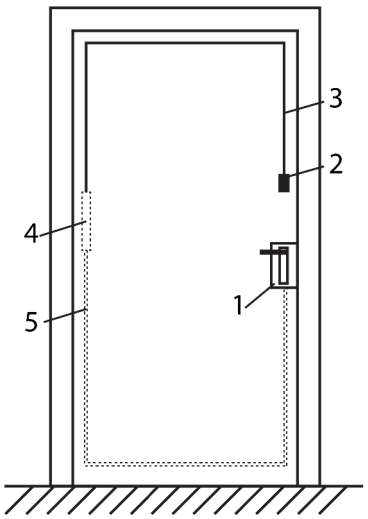
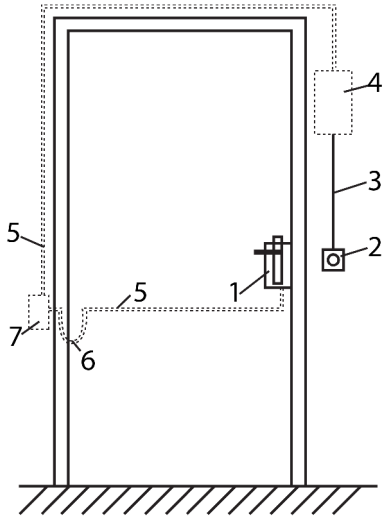


a) Tür mit Steuereinheit im Türblatt



b) Tür mit getrennter Steuereinheit

Legende

1 Mechatronikschloss
2 Eingabeeinheit für Berechtigungsnachweis
3 Kabel mit verschlüsseltem Signal zur Steuereinheit
4 Steuereinheit
5 Kabel zur abschließbaren Vorrichtung, RC 5 bis RC 6 überwachte Verbindung
6 Kabelzugangspunkt für Kabel
7 Anschlussdose

Die Komponenten Nr. 4 bis 7 müssen auf der Nichtangriffsseite eingebaut werden.

Bild E.2

Diese Komponenten dürfen bei manuellem Angriff nach prEN 1630:2019 in der entsprechenden Widerstandsklasse nicht erreichbar sein, damit eine Manipulation, z. B. Abisolieren von Drähten und Befestigung eines Anschlusses, nicht möglich ist.

E.5.5 Beschläge

Die Beschlagteile müssen über ein bewährtes Änderungsprotokoll für mehr als 1 000 autorisierte Zugangsversuche in Klasse 2 und 3verfügen und mehr als 1 000 insgesamt für autorisierte und unberechtigte Zugangsversuche.

E.6 Prüfverfahren - Abläufe

E.6.1 Allgemeines

Dieser Anhang erfordert keine speziellen Prüfungen für das elektronische Sicherheitssystem. Prüfungen müssen vom Hersteller oder einem Dritten erfolgen, um besondere Prüfergebnisse aufzuzeigen und den Hersteller in die Lage zu versetzen, eine bestimmte Herstellererklärung auszustellen.

Die Entscheidung, welche Anforderungen und Prüfverfahren für die technische Ausführung relevant sind, obliegt dem Prüfer gemeinsam mit dem Antragsteller.

Da ein elektronisches Sicherheitssystem aus vielen verschiedenen Berechtigungsnachweisen und Beschlagteilen bestehen kann, muss der Hersteller eindeutig angeben, für welche Klasse das elektronische Sicherheitssystem geeignet ist.

E.6.2 Berechtigungsnachweisprüfung ICC

E.6.2.1 Allgemeines

Die ICC-Berechtigungsnachweise müssen durch eine schriftliche Herstellererklärung und/oder Prüfberichte bzw. technische Spezifikationen von Dritten überprüft werden.

E.6.2.2 ICC - Codevarianten/maximale Anzahl der Autorisierungscodes

Die Codevarianten und maximale Anzahl der Autorisierungscodes müssen E.5.3.2.1 entsprechen.

Der Hersteller muss Dokumente oder mathematische Gleichungen vorlegen, die den Werten in Tabelle E.2 entsprechen.

E.6.2.3 ICC - Datenverschlüsselungsstandard

Der Datenverschlüsselungsstandard muss E.5.3.2.2 entsprechen.

Die Konformität wird durch eine Herstellererklärung überprüft, welche Verschlüsselungsverfahren angewendet werden.

E.6.2.4 ICC - Länge der Verschlüsselung

Die Länge der Verschlüsselung muss E.5.3.2.3 entsprechen.

Die Konformität wird durch eine Herstellererklärung oder andere relevante Dokumente überprüft, die die Werte in Tabelle E.2 bestätigen.

E.6.2.5 ICC - Kopierschutz

Die Länge der Verschlüsselung muss E.5.3.2.4 entsprechen.

Die Konformität wird durch eine Herstellererklärung überprüft.

E.6.3 Berechtigungsnachweisprüfung PIN-Code

E.6.3.1 Allgemeines

PIN-Codes sind ebenfalls eine Art Berechtigungsnachweis. Die Einhaltung wird in den Abschnitten E.5.3.3.1 bis E.5.3.3.2 überprüft.

E.6.3.2 PIN-Code - Codevarianten/maximale Anzahl der Autorisierungscodes

Die Codevarianten und maximale Anzahl der Autorisierungscodes müssen E.5.3.3.1 entsprechen.

Der Hersteller muss Dokumente oder mathematische Gleichungen vorlegen, die den Werten in Tabelle E.2 entsprechen.

E.6.3.3 PIN-Code - Totzeit nach fehlgeschlagenem Versuch

Die Totzeit nach fehlgeschlagenem Versuch muss E.5.3.3.2 entsprechen.

Die Konformität wird durch eine Herstellererklärung überprüft.

Verschlüsselte Tastaturen sollten auf alternative Verschlüsselung durch den Hersteller überprüft werden.

E.6.3.4 PIN-Code – Geschützter Sichtbarkeitsbereich

Der geschützte Sichtbarkeitsbereich muss E.5.3.3.3 entsprechen.

Die Konformität wird durch eine Bewertung der Gestaltung überprüft.

E.6.4 Berechtigungsnachweisprüfung – Zugangskarten

E.6.4.1 Allgemeines

Zugangskarten, z. B. Karten mit Magnetstreifen, müssen E.5.3.4.1 bis E.5.3.4.2 entsprechen.

Zugangskarten sind in den Klassen 4, 5 und 6 nicht zulässig.

E.6.4.2 Zugangskarten – Codevarianten/maximale Anzahl der Autorisierungscodes

Die Codevarianten und die maximale Anzahl der Autorisierungscodes müssen E.5.3.4.1 entsprechen.

Der Hersteller muss Dokumente oder mathematische Gleichungen vorlegen, die den Werten in Tabelle E.2 entsprechen.

E.6.4.3 Zugangskarten - Kopierschutz

Die Länge der Verschlüsselung muss E.5.3.4.2 entsprechen.

Die Konformität wird durch eine Herstellererklärung überprüft.

E.6.4.4 Zugangskarten - Totzeit nach fehlgeschlagenem Versuch

Die Totzeit nach fehlgeschlagenem Versuch muss E.5.3.4.3 entsprechen.

Die Konformität wird durch eine Herstellererklärung überprüft.

E.6.5 Berechtigungsnachweisprüfung – Biometrie

E.6.5.1 Allgemeines

Auf Biometrie basierte Berechtigungsnachweise müssen E.5.3.5.1 bis E.5.3.5.2 entsprechen.

ANMERKUNG Die Prüfung zur Biometrie wird in verschiedenen ISO/IEC-Normen aufgezeigt. Die Anforderungen in diesem Anhang sind die Anforderungen an die Einbruchhemmung.

E.6.5.2 Biometrie – Falschakzeptanzrate

Die Falschakzeptanzrate muss den Vorgaben in E.5.3.5.1 entsprechen. Die Berechnung zur Überprüfung der Konformität muss vom Hersteller zur Verfügung gestellt werden.

Die Konformität wird durch eine Herstellererklärung überprüft.

E.6.5.3 Biometrie – Lebenderkennung

Die Lebenderkennung muss den Vorgaben in E.5.3.5.2 entsprechen. Die Konformität wird durch eine Herstellererklärung und eine mögliche stichprobenartige Prüfung durch den Prüfer überprüft.

E.6.6 Berechtigungsnachweisprüfung – Smart Device

E.6.6.1 Allgemeines

Smart Devices müssen die Vorgaben in E.5.3.6.1 bis E.5.3.6.15 erfüllen.

