

Prüfmittelmanagement im GxP-regulierten Umfeld

Anforderungen & Umsetzung – Teil 2*)

Hansjörg Gutmann, Mario Meister, Dr. Susan Spiller •
Testo Industrial Services GmbH, Kirchzarten

Korrespondenz: Hansjörg Gutmann, Testo Industrial Services GmbH,
Gewerbestