System Assessment Bericht

bezogen auf elektronische Daten und elektronische Unterschriften;

21 CFR Part 11

System: 900 Touch Control
(Software-Version 5.900.0031)

1 Verfahren und Kontrollen für geschlossene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.1	11.10 (a)	Validierung, IQ, OQ	Ist das System validiert?	**B**		Für die Validierung des Systems ist ausschliesslich der Betreiber verantwortlich. Die Verantwortung des Lieferanten liegt in der Bereitstellung validierfähiger Systeme. Dabei hilft das Metrohm-interne Qualitätswesen, welches jederzeit auditiert werden kann. Metrohm bietet diesbezüglich eine Reihe von Validierungs-Services an: Konformitätszertifikate, vorbereitete Unterlagen für IQ und OQ, Durchführung der IQ und OQ beim Betreiber,... Im System sind Standardmethoden für die Systemvalidierung gespeichert.
1.2	11.10 (a)	Audit Trail, Änderung	Kann das System ungültige oder geänderte Aufzeichnungen erkennen?	**X**		Alle relevanten Bedienereingaben werden in einem automatisch generierten Audit Trail mit Datum, Uhrzeit mit Differenz zu UTC (Coordinated Universal Time) und Anwender dokumentiert. Der Audit Trail wird intern gespeichert und kann mit der Backup Funktion auf den USB-Stick kopiert werden. Mittels Audit Trail Viewer kann das Audit Trail auf dem USB-Stick angeschaut werden. Im Report werden geänderte Ergebnisdaten (Resultate) mit dem Vermerk "nachgerechnet am/von" angezeigt. Bei Methodenänderung wird die geänderte Version mit dem Status "modifiziert" angezeigt. Sowohl beim Speichern von geänderten Methoden als auch beim Ändern von Ergebnisdaten (Nachrechnen) können eine Begründung und zusätzlich ein Kommentar eingegeben werden. Ungültige Resultate können dadurch erkannt werden, dass Grenzwerte definiert werden. Bei deren Überschreiten wird das Resultat markiert und eine Meldung ausgegeben.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.3	11.10 (b)	Report, Ausdruck, elektronische Aufzeichnung	Kann das System einen genauen und vollständigen Papierausdruck der elektronischen Aufzeichnungen erstellen?	**X**		Für Methoden und Bestimmungen (Ergebnisdaten) können konfigurierbare Reports gedruckt werden. Das Ändern der Report-Konfiguration kann für Routineanwender gesperrt werden. Der automatische Ausdruck am Ende einer Analyse kann im System durch Systemeinstellung erzwungen werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann. Jeder Ausdruck ist mit einem Zeitstempel mit Angabe der Differenz zu UTC (Coordinated Universal Time) versehen.
1.4	11.10 (b)	Report, elektronische Aufzeichnung, FDA	Kann das System genaue und vollständige Kopien der Aufzeichnungen in elektronischer Form zur Kontrolle, Überprüfung und Vervielfältigung durch die FDA erstellen?	**X**		Als PC/LIMS-Report werden alle Daten im formatted ASCII-Format abgespeichert. Die automatische Ausgabe am Ende einer Analyse kann im System durch Systemeinstellung erzwungen werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann.
1.5	11.10 (c)	Elektronische Aufzeichnung, Aufbewahrungszeit, Archivierung	Sind die Aufzeichnungen während der ganzen Aufbewahrungszeit ohne weiteres wiederauffindbar?	**B**		Für die Aufbewahrung/Archivierung ist ausschliesslich der Betreiber verantwortlich. Das System kann Daten auf einem USB-Stick, mittels Archivierungssystem oder mittels Papier dauerhaft speichern. Die Daten auf den Datenträgern werden verschlüsselt und mit einer Checksumme versehen. Sie sind so vor ungewollter und unsachgemässer Änderung geschützt. Änderungen werden vom System erkannt. Der Inhalt kann mit der Touch Control Software jederzeit gelesen werden. Das Verfahren, wie Daten archiviert werden und welche Daten das sind, muss vom Betreiber festlegt werden. Schnittstellen zur Archivierung (USB-Stick oder PC/LIMS) sind im System vorhanden.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.6	11.10 (d)	Login, Zugriffsschutz, Berechtigung Benutzer, Administrator	Ist der Systemzugriff auf berechtigte Personen beschränkt?	**X**		Das System besitzt ein Login mit 3 internen Berechtigungsstufen (Administrator, Experte, Routineanwender). Bei Verwendung von Identifikationskarten sind beliebig viele Stufen konfigurierbar, siehe auch 11.10 (g), Nr. 1.12. Die für das System verantwortliche Person (Administrator) muss sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.
1.7	11.10 (e)	Audit Trail, elektronische Aufzeichnung, Bedienereingaben	Besteht ein sicherer, rechnergenerierter, zeitgestempelter Audit Trail, der Datum und Zeit der Bedienereingaben und Aktionen protokolliert, welche elektronische Aufzeichnungen erstellen, ändern oder löschen?	**X**		Im Audit Trail werden alle relevanten Bedienereingaben und Aktionen mit Datum, Uhrzeit mit Differenz zu UTC und Anwender dokumentiert. Der Audit Trail wird intern gespeichert und mit der Backup Funktion auf den USB-Stick kopiert. Mittels Audit Trail Viewer kann das Audit Trail auf dem USB-Stick angeschaut werden.
1.8	11.10 (e)	Elektronische Aufzeichnung, Überschreiben von Daten, Änderung	Wenn elektronische Aufzeichnungen geändert werden, bleiben früher aufgezeichneten Informationen im System noch verfügbar (d. h. werden diese durch die Änderung nicht überschrieben)?	**(X)** **B**		Das System überschreibt die Informationen im internen Speicher. Wenn Daten verändert und gespeichert werden, wird automatisch eine neue Version erstellt, die die letzte Version überschreibt. Es muss organisatorisch sichergestellt werden, dass nach der Datenänderung eine Datei mit eindeutiger Dateibezeichnung gespeichert und archiviert wird. Sofern Ausdrucke der elektronischen Aufzeichnungen existieren, muss organisatorisch sichergestellt werden, dass Ausdrucke nach der Datenänderung eindeutig identifizierbar und den jeweiligen Methoden und Bestimmungen eindeutig zuzuordnen sind.