E.6.6.2 Smart Device – Firewall

Nach E.5.3.6.1 wird überprüft, ob der Hersteller in den Betriebsunterlagen darauf hinweist, dass für einen sicheren Betrieb der Anwendung eine Firewall auf dem Smart Device oder dem Master betrieben werden muss, und geeignete Maßnahmen für die automatische und regelmäßige Aktualisierung der Firewall-Software empfiehlt.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Betrieb einer Firewall auf dem Smart Device oder dem Master zur automatischen und regelmäßigen Aktualisierung enthalten.

Es wird überprüft, ob der Master über ein öffentliches Netzwerk erreichbar ist. Ist dies der Fall, wird überprüft, ob der Hersteller in den Betriebsunterlagen angibt, dass eine Anwendungs-Firewall für den sicheren Betrieb der Anwendung auf dem Master betrieben werden muss, und geeignete Maßnahmen für die automatische und regelmäßige Aktualisierung der Firewall-Software empfiehlt.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Betrieb der Anwendungs-Firewall auf dem Master und automatische Aktualisierungsmaßnahmen enthalten.

E.6.6.3 Smart Device – Virenschutz

Es wird überprüft, ob der Hersteller in den Betriebsunterlagen nach E.5.3.6.2 angibt, dass für einen sicheren Betrieb der Anwendung ein aktuelles Schutzprogramm gegen Schadsoftware auf dem Smart Device, dem Master und anderen Servern betrieben werden muss, und ob eine regelmäßige Überprüfung und automatische Aktualisierung der Signaturdatenbank empfohlen wird.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Einsatz eines Schutzprogramms gegen Schadsoftware auf dem Smart Device, dem Master und anderen Servern enthalten und eine regelmäßige Überprüfung und automatische Aktualisierung der Signaturdatenbank empfehlen.

Es wird überprüft, ob der Hersteller in den Betriebsunterlagen nach E.5.3.6.2 angibt, dass der Betreiber für einen sicheren Betrieb der Anwendung gewährleisten muss, dass im Falle einer Infektion durch Schadprogramme die Virenerkennung durch das Schutzprogramm dokumentiert und geeignete Maßnahmen ergriffen werden.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung enthalten, dass der Betreiber im Falle einer Infektion durch Schadprogramme gewährleisten muss, dass die Virenerkennung durch das Schutzprogramm dokumentiert und die Infektion durch geeignete Maßnahmen behoben wird.

E.6.6.4 Smart Device – Benutzerkennung

Es wird überprüft, ob das Starten der Anwendung die Eingabe einer Benutzerkennung nach E.5.3.6.3 oder die Authentifizierung durch ein anderes gleichwertiges Identifikationsmerkmal erfordert (zum Beispiel Fingerabdruck).

Es wird überprüft, ob ein entsprechendes Identifikationsmerkmal beim Starten der Anwendung angefordert wird.

Es wird überprüft, ob die Bedienungsanleitung für den Betreiber und/oder Benutzer der Anwendung eine Angabe über die Bedeutung der Auswahl einer sicheren Benutzerkennung und eines sicheren Sperrcodes enthält.

Es wird überprüft, ob das Betriebshandbuch eine entsprechende Anmerkung über die Bedeutung der Wahl einer sicheren Benutzerkennung und eines sicheren Sperrcodes enthält.

E.6.6.5 Smart Device – Aktualisierungsmanagement

Es wird überprüft, ob der Hersteller in den Betriebsunterlagen angibt, dass für den sicheren Betrieb die aktuelle Software-Version aller Programme, die für den ordnungsgemäßen Betrieb der Anwendung erforderlich sind, auf dem Smart Device, dem Master und jedem erforderlichen Server verwendet werden muss. Die Anwendung selbst und die jeweiligen Betriebssysteme der aufgeführten Beschlagteile müssen ebenfalls explizit genannt werden.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Einsatz der aktuellen Software-Version jeglicher für den sicheren Betrieb der Anwendung auf dem Smart Device, dem Master und möglicherweise erforderlichen Server enthalten sowie eine Angabe der aktuellen Betriebssystemversionen der aufgeführten Beschlagteile und der Anwendung selbst.

