

DIN EN 1300



ICS 13.310

Ersatz für
DIN EN 1300:2004-09

**Wertbehältnisse –
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen;
Deutsche Fassung EN 1300:2004+A1:2011**

Secure storage units –

Classification for high security locks according to their resistance to unauthorized opening;
German version EN 1300:2004+A1:2011

Unités de stockage en lieux sûrs –

Classification des serrures haute sécurité en fonction de leur résistance à l'effraction;
Version allemande EN 1300:2004+A1:2011

Gesamtumfang 41 Seiten

Normenausschuss Eisen-, Blech- und Metallwaren (NAEBM) im DIN

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist 2011-10-01.

Nationales Vorwort

Dieses Dokument beinhaltet die Deutsche Fassung der von der Arbeitsgruppe 3 „Sicherheitsschlösser“ (Sekretariat: DIN, Deutschland) des Technischen Komitees 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ (Sekretariat: BSI, Vereinigtes Königreich) des Europäischen Komitees für Normung (CEN) ausgearbeiteten Norm EN 1300:2004+A1:2011.

Das zuständige nationale Gremium ist der Arbeitsausschuss 15 „Hochsicherheitsschlösser“ im Normenausschuss Eisen-, Blech- und Metallwaren (NAEBM) im DIN, Deutsches Institut für Normung e. V.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. Das DIN [und/oder die DKE] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die im Abschnitt 2 zitierten Europäischen Normen sind als DIN-EN- bzw. DIN-EN-ISO-Normen mit gleicher Normnummer veröffentlicht.

Änderungen

Gegenüber DIN EN 1300:2004-09 wurden folgende Änderungen vorgenommen:

- a) die normativen Verweisungen wurden aktualisiert bzw. ergänzt;
- b) der Begriff Einmalcode wurde aufgenommen und die Anforderungen im Abschnitt 5 entsprechend geändert;
- c) die Tabellen 2 und 3 wurden ersetzt;
- d) ein neuer Unterabschnitt 8.2.1.4 zur Prüfung der Festigkeit des Schlüssels wurde aufgenommen;
- e) die Prüfung des Verhaltens bei Stromausfall in 8.2.5.3 wurde ergänzt;
- f) zur Schockprüfung in 8.2.6.2 wurde die Möglichkeit einer zusätzlichen Prüfung mit Schocks von mehr als 50 g aufgenommen;
- g) mit 8.2.6.3 wurde eine Immersionsprüfung aufgenommen;
- h) der Anhang A wurde zu einem normativen Anhang erklärt und der Inhalt der Montageanleitung überarbeitet bzw. ergänzt, z. B. durch Angaben der verwendbaren Befestigungsschrauben, der Drehmomente und Schraubensicherungen;
- i) der Anhang D „Schlossmaße“ wurde neu aufgenommen.

Frühere Ausgaben

DIN EN 1300: 2004-09
DIN V ENV 1300: 1999-04

Deutsche Fassung

Wertbehältnisse —
Klassifizierung von Hochsicherheitsschlössern nach ihrem
Widerstandswert gegen unbefugtes Öffnen

Secure storage units —
Classification for high security locks according to their
resistance to unauthorized opening

Unités de stockage en lieux sûrs —
Classification des serrures haute sécurité en fonction de
leur résistance à l'effraction

Diese Europäische Norm wurde vom CEN am 24. März 2004 angenommen und schließt Änderung 1 ein, die am 14. April 2011 vom CEN angenommen wurde.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

Seite

Vorwort	3
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Begriffe	5
4 Klassifizierung	8
5 Anforderungen	8
6 Technische Dokumentation	14
7 Prüfmuster	15
8 Prüfverfahren	15
9 Prüfbericht	27
10 Kennzeichnung	27
Anhang A (normativ) ■ Montageanleitung	28
Anhang B (normativ) Bestimmung des Widerstandes gegen Manipulation aufgrund von konstruktiven Anforderungen	29
Anhang C (normativ) Herstellererklärung (nur für Schlüsselschlösser)	37
Anhang D (informativ) ■ Schlossmaße	38
Literaturhinweise	39

Vorwort

Dieses Dokument (EN 1300:2004+A1:2011) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat vom BSI gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Dezember 2011, und etwaige entgegenstehende nationale Normen müssen bis Dezember 2011 zurückgezogen werden.

Dieses Dokument schließt die Änderung 1 ein, die von CEN am 14.04.2011 angenommen worden ist.

Dieses Dokument ersetzt  EN 1300:2004 .

Anfang und Ende des eingefügten oder durch die Änderung geänderten Textes sind durch die Änderungsmarken   im Text kenntlich gemacht.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Diese Europäische Norm wurde von der Arbeitsgruppe 3 des CEN/TC 263 im Rahmen einer Normenreihe zur sicheren Aufbewahrung von Wertsachen und von Datenträgern erarbeitet. Weitere Normen dieser Reihe tragen folgende Titel und weitere Normen befinden sich noch in Vorbereitung:

EN 1047-1, *Wertbehältnisse — Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand — Teil 1: Datensicherungsschränke.*

EN 1047-2, *Wertbehältnisse — Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand — Teil 2: Datensicherungsräume und Datensicherungscontainer.*

EN 1143-1, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 1: Geldschränke, Tresorraumtüren und Tresorräume.*

EN 1143-2, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 2: Deposit-Systeme.*

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

1 Anwendungsbereich

Diese Europäische Norm legt die Anforderungen an Hochsicherheitsschlösser hinsichtlich ihrer Zuverlässigkeit, ihres Widerstandswertes gegen zerstörende Angriffe und gegen unbefugtes Öffnen sowie die Prüfverfahren fest. Sie bietet außerdem ein Schema zur Klassifizierung von Hochsicherheitsschlössern auf der Grundlage einer Bewertung ihres Widerstandswertes gegen zerstörende Angriffe und gegen unbefugtes Öffnen.

Sie gilt für mechanische und elektronische Hochsicherheitsschlösser. Die Schlösser können die folgenden Merkmale als Option enthalten, diese sind aber nicht zwingend erforderlich:

- 1) Berechtigungscode zur Verhinderung einer Codeänderung und/oder der Freigabe/Sperrung eines Parallelcodes,
- 2) Berechtigungscode zur Freigabe einer Zeitschlossfunktion,
- 3) Einbau von Bauteilen oder Funktionen einer Alarmanlage,
- 4) Funktionen zur Fernsteuerung und -überwachung,
- 5) Widerstand gegen Angriffe mit Säuren,
- 6) Widerstand gegen Angriffe mit Röntgenstrahlung,
- 7) Widerstand gegen Angriffe mit Sprengstoffen,
- 8) Zeitfunktionen.

2 Normative Verweisungen

[A1] Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen). **[A1]**

EN 1143-1, *Wertbehältnisse — Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl — Teil 1: Geldschränke, Tresorraumtüren und Tresorräume*

[A1] EN 50130-4:1995, *Alarmanlagen — Teil 4: Elektromagnetische Verträglichkeit — Produktfamiliennorm: Anforderungen an die Störfestigkeit von Anlageteilen für Brand- und Einbruchmeldeanlagen sowie Personen-Hilferufanlagen* **[A1]**

[A1] EN 60068-2-1:2007, *Umgebungseinflüsse — Teil 2-1: Prüfverfahren — Prüfung A: Kälte IEC 60068-2-1:2007* **[A1]**

[A1] EN 60068-2-2:2007, *Umgebungseinflüsse — Teil 2-2: Prüfverfahren — Prüfung B: Trockene Wärme (IEC 60068-2-2:2007)* **[A1]**

[A1] EN 60068-2-6, *Umgebungseinflüsse — Teil 2-6: Prüfverfahren — Prüfung Fc: Schwingen (sinusförmig) (IEC 60068-2-6:2007)* **[A1]**

[A1] EN 60068-2-17, *Umweltprüfungen — Teil 2: Prüfungen — Prüfung Q: Dichtheit (IEC 60068-2-17:19094)* **[A1]**

[A1] EN 61000-4-2, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-2: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2:2008)* **[A1]**

[A1] EN 61000-4-3:2006, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-3: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen die elektromagnetische Felder (IEC 61000-4-3:2006)* **[A1]**

[A1] EN 61000-4-4:2004, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-4: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst (IEC 61000-4-4:2004)* **[A1]**

EN 61000-4-5:2006, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-5: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5:2005)* ^{A1}

EN 61000-4-6:2009, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-6: Prüf- und Messverfahren — Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder (IEC 61000-4-6:2008)* ^{A1}

EN 61000-4-11:2004, *Elektromagnetische Verträglichkeit (EMV) — Teil 4-11: Prüf- und Messverfahren — Prüfung der Störfestigkeit gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen (IEC 61000-4-11:2004)* ^{A1}

EN ISO 6988 ^{A1}, *Metallische und andere anorganische Überzüge — Schwefeldioxid-Prüfung mit allgemeiner Feuchtigkeitskondensation (ISO 6988:1985)*

3 Begriffe

Für die Anwendung dieser Europäischen Norm gelten die folgenden Begriffe.

3.1

Hochsicherheitsschloss (HSS)

unabhängige Einheit, die gewöhnlich an Türen von Wertbehältnissen angebracht ist. In diese Einheit kann die Eingabe eines Codes erfolgen, der dann mit einem gespeicherten Code verglichen wird (Auswerteeinheit). Bei Übereinstimmung der Codes kann eine Blockiereinheit bewegt werden

3.2

Code

erforderliche Identifikationsinformation, die, wenn sie die richtige ist, es bei Eingabe in ein Hochsicherheitsschloss ermöglicht, den Sicherheitszustand des Schlosses zu ändern

3.2.1

Öffnungscod

Identifikationsinformation, die ein Entsperren des Hochsicherheitsschlosses gestattet

3.2.2

Berechtigungscod

Identifikationsinformation, die einen Zugang zur Auswerteeinheit gestattet. Der Berechtigungscod kann auch der Öffnungscod sein

3.2.3

Überfallcod

Parallelcod, der zusätzliche Funktionen aktiviert

3.2.4

Parallelcod

Öffnungscod, der identische Funktionen wie ein bereits existierender Öffnungscod aufweist, aber aus anderen Zeichen besteht

3.3

Codierarten

alle Mittel/Verfahren, durch die der Code gespeichert wird

3.3.1

materieller Cod

Code, der durch physikalische Merkmale oder andere Eigenschaften des Codeträgers bestimmt wird

3.3.2

mnemonischer Code

Code, der aus numerischen und/oder alphabetischen Informationen besteht und im Gedächtnis festgehalten wird

3.3.3

biometrischer Code

Code, der aus charakteristischen Merkmalen des Menschen besteht



3.3.4

Einmalcode

Code, welcher sich nach jeder Verwendung verändert und mit Hilfe eines Algorithmus erzeugt wird 

3.4

Eingabeeinheit

Teil eines HSS, über das Codes in die Auswerteeinheit eingegeben werden

3.5

Auswerteeinheit

Teil eines HSS, das auswertet, ob der eingegebene Code richtig ist und die Bewegung einer Sperreinheit freigibt oder sie verhindert

3.6

Sperreinheit

Tourstift (ggf. Tourstifte), der Teil eines HSS ist und der die Bewegung der Blockiereinheit freigibt oder sie verhindert

3.7

Codeträger

Gegenstand, dessen physische Form oder physikalische Eigenschaften den Berechtigungscode bestimmen, z. B. ein Schlüssel

3.8

mechanisches HSS

HSS, das nur durch mechanische Elemente gesichert wird

3.9

elektronisches HSS

HSS, das teilweise oder vollständig durch elektrische oder elektronische Elemente gesichert wird

3.10

Blockiereinheit

Teil eines HSS, das sich nach Eingabe des richtigen Öffnungscodes bewegt oder bewegt werden kann, um entweder eine Tür zu sichern oder die Bewegung eines Riegelwerks zu verhindern. Ein Beispiel für eine Blockiereinheit ist der Riegel eines mechanischen Schlosses

3.11

zerstörender Angriff

Angriff, der an einem HSS Schäden verursacht, die irreversibel sind und vor dem rechtmäßigen Benutzer nicht verborgen werden können

3.12

Zuverlässigkeit

Fähigkeit, nach einer großen Anzahl von Schließzyklen noch richtig zu funktionieren und die Sicherheitsanforderungen zu erfüllen

3.13

Manipulation

Angriffsverfahren, das darauf abzielt, die Blockierfunktion aufzuheben, ohne dabei Schäden zu verursachen, die für den Nutzer offensichtlich sind

ANMERKUNG Nach einer Manipulation kann ein HSS funktionsfähig bleiben, obwohl sein Sicherheitswert dauerhaft beeinträchtigt sein könnte.