1.9	11.10 (e)	Audit Trail, Aufbewahrungszeit	Bleibt der Audit Trail einer elektronischen Aufzeichnung während der ganzen Aufbewahrungszeit der Aufzeichnung wiederauffindbar?	**(X)** **B**		Der Audit Trail wird intern gespeichert und mit der Backup Funktion auf den USB-Stick kopiert. Mittels Audit Trail Viewer kann das Audit Trail auf dem USB-Stick angeschaut werden. Für die sichere Aufbewahrung/Archivierung des Audit Trails ist ausschliesslich der Betreiber verantwortlich.
1.10	11.10 (e)	Audit Trail, FDA, Einsichtnahme	Ist der Audit Trail zur Überprüfung und Vervielfältigung durch die FDA verfügbar?	**X**		Der Audit Trail kann mit Hilfe des mitgelieferten Audit Trail Viewers als Textdatei exportiert werden und ist so in elektronischer Form und auf Papier verfügbar. Unabhängig davon kann eine schreibgeschützte PDF-Datei des Audit Trails erzeugt und gedruckt werden.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.11	11.10 (f)	Ablaufsteuerung, Plausibilitätsprüfung, Geräte	Wenn der Ablauf der Systemschritte oder Ereignisse wichtig ist, wird dieser durch das System erzwungen (z. B. wie es in einem Steuerungssystem der Fall wäre)?	**X**		Im System werden Plausibilitätsprüfungen schon beim Start der Bestimmung durchgeführt, so wird zum Beispiel überprüft, ob alle benötigten Geräte vorhanden sind. Der Ablauf der Bestimmung ist in der Methode festgelegt und muss strikt eingehalten werden. Das Einhalten des Ablaufs wird durch die Verwendung der Probenzuordnungstabelle oder der automatischen Probedatenabfrage unterstützt. So sind immer nur die Funktionen zugänglich, die ausgeführt werden können.
1.12	11.10 (g)	Login, Zugriffsschutz, Berechtigung, Benutzer, Administrator	Stellt das System sicher, dass nur berechtigte Personen das System benutzen, Aufzeichnungen elektronisch visieren, auf die Funktion, die Rechnersystemeingabe- oder Ausgabeeinheit zugreifen, eine Aufzeichnung ändern oder andere Funktionen ausführen können?	**X**		Durch die Loginfunktion kann der Benutzer identifiziert werden. (Die für das System verantwortliche Person (Administrator) muss sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.) Die Administratorfunktion kann von Benutzerrollen klar getrennt werden, siehe auch 11.10 (d), Nr. 1.6. Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht dieselbe Person ist.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.13	11.10 (h)	Waage, Anschluss, Endgerät, Eingabedaten, Geräte	Kontrolliert das System die Gültigkeit der angeschlossenen Geräte? *Wenn die Systemanforderung besteht, dass Eingabedaten oder Befehle nur über gewisse Eingabegeräte (z. B. Endgeräte) eingehen können, kontrolliert dann das System die Gültigkeit der Quelle der erhaltenen Daten oder Befehle?* *(Hinweis: Gilt in Fällen, wo Daten oder Befehle über mehr als ein Gerät eingehen können, so dass das System die Integrität der Quelle, z. B. ein Netz von Waagen oder funkgesteuerte Fernendgeräte), überprüfen muss.*	**X/B**		USB-Geräte, z. B. Drucker, Barcode-Scanner und Tastatur, werden erkannt und auf Gültigkeit geprüft. Die Vendor-ID wird automatisch ausgelesen und automatisch in die Geräteliste eingetragen. Während der IQ werden alle angeschlossenen Geräte in die Geräteliste eingetragen und später geprüft. Für Barcodescanner ist die Systemeinstellung "Eingabeziel" zu prüfen und der Barcode-Scanner korrekt einzustellen (IQ). Metrohm-Geräte werden erkannt, auf Gültigkeit geprüft und in die Geräteliste eingetragen. Waage: Im System wird die Konfiguration der Waage gespeichert. Um zu kontrollieren, dass die korrekte Waage angeschlossen ist, obliegt es dem Betreiber, eine IQ nach einer Systeminstallation oder -änderung durchzuführen. Die erhaltenen Daten werden auf die korrekte Kennung und die Position des Gewichts in der Zeichenfolge geprüft. Eine weitergehende inhaltliche Prüfung findet nicht statt. Die Validierung der angeschlossenen Geräte erfolgt im Rahmen der Systemvalidierung (siehe auch 11.10 (a), Nr. 1.1) in der Verantwortung des Betreibers.
1.14	11.10 (i)	Schulung, Support, Benutzer, Administrator	Gibt es dokumentierte Schulungen, einschliesslich Ausbildung am Arbeitsplatz (training on the job), für Systembenutzer, Entwickler, IT-Supportpersonal?	**X/B**		Die Schulung der Anwender und Gerätebetreuer liegt in der Verantwortung des Betreibers. Metrohm bietet Standard-Schulungen für alle Anwendungsbereiche an. Individuelle Trainings können gesondert vereinbart werden. Entwickler und Service-Personal der Metrohm werden regelmässig weitergebildet.
1.15	11.10 (j)	Policy, Verantwortung, elektronische Unterschrift	Bestehen schriftliche Grundsätze (Policy), welche die Zuständigkeit und volle Verantwortung von Personen für Handlungen vorschreiben, die mit ihren elektronischen Unterschriften unternommen wurden?	**B**		Der Betreiber muss im Falle der Nutzung der elektronischen Unterschrift eine Policy haben, die die Gleichheit der handschriftlichen und der elektronischen Unterschrift klarstellt.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
1.16	11.10 (k)	Dokumentation, Verteilung Dokumentation, Zugriff auf Dokumentation, Systemdokumentation, Logbuch, Gebrauchsanleitungen	Wird die Verteilung, der Zugriff auf sowie die Benutzung der Systembedienungs- und Wartungsdokumentation kontrolliert?	**B**		Das System besitzt eine umfangreiche Online-Hilfe, die den Benutzer und das Wartungspersonal unterstützt. Die Verteilung der papierbasierten Dokumentation liegt beim Betreiber.
1.17	11.10 (k)	SOP, Dokumentation, Gebrauchsanleitungen, Systemdokumentation, Audit Trail, Logbuch	Besteht ein formeller Änderungskontrollablauf für die Systemdokumentation, der einen Audit Trail der Änderungen mit Zeitablauf festhält?	**X/B**		Die Systemdokumentation ist eindeutig einem System und einer Softwareversion zugeordnet. Zu jeder Softwareversion werden Release Notes geführt. Die Protokollierung von Änderungen der Systemdokumentation und Software – bspw. im Gerätelogbuch – liegt in der Verantwortung des Betreibers. Vorlagen für diese Dokumente werden von Metrohm zur Verfügung gestellt.

2 Zusätzliche Verfahren und Kontrollen für offene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
2.1	11.30	Daten, Verschlüsselung, Datenübertragung	Können Methoden oder Bestimmungen sicher von einem System zum Nächsten übertragen werden? Sind Daten auf dem Weg vom Absender zum Empfänger verschlüsselt?	**N/A**		Ein Zugriff auf 900 Touch Control über das Internet ist nicht vorgesehen. Die Daten werden als Datei gespeichert, verschlüsselt und mit Prüfsumme versehen abgelegt. Die Daten sind somit vor unerlaubter Veränderung geschützt. Im Falle einer Änderung werden die Daten unbrauchbar. Auch wenn beschädigte Daten auf ein anderes System übertragen werden, wird dies erkannt.
2.2	11.30	Elektronische Unterschrift	Werden elektronische Unterschriften verwendet?	**N/A**		Ein Zugriff auf 900 Touch Control über das Internet ist nicht vorgesehen. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht dieselbe Person ist. Die Daten werden als Datei gespeichert, verschlüsselt und mit Prüfsumme versehen abgelegt. Die Daten sind somit vor unerlaubter Veränderung geschützt. Im Falle einer Änderung werden die Daten unbrauchbar. Auch wenn beschädigte Daten auf ein anderes System übertragen werden, wird dies erkannt

3 Unterschriebene elektronische Daten

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
3.1	11.50	Elektronische Unterschrift	Enthalten unterschriebene elektronische Aufzeichnungen die folgenden verwandten Informationen? - vollständiger Name des Unterzeichners - Datum und Zeit der Unterschrift - Bedeutung der Unterschrift (wie Genehmigung, Überprüfung, Verantwortung)	**X**		Bei Methoden und Bestimmungen enthalten alle Unterschriften den vollständigen Namen des Unterschreibenden, das Datum und die Uhrzeit zum Zeitpunkt der Unterschrift, und die Bedeutung (aus Auswahlliste) für die Unterschrift. Zusätzlich kann zu einer Unterschrift ein Kommentar eingegeben werden, der zusammen mit der elektronischen Unterschrift abgespeichert wird.
3.2	11.50	Elektronische Unterschrift	Erscheint die oben erwähnte Information in angezeigten und gedruckten Kopien der elektronischen Aufzeichnung?	**X**		Bei der Anzeige im Display und auf Ausdrucken werden die kompletten Unterschriftsdaten ausgegeben.
3.3	11.70	Elektronische Unterschrift	Besteht eine Verbindung zwischen den Unterschriften und den entsprechenden elektronischen Aufzeichnungen, um sicherzustellen, dass sie nicht mit gewöhnlichen Mitteln zu Fälschungszwecken ausgeschnitten, kopiert oder sonst übertragen werden können?	**X**		Die Unterschrift ist sicher mit der Methode oder der Bestimmung verbunden. Das Ausschneiden, Kopieren oder Übertragen der Unterschriftsdaten ist mit gewöhnlichen Mitteln nicht möglich. In die Unterschrift werden die Benutzerinformationen komplett übernommen. Diese sind bei der Darstellung der Unterschrift dann immer in Klartext lesbar!

4 Elektronische Unterschriften (allgemein)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
4.1	11.100 (a)	Elektronische Unterschrift	Sind elektronische Unterschriften eindeutig einer Person zugeordnet?	**X**		Jedem Benutzer ist ein eindeutiger Anmeldenamen zugeordnet. Betrieblich ist sicherzustellen, dass keine Mehrfachverwendung eines Anmeldenamens stattfindet (das System überwacht die Eindeutigkeit des Anmeldenamens).
4.2	11.100 (a)	Elektronische Unterschrift	Werden elektronische Unterschriften je durch andere Personen wiederverwendet oder anderen Personen zugeteilt?	**B**		Ein verwendeter Anmeldename ist einer Person zugeordnet. Es ist betrieblich sicherzustellen, dass dieser Anmeldename nicht einer anderen Person zugeordnet wird. Eine Reaktivierung bleibt davon unberührt.
4.3	11.100 (a)	Elektronische Unterschrift, Stellvertreterregelung	Erlaubt das System die Übertragung der Berechtigung von elektronischen Unterschriften (Stellvertreterregelung)?	**B**		Die sichere und nachvollziehbare Verwaltung von Benutzerrechten ist Aufgabe des Betreibers. Die Zuordnung eines Stellvertreters ist Teil der regulären Benutzerverwaltung und ist durch den Administrator durchzuführen. Hierfür muss eine betriebliche Regelung vorhanden sein.
4.4	11.100 (b)	Elektronische Unterschrift	Wird die Identität einer Person vor der Zuteilung einer elektronischen Unterschrift überprüft?	**B**		Der Betreiber muss im Zuge der Berechtigungsvergabe die Identität der jeweiligen Person gegen den Berechtigungsantrag prüfen.

5 Elektronische Unterschriften (nicht-biometrisch)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
5.1	11.200 (a) (1)(i)	Elektronische Unterschrift	Besteht die Unterschrift aus mindestens zwei Elementen, wie Identifikationscode (z. B. Benutzername) und Passwort oder Identifikationskarte und Passwort?	**X**		Die Unterschriftsfunktion wird mittels Anmeldename und Passwort ausgeführt.
5.2	11.200 (a) (1)(ii)	Elektronische Unterschrift	Wird das Passwort bei jeder Unterschrift verlangt, wenn mehrere Unterschriften im Laufe einer durchgehenden Sitzung angebracht werden? (Hinweis: beide Elemente müssen bei der ersten Unterschrift einer Sitzung angegeben werden)	**X**		Zu jeder Unterschrift muss das Passwort eingegeben werden.
5.3	11.200 (a) (1)(iii)	Elektronische Unterschrift	Werden immer beide Elemente der elektronischen Unterschrift verlangt, wenn Unterschriften nicht während einer durchgehenden Arbeitssitzung angebracht werden?	**X**		Zu jeder Unterschrift muss der Anmeldename und das Passwort eingegeben werden.
5.4	11.200 (a) (2)	Elektronische Unterschrift	Werden nichtbiometrische Unterschriften ausschliesslich durch ihre tatsächlichen Eigentümer verwendet?	**B**		Der Betreiber muss sicherstellen, dass jeder Anwender nur seine eigene Unterschrift verwendet.
5.5	11.200 (a) (3)	Elektronische Unterschrift, elektronische Unterschrift fälschen	Benötigt ein Versuch, eine elektronische Unterschrift zu fälschen, das Zusammenwirken von mindestens zwei Personen?	**X**		Es gibt keinen regulären Weg, auf die gespeicherten Unterschriftsdaten zuzugreifen.

6 Elektronische Unterschriften (biometrisch)

lfd. Nr.	Ref.		Frage	Ja	Nein	Bemerkungen
6.1	11.200 (b)	Elektronische Unterschrift, biometrische elektronische Unterschrift	Ist es erwiesen, dass biometrische elektronische Unterschriften ausschliesslich durch ihren tatsächlichen Eigentümer verwendet werden können?	**N/A**		Mit dem System werden keine biometrische Unterschriften verwaltet.

7 Kontrolle von Identifikationscode und Passwort

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
7.1	11.300 (a)	Identifikationscode, Eindeutigkeit, Passwort, Identifikation, Login, Zugriffsschutz	Bestehen Kontrollen, um die Einmaligkeit jeder Kombination von Identifikationscode und Passwort sicherzustellen, so dass keine Person die gleiche Kombination von Identifikationscode und Passwort haben kann?	**X**		Das System stellt sicher, dass jeder Identifikationscode (Anwendername) nur einmal innerhalb des Systems verwendet wird, so kann auch eine Kombination von Identifikationscode und Passwort nur einmal vorkommen. Namensänderungen müssen vom Betreiber organisatorisch verwaltet werden! Der Betreiber muss organisatorisch sicherstellen, dass die Identifikationscodes in allen Systemen identisch sind, da sonst die Eindeutigkeit der Benutzer nicht gewährleistet ist. Es wird empfohlen, unternehmensweit eindeutige systemübergreifende Identifikationscodes (z. B. Personalnummer oder Namenskürzel) zu verwenden. Generell wird empfohlen, organisationsweit Richtlinien festzulegen, in denen die Erstellung von Anwenderkonten und die Verwendung von Passwörtern (Länge, Gültigkeitsdauer,...) festgelegt wird.
7.2	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Identifikation, Login, Zugriffsschutz	Sind Verfahren vorgeschrieben, um sicherzustellen, dass die Gültigkeit der Identifikationscodes periodisch überprüft wird?	**B**		Für die periodische Überprüfung der Identifikationscodes ist der Betreiber verantwortlich; zur Unterstützung kann aus dem System vom Administrator eine Liste mit allen Benutzern ausdruckt werden.
7.3	11.300 (b)	Passwort, Gültigkeit, Verfall Passwort, Identifikation, Login, Zugriffsschutz	Unterstehen Passwörter dem periodischen Verfall, damit sie regelmässig geändert werden müssen?	**X**		Die Gültigkeitsdauer für das Passwort kann vom Administrator festgelegt werden. Werte zwischen 30 und 90 Tagen sind gebräuchlich. Nach Ablauf dieser Frist muss das Passwort vom Benutzer zwingend geändert werden. Das System speichert die Passworthistorie, somit ist eine Wiederverwendung von Passwörtern nicht möglich.
7.4	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsberechtigung, Identifikation, Login, Zugriffsschutz	Besteht ein Verfahren für den Rückruf oder die Sperrung von Identifikationscodes und Passwörtern, wenn eine Person austritt oder den Arbeitsplatz wechselt?	**B**		Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator deaktiviert werden, bleibt jedoch im System in der Gruppe „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	Bemerkungen
7.5	11.300 (c)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsberechtigung, Identifikation, Login, Zugriffsschutz, Verlust ID-Karte	Besteht ein Verfahren zur elektronischen Sperrung eines Identifikationscodes oder Passwortes, wenn es möglicherweise unsicher oder verloren gegangen ist?	**B**		Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator deaktiviert werden.
7.6	11.300 (c)	Verlust / Kompromittierung ID-Karte, elektronische Sperrung	Besteht ein Verfahren zur elektronischen Sperrung eines Zugangsgeräts (z. B. ID-Karte), falls es verloren oder gestohlen wurde, oder möglicherweise unsicher ist?	**N/A**		Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen.
7.7	11.300 (c)	ID-Karte, Ersatz	Gibt es kontrollierte Verfahren wie ein Zugangsgerät (z. B. ID-Karte) vorübergehend oder dauerhaft gegen ein Ersatzgerät ausgetauscht wird?	**N/A**		Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen.
7.8	11.300 (d)	Missbrauch, Login, Zugriffsschutz	Bestehen Kontrollen zur Verhinderung und/oder Erkennung von missbräuchlicher Verwendung von Benutzerkennung oder Passwort?	**X/B**		Nach n-maligen Fehlversuchen (Anzahl kann vom Administrator definiert werden) wird eine Meldung ausgegeben, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde und der Benutzer gesperrt; diese Meldung kann per E-Mail verschickt werden.
7.9	11.300 (d)	Missbrauch, Login, Zugriffsschutz, Information an verantwortliche Stelle	Existiert ein Verfahren, nach dem beim Auftreten einer missbräuchlichen Verwendung von Benutzerkennung oder Passwort, die für Sicherheitsfragen zuständigen Stelle(n) sofort und direkt informiert werden?	**B**		Ein Verfahren zur Meldung an das Management muss vom Betreiber festgelegt werden.
7.10	11.300 (e)	Überprüfung ID-Karte, ID-Karte, Zugriffsschutz	Werden Identifikationsmarken und Karten am Anfang und danach periodisch überprüft?	**N/A**		Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen.
7.11	11.300 (e)	Änderung ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz	Beinhaltet diese Prüfung auch eine Kontrolle, dass keine unerlaubten Änderungen vorgenommen wurden?	**N/A**		Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen.

B = Der Betreiber ist für die Umsetzung verantwortlich
N/A = Trifft auf das System nicht zu (not applicable)

Das hier dokumentierte 21 CFR Part 11 Assessment basiert auf einem Audit, das am 02.03.2004 durchgeführt wurde; Gegenstand der Überprüfung war die Version 5.840.0120. Alle nachfolgenden Softwareversionen – einschliesslich der aktuellen – beinhalten gemäss Aussage der Leitung Entwicklung und Qualitätssicherung der Metrohm AG keine 21 CFR Part 11 relevanten Änderungen, bzw. sind 21 CFR Part 11 konform (s. Release Notes 8.840.8009EN, 8.900.8004EN, 8.900.8009EN, 8.900.8016EN, 8.900.8017EN, 8.900.8019EN). Aus diesem Grunde konnte auf eine physische Nachprüfung verzichtet werden.

8 Indizes

Verweise auf die Seitenzahl:

Verweise auf die laufende Nummer des Tabelleneintrags: