnahmen zur Beseitigung der Mängel getroffen worden, kann ein neuer Zertifizierungsprozess (evtl. auf Basis der alten Zertifizierung) angestrebt werden.

Bei Änderungen im Zertifizierungsprogramm oder Zertifizierungsprozess werden von der Zertifizierungsstellenleitung geeignete Maßnahmen ergriffen und alle Prozessbeteiligten, die davon betroffen sind, informiert.

Das gleiche Verfahren findet statt, wenn z. B. die Zertifizierungsvereinbarung missachtet wird oder sich im Nachhinein herausstellt, dass fehlerhafte oder falsche Nachweisdokumente bei der Zertifizierung vorlagen, oder wenn fehlerhafte oder falsche prozessrelevante Informationen geliefert wurden.

Weiteres zum Thema Änderungen und Zurückziehung von Zertifikaten ist der Zertifizierungsvereinbarung ZE_650_050 zu entnehmen.

3.11 Aufzeichnungen

Der Umgang mit und die Aufbewahrung von Dokumentationen und Aufzeichnungen ist im Zertifizierungsstellenhandbuch VA_650_050 beschrieben.

3.12 Beschwerden und Einsprüche

Für Beschwerden gilt der im QM-Handbuch sowie der im Zertifizierungsstellenhandbuch VA_650_050 beschriebene Prozess. Auf Anfrage werden Informationen zum Umgang mit Beschwerden und Einsprüchen zur Verfügung gestellt.