3.14

ausspähen

Angriff, bei dem versucht wird, den richtigen Code zu ermitteln, ohne das HSS mit der Hand zu berühren, es mit einem Werkzeug in Kontakt zu bringen oder sonstige Instrumente zu benutzen

3.15

nutzbare Codes

Codes oder Codeträger, die vom Hersteller zugelassen sind und die den Anforderungen dieser Norm entsprechen. Bei mechanischen HSS ist im Allgemeinen die Anzahl der nutzbaren Codes weit geringer als die Gesamtzahl der Codes, auf die das HSS eingestellt werden kann

3.16

verworfen-Zustand

Zustand, bei dem sich die Codierungselemente nicht in der Anordnung befinden, die erforderlich ist, um das HSS ohne Eingabe des richtigen Codes oder passenden Codeträger zu entsperren

3.17

Schließsequenz

Handlungsablauf, der mit einer offenen Tür beginnt und der beendet ist, wenn die Tür geschlossen, verriegelt, gesperrt und gesichert ist

3.18

offene Tür

die Tür liegt nicht im Rahmen

3.19

geschlossene Tür

die Tür liegt im Rahmen, der/die Riegel können jetzt ausgefahren werden

3.20

verriegelte Tür

die Riegel sind ausgefahren

3.21

gesperrte Tür

das Riegelwerk kann nicht eingefahren werden, weil es vom Hochsicherheitsschloss blockiert wird

3.22

gesicherte Tür

die Tür ist geschlossen, verriegelt und mit einem Hochsicherheitsschloss, das sich im gesicherten Zustand befindet, gesperrt

3.23

HSS im gesicherten Zustand

die Blockiereinheit ist ausgefahren und kann nur nach Eingabe des/der Öffnungscodes wieder eingefahren werden

3.24

Normalzustand

das HSS befindet sich nach einer Prüfung im gesicherten Zustand und alle Schlossfunktionen können ausgeführt werden

3.25

Zustand der Funktionsfähigkeit

das HSS befindet sich nach einer Prüfung im gesicherten Zustand und kann mit dem (den) Öffnungscod(e)s entsperrt werden, es sind aber nicht alle Schlossfunktionen ausführbar

3.26

Sicherheit bei Ausfall

das HSS befindet sich nach einer Prüfung im gesicherten Zustand, aber nicht alle Schlossfunktionen sind funktionsfähig, es kann deshalb mit dem (den) Öffnungscod(e)s nicht mehr entsperrt werden

3.27

Widerstandseinheiten RU

RU: der Widerstandswert gegen einen zerstörenden Angriff bei Einsatz eines Werkzeugs mit dem Koeffizienten 1 und dem Basiswert 0 über einen Zeitraum von 1 Minute

3.28

Sperrzeit

Zeitverzögerung aufgrund der Überschreitung der zulässigen Zahl falscher Codeeingaben

4 Klassifizierung

Aufgrund der Sicherheitsanforderungen erfolgt bei Hochsicherheitsschlössern die Klassifizierung in die Schlossklassen A, B, C und D nach den Tabellen 1, 2 und 3. Allgemeine Anforderungen und Zuverlässigkeitsanforderungen (siehe 5.1, 5.2 und 5.3) müssen erfüllt sein.

ANMERKUNG Für Hochsicherheitsschlösser der Klasse A gelten die niedrigsten Anforderungen und für Hochsicherheitsschlösser der Klasse D die höchsten Anforderungen.

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Anforderungen an alle Klassen

5.1.1.1 Der (die) Öffnungscod(e)s müssen so lange als allein gültige Codes erhalten bleiben, bis sie absichtlich umgestellt werden. Die Bewertung erfolgt nach 8.1.2.  Übergelagerte oder undokumentierte Codes sind nicht zulässig. 

5.1.1.2 Werden bei HSS mnemonische Codes benutzt, müssen diese geändert werden können.

5.1.1.3 Es darf nicht möglich sein, dass durch zusätzliche vom Schlosshersteller eingebaute Vorrichtungen (z. B. Mikroschalter) Informationen über den Code gewonnen werden können. Die Bewertung erfolgt nach 8.1.2.

5.1.1.4 Eine Eingabeeinheit ist notwendiger Teil eines HSS. Mit einer Eingabeeinheit können mehrere HSS (Auswerteeinheit) bedient werden. Jedes HSS muss eine Auswerteeinheit besitzen, die den richtigen Code von der Eingabeeinheit verarbeitet. Jedes HSS muss auch eine Blockiereinheit enthalten oder die Bewegung einer Blockiereinheit steuern können. Wenn diese Einheit vor der ersten Nutzung aktiviert werden muss, ist in der Bedienungsanleitung des Schlosses darauf hinzuweisen.

5.1.1.5 Wird die Blockiereinheit nicht manuell betätigt, muss eine Vorrichtung vorhanden sein, die anzeigt, ob das HSS gesichert, verriegelt und verworfen ist.

5.1.1.6 Es darf nicht möglich sein, einen Öffnungscod(e) zu ändern, ohne einen Autorisierungscode einzugeben. Die Bewertung erfolgt nach 8.1.2.

5.1.2 HSS der Klasse D

5.1.2.1 Der Verschlusszustand des Schlosses, ob gesperrt oder entsperrt, muss offensichtlich sein.

5.1.2.2 Ein mechanisches Kombinationsschloss muss sich nach dem Sperren im Verworfen-Zustand befinden. Die Bewertung erfolgt nach 8.1.2.

5.1.2.3 Ein HSS der Klasse D muss eine Vorrichtung enthalten, die den Verworfen-Zustand anzeigt.

5.1.3 Mechanische Schlüsselschlösser

5.1.3.1 Bei HSS der Klasse A (siehe 4) darf der gleiche Code erst dann wiederholt werden, wenn mindestens 80% der nutzbaren Codes schon verwendet wurden. Die Bewertung erfolgt nach 8.1.2.

5.1.3.2 Codes (und gleichschließende Codeträger) müssen nach einem Zufallsverfahren ausgewählt werden. Die Bewertung erfolgt nach 8.1.2.

5.1.3.3 Bei Bewertung nach 8.1.2 dürfen sich weder auf dem Codeträger noch auf dem HSS eine Nummer oder eine Kennzeichnung befinden, mit denen sich der Code feststellen lässt. ^[A1] Es soll außerdem keine Legitimationskarte ausgegeben werden. ^[A1]

5.1.3.4 Es darf nicht möglich sein den Schlüssel von einem HSS abziehen, wenn das HSS entsperrt ist, außer für die Codeumstellung. Diese Anforderung gilt für alle Klassen. Es ist zulässig, dass diese Funktion erst vor der ersten Nutzung des HSS aktiviert wird.

5.1.3.5 ^[A1] Der Schlüssel darf bei Anwendung eines maximalen Drehmoments von 2,5 Nm nicht abbrechen. Der Test ist nach 8.2.1.4 durchzuführen. ^[A1]

^[A1] 5.1.3.6 Neben der Erfüllung der vorhergehenden Anforderungen muss der Hersteller auch eine Herstellererklärung nach Anhang C abgeben. ^[A1]

5.1.4 Codierungsstufen für mechanische Schlüsselschlösser

5.1.4.1 Nutzbare Codes dürfen höchstens 40% der Codierelemente (Zuhaltungen) mit gleich hohen Codierungsstufen enthalten.

5.1.4.2 Bei nutzbaren Codes dürfen höchstens zwei gleiche Codierungsstufen einander benachbart sein, z. B. zwei gleiche Zuhaltungen.

5.1.4.3 Bei nutzbaren Codes muss der Unterschied zwischen der höchsten und tiefsten Codierungsstufe größer als 60% des größtmöglichen Stufensprungs des HSS sein.

5.1.5 Elektronische HSS

5.1.5.1 Bei elektronischen HSS mit mehr als einem Parallelcode müssen die Aufzeichnungen der durchgeführten Öffnungsvorgänge nach Tabelle 1 gespeichert werden. Die gespeicherten Daten müssen selbst bei Stromausfall mindestens 1 Jahr erhalten bleiben.

5.1.5.2 Bei elektronischen HSS in gesichertem Zustand darf ein Datenverkehr mit der Auswerteeinheit nur möglich sein zur Eingabe eines Berechtigungscodes und Anzeige des Schlosszustandes.

5.1.5.3 Bei elektronischen HSS der Klassen B, C und D muss die Eingabeeinheit fest an der zu sichernden Tür oder dem Türrahmen des Wertbehältnisses befestigt sein. Es darf nicht möglich sein, die Eingabeeinheit gewaltsam zu entfernen, ohne dass für den Nutzer offensichtliche dauerhafte Spuren oder Beschädigungen entstehen oder es dem Nutzer angezeigt wird. Die Prüfung erfolgt nach 8.1.2.

5.1.5.4 Bei elektronischen HSS der Klassen B, C und D dürfen unberechtigte Versuche, Zugriff auf sicherheitsempfindliche Teile der Eingabeeinheit zu erlangen, nicht möglich sein, ohne dass für den Nutzer offensichtliche dauerhafte Spuren oder Beschädigungen entstehen oder es dem Nutzer angezeigt wird. Die Prüfung erfolgt nach 8.1.2.

5.1.5.5 Bei elektronischen HSS der Klasse A können die Eingabeeinheiten vom Schloss getrennt sein. Sie sollten dann aber mit einem abgeschirmten Kabel dauerhaft und sichtbar mit der Tür oder dem Türrahmen des Wertbehältnisses verbunden sein.

5.1.5.6 Bei elektronischen HSS aller Klassen muss es dem Nutzer eindeutig angezeigt werden, wenn eine Sperrzeit aktiviert ist.

5.1.5.7 Anzeige des Batteriezustandes: mit Batterie betriebene Schlösser müssen für mindestens 3 000 vollständige Öffnungsvorgänge funktionsfähig bleiben. Die Batteriekapazität muss überwacht werden. Im Falle eines Spannungsabfalls der Batterien muss während oder unmittelbar nach dem Entsperrvorgang ein akustisches oder optisches Signal erfolgen. Nach der ersten Anzeige des Spannungsabfalls der Batterien müssen noch mindestens zehn vollständige Entsperr- und Sperrvorgänge möglich sein. Diese Anforderung muss nicht erfüllt werden, wenn eine Stromversorgung von außen möglich ist.

A1 **5.1.5.8** Der Prozessor, der die Codeauswertung vornimmt, muss sich innerhalb des Wertbehältnisses befinden.

5.1.5.9 HSS der Klasse B oder höher sind auf Einflüsse durch Stromversorgung nach 8.2.5 zu prüfen. **A1**

5.2 Sicherheitsanforderungen

5.2.1 Nutzbare Codes

Die Mindestzahl der nutzbaren Codes für alle Klassen und Arten von Hochsicherheitsschlössern muss den Werten von Tabelle 1 entsprechen. Die Prüfung erfolgt nach 8.2.1. **A1** Die Mindestzahl von 25 000 nutzbaren Codes für mechanische Schlösser der Klasse A ist nur dann als ausreichend einzustufen, wenn der Manipulationswiderstand nach Tabelle 1 mittels manuellem Test nach 8.2.2. nachgewiesen wird. Ab 80 000 oder mehr nutzbaren Codes ist der manuelle Manipulationstest nicht mehr obligatorisch erforderlich. **A1**

HSS mit Parallelcodes: die Mindestzahl der nutzbaren Codes muss mit der Zahl der möglichen Parallelcodes multipliziert werden.

HSS mit variabler Länge der Öffnungscodes: die niedrigste Zahl der benutzten Zeichen, die das HSS als Öffnungscode verarbeiten kann, ist für die Berechnung der nutzbaren Codes heranzuziehen.

Mechanische Schlüsselschlösser dürfen von den zusätzlichen Schlüsseln nicht entsperrt werden. Die Prüfung erfolgt nach 8.2.1.3.

5.2.2 Hochsicherheitsschlösser mit Parallelschloss

Bei HSS mit einem Parallelschloss (z. B. ein elektronisches HSS parallel mit einem mechanischen HSS) erfolgt die Klassifizierung nach dem Schloss mit dem geringsten Sicherheitswert.

5.2.3 Widerstand gegen Manipulation

5.2.3.1 Höchstwerte für Öffnungsversuche

Die zulässige maximale Anzahl der Öffnungsversuche pro Stunde muss den Werten in Tabelle 1 entsprechen.

ANMERKUNG Tabelle 1 enthält für mechanische HSS mit Codeträgern keine Anforderungen an die Anzahl der Öffnungsversuche, weil der Zeitaufwand für den Wechsel der Codeträger die Anzahl der Öffnungsversuche ausreichend begrenzt.

5.2.3.2 Manipulation

Bei den Prüfungen zur Ermittlung des Widerstandswertes gegen Manipulation nach 8.2.2. müssen die Mindestwiderstandswerte M nach Tabelle 1 bei mindestens 2 der 3 Prüfmuster überschritten werden.

5.2.4 Widerstand gegen zerstörende Angriffe

Bei den Prüfungen nach 8.2.3, bei denen eine äußere Kraft aufgebracht wird, müssen die Mindestwiderstandswerte nach Tabelle 1 überschritten werden.

5.2.5 Widerstand gegen Ausspähen

5.2.5.1 Alle Eingabeformationen in ein elektronisches HSS dürfen 30 s nach der Eingabe nicht mehr erkennbar sein, selbst wenn nur ein Teil des Öffnungscodes eingegeben wurde.

5.2.5.2 Bei HSS der Klassen C und D darf der Winkelbereich, in dem die Codeinformation optisch beobachtet werden kann, nicht größer als 30° sein, gemessen von der Mittellinie aus  wie in 8.2.4 festgelegt. 

 **5.2.5.3** Bei HSS der Klassen C und D ist die direkte Codeeingabe über eine Tastatur mit fester Zeichenbelegung nicht gestattet. Dies gilt nicht, wenn ein Einmalcode verwendet wird. 

5.2.6 Widerstand gegen elektrische und elektromagnetische Einflüsse

5.2.6.1 Elektronische HSS, die aus dem Netz gespeist werden, müssen bei Spannungsschwankungen, Spannungseinbrüchen und Kurzzeitunterbrechungen im Normalzustand bleiben. Die Prüfung erfolgt nach 8.2.5.5.

Befindet sich ein elektronisches Schloss im gesicherten Zustand, so muss es bei einem Ausfall der Versorgungsspannung auch gesichert bleiben (siehe 8.2.5.3).

Netzbetriebene HSS müssen bei einem bis zu 12 h dauernden Ausfall der Netzversorgung gesichert werden können (siehe 8.2.5.4).

5.2.6.2 Elektronische HSS müssen nach der Prüfung ihrer Widerstandsfähigkeit gegen elektrostatische Entladung die Anforderungen nach Tabelle 2 erfüllen. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen. Die Prüfung erfolgt nach 8.2.5.6.

5.2.6.3 Bei der Prüfung der Widerstandsfähigkeit von elektronischen HSS gegen eingestrahelte elektromagnetische Felder müssen die Anforderungen der Tabelle 2 erfüllt werden. Die Prüfung erfolgt nach 8.2.5.9.

5.2.6.4 Nach der Prüfung der Widerstandsfähigkeit von netzbetriebenen elektronischen HSS (ggf. mit Kabel mit mehr als 10 m Länge, die an externe Geräte angeschlossen sind) gegen schnelle transiente elektrische Störgrößen (Burst) müssen die Anforderungen der Tabelle 2 erfüllt werden. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen. Die Prüfung erfolgt nach 8.2.5.7.

5.2.6.5 Nach der Prüfung der Störfestigkeit von elektronischen HSS gegen Stoßspannungen (Surge) müssen die Anforderungen der Tabelle 2 erfüllt werden. Während der Prüfung dürfen die Prüfmuster höchstens 5 ms lang in den ungesicherten Zustand gehen. Die Prüfung erfolgt nach 8.2.5.8.

5.2.7 Widerstand gegen physikalische Umwelteinflüsse

 Alle HSS müssen nach 8.2.6.1, 8.2.6.2 und 8.2.6.3 in Bezug auf Widerstandsfähigkeit gegen Schwingen, Schockeinwirkung und Immersion geprüft werden. 