Es wird überprüft, ob die Anwendung bei jedem Start nach Aktualisierungen sucht (mindestens einmal pro Tag) und den Benutzer informiert, sobald eine Aktualisierung verfügbar ist.

Es wird überprüft, ob eine entsprechende Anmerkung den Betreiber im Falle einer Aktualisierung informiert oder ob diese Funktionalität anhand des Quellcodes rekonstruiert werden kann.

Es wird überprüft, ob die Anwendung nicht länger gestartet werden kann, was seit der Kenntnis der Anwendung über eine vorhandene Aktualisierung nach E.5.3.6.4, Tabelle E.3 Wartezeit überschritten wurde.

Es wird überprüft, dass die Anwendung nach der festgelegten Wartezeit nicht gestartet oder diese Funktionalität mit dem Quellcode rekonstruiert werden kann.

E.6.6.6 Smart Device – Zeitkonstante

Es wird überprüft, ob der nächste Eingabeversuch nach Eingabe einer falschen Benutzerkennung um eine Zeitkonstante nach E.5.3.6.5 verzögert wird.

Es wird überprüft, ob der nächste Eingabeversuch der Benutzerkennung um die Zeit (t) nach E.5.3.6.5 nach der vorherigen Falscheingabe verzögert ist.

E.6.6.7 Smart Device – Länge der Benutzerkennung

Es wird überprüft, ob das Benutzerhandbuch für den Benutzer der Anwendung eine Angabe über die Bedeutung der Auswahl einer sicheren Benutzerkennung und eines sicheren Sperrcodes enthält.

Es wird überprüft, ob die Bedienungsanleitung eine Anmerkung über die Bedeutung der Auswahl einer sicheren Benutzerkennung und eines sicheren Sperrcodes nach Tabelle E.2 enthält.

In der Bedienungsanleitung muss der Hersteller den Betreiber oder Benutzer über die spezielle Passwortvergabe des Serverzugriffs informieren.

E.6.6.8 Smart Device – Vollständige Sperrung

Es wird überprüft, ob nach zehnmaliger falscher Eingabe der Benutzerkennung nach E.5.3.6.7 der Start der Anwendung vollständig gesperrt ist.

Es wird überprüft, ob nach E.5.3.6.7 nach zehnmaligem Fehldruck der Benutzerkennung der Start der Anwendung blockiert wird oder diese vollständige Sperrung in der Bedienerinformation dokumentiert ist.

Es wird überprüft, ob die vollständige Sperre durch Eingabe eines PUK deaktiviert werden kann.

Es wird überprüft, ob nach E.5.3.6.7 nach der Eingabe des korrekten PUK die vollständige Sperrung deaktiviert wird oder ob dies in der Bedienerinformation dokumentiert ist.

Es wird überprüft, ob nach drei falschen Eingaben des PUK alle anwendungsbezogenen Informationen gelöscht werden.

Es wird überprüft, ob nach E.5.3.6.7 die Bedienerinformationen einen entsprechenden Hinweis auf eine vollständige Löschung der Daten nach drei falschen Eingaben des PUK enthalten.

E.6.6.9 Smart Device – Verschleierung

Es wird überprüft, ob der Quellcode der Anwendung grundsätzlich verschleiert wird.

Es wird überprüft, ob nach E.5.3.6.8 der Hersteller in seiner Herstellererklärung die Art der Verschleierung angibt und bestätigt. Für die Klassen 3 und 4 ist eine Standardverschleierung ausreichend, für die Klassen 5 und 6 muss eine höhere Verschleierung implementiert und vom Hersteller der Anwendung bestätigt werden.

E.6.6.10 Smart Device – Vertraulichkeit auf dem Übertragungsweg

E.6.6.10.1 Allgemeines

Es wird überprüft, ob der Hersteller bei der Übertragung über Datennetze geeignete Verfahren zur Datensicherung anwendet (z. B. https: //) und die Anforderungen in E.5.3.6.9 erfüllt und dass nur gültige Zertifikate verwendet und akzeptiert werden, wenn Daten übertragen werden.

Es wird überprüft, ob in der Herstellererklärung die Verfahren und Algorithmen aufgeführt sind, die zum Speichern und Sichern der Daten in der Herstellerdokumentation verwendet werden, und nur die Verwendung gültiger Zertifikate bei der Datenübertragung in der Herstellererklärung bestätigt. Falls erforderlich, kann dies auch mit mehreren ungültigen Zertifikaten bestätigt werden.

E.6.6.10.2 Smart Device – Stufe der Online-Kommunikation

Es wird überprüft, ob die Kommunikation zwischen Smart Device, Master und ggf. weiteren Servern mit einer Schlüssellänge nach Tabelle E.4 verschlüsselt ist.

Es wird überprüft, ob der Hersteller in seiner Herstellererklärung die Schlüssellängen dokumentiert hat.

E.6.6.10.3 Smart Device – Stufe der Offline-Kommunikation

Es wird überprüft, ob die Kommunikation zwischen Smart Device, Master und ggf. weiteren Servern mit einer Schlüssellänge der entsprechenden Klassen nach Tabelle E.5 verschlüsselt ist.

Es wird überprüft, ob der Hersteller in seiner Herstellererklärung die Schlüssellänge dokumentiert hat

E.6.6.11 Smart Device – Einzeltastatur

Es wird überprüft, ob in der Anwendung nach E.5.3.6.10 bei fehlendem Sperrcode auf dem Smart Device eine herstellerspezifische Einzeltastatur wirksam implementiert ist.

Es wird überprüft, ob anhand des Quellcodes erkennbar ist, dass eine proprietäre Tastatur effektiv implementiert und im Benutzerhandbuch angemessen beschrieben wird.

E.6.6.12 Smart Device – Verschlüsselte Einzeltastatur

Es wird überprüft, ob eine proprietäre Einzeltastatur nach E.5.3.6.11 in der Anwendung effektiv implementiert ist, wenn der Sperrcode auf dem Smart Device fehlt. Zusätzlich sollte die Anordnung der Eingabetasten bei jedem Aufruf verschlüsselt werden (verschlüsselte Funktion).

Es wird überprüft, ob im Quellcode angezeigt wird, dass eine proprietäre Tastaturfunktion effektiv implementiert ist, und die Tastatur über eine Verschlüsselungsfunktion verfügt.

E.6.6.13 Smart Device – Verschlüsselt gespeichert im Gerät

Es wird überprüft, ob Daten in besonders gesicherten Speicherbereichen gespeichert oder auf dem Smart Device verschlüsselt sind und ob das verwendete Verschlüsselungsverfahren in der Dokumentation des Herstellers aufgelistet ist.

Es wird überprüft, ob die Herstellerdokumentation im Detail das Verschlüsselungsverfahren und den Ort der gespeicherten und gesicherten Daten beschreibt.

E.6.6.14 Smart Device – Integritätsschutz

Es wird überprüft, ob Prüfsummen der übertragenen Daten generiert und von der Anwendung überprüft werden.

Es wird überprüft, ob Veränderungen an mehreren Prüfsummen der zu verarbeitenden Daten von der Anwendung abgelehnt werden. Der Hersteller muss dies schriftlich in einem getrennten Prüfszenario dokumentieren.

E.6.6.15 Smart Device – Secure Element

Es wird überprüft, ob das Secure Element nach E.5.3.6.14 verwendet wird und die Daten auf dem Secure Element gespeichert sind und ob der Hersteller den Benutzer in den Betriebsunterlagen über einen zusätzlichen Schutz durch ein Secure Element informiert und die Verwendung eines geeigneten Smart Devices empfiehlt.

Es wird überprüft, ob anhand des Quellcodes oder in der Herstellererklärung die Logik des Dateisystems des Smart Devices rekonstruiert werden kann, die Daten der Anwendung in einem Secure Element gespeichert werden und eine entsprechende Anmerkung in den Betriebsunterlagen vorhanden ist.

E.6.6.16 Smart Device – Verhütung und Aufdeckung

Es wird überprüft, ob nach E.5.3.6.15 in den Betriebsunterlagen eine Anmerkung enthalten ist, dass der Betreiber sicherstellen muss, dass sichere Maßnahmen zum Schutz vor Exploits getroffen werden und dass der Benutzer, sobald die entsprechenden Exploits bekannt werden, unverzüglich informiert wird, ob ein korrigierendes Software-Update verfügbar ist. Gibt es eine Aktualisierung, muss er sie installieren.

Es wird überprüft, ob in den Betriebsunterlagen und der Benutzerdokumentation eine entsprechende Anmerkung vorhanden ist.

Es wird überprüft, ob die Anwendung nach E.5.3.6.15 zuverlässig erkennt, dass ein Betreiber Administratorberechtigungen auf dem Smart Device erhalten hat. Ist dies der Fall, muss die weitere Ausführung der Anwendung sofort gestoppt werden.

Es wird überprüft, ob die Ausführung der Anwendung mit Administratorrechten auf dem Smart Device die Anwendung sofort abbricht und sie vor einem Neustart schützt.

E.6.7 WLAN – Verschlüsselung

Es wird überprüft, ob in der Benutzerdokumentation nach E.5.3.6.16 der Schutz des WLAN im Detail angegeben ist und die Benutzerdokumentation die Verschlüsselung des Netzwerks für den sicheren Betrieb übernimmt.

Es wird überprüft, ob die Anforderungen in der Benutzerdokumentation explizit angegeben werden.

E.6.8 WLAN – Firewall

Es wird überprüft, ob der Hersteller nach E.5.3.6.17 in den Betriebsunterlagen darauf hinweist, dass für einen sicheren Betrieb des über WLAN verbundenen elektronischen Sicherheitssystems eine Firewall am Master betrieben werden muss, und geeignete Maßnahmen zur automatischen und regelmäßigen Aktualisierung der Firewall-Software empfiehlt.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Betrieb einer Firewall auf dem Master und Maßnahmen zur automatischen und regelmäßigen Aktualisierung enthalten.

Es wird überprüft, ob der Master über ein öffentliches Netzwerk erreichbar ist. Ist dies der Fall, wird überprüft, ob der Hersteller in den Betriebsunterlagen mitteilt, dass Maßnahmen zum sicheren Betrieb des elektronischen Sicherheitssystems empfohlen werden und eine regelmäßige Aktualisierung der Firewall-Software von wesentlicher Bedeutung ist.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Betrieb der Firewall und eine automatische Aktualisierung der Firewall enthalten.

E.6.9 WLAN –Aktualisierungsmanagement

E.6.9.1 Allgemeines

Es wird überprüft, ob der Hersteller nach E.5.3.6.18 in den Betriebsunterlagen darauf hinweisen muss, dass für den sicheren Betrieb nur die aktuelle Firmware- und Software-Version verwendet werden muss, die auf allen Beschlagteilen des elektronischen Sicherheitssystems installiert ist. Die Anwendung selbst und die jeweiligen Betriebssysteme der Beschlagteile müssen ebenfalls explizit genannt werden.

Es wird überprüft, ob die Betriebsunterlagen eine entsprechende Anmerkung über den Einsatz der aktuellen Firmware- und Software-Version aller für den sicheren Betrieb der Anwendung erforderlichen Beschlagteile sowie einen Hinweis zur Verwendung der aktuellen Betriebssystemversionen der Beschlagteile und die Anwendung selbst enthalten.

E.6.9.2 Verkabelung und Stromausfall

Der Hersteller muss in seinen Einbauanweisungen in Übereinstimmung mit E.5.4.2 für drahtgebundene elektronische Sicherheitssysteme angeben, wie sicher die Verkabelung bereitgestellt werden muss. Die Anschlusspläne und Verkabelungsarten sind in der Herstellerdokumentation zu beschreiben.

Es wird überprüft, ob die Herstellerdokumentation und Einbauanweisungen eine entsprechende Anmerkung bieten.

E.6.9.3 Beschläge

Die Beschlagteile nach E.5.35 müssen über ein bewährtes Änderungsprotokoll für mehr als 1 000 Zugangsversuche verfügen. Diese Zugangsversuche werden normalerweise in der elektronischen Sicherheitssystem-Hardware gespeichert und können ausgelesen werden.

Es wird überprüft, ob die Herstellerdokumentation und die Betriebsunterlagen angeben, wie und auf welche Art die Zugangsversuche ausgelesen werden können.

Literaturhinweise

[1] EN 13241, *Tore — Produktnorm, Leistungseigenschaften*

[2] EN ISO 6508-1, *Metallische Werkstoffe — Härteprüfung nach Rockwell — Teil 1: Prüfverfahren (ISO 6508-1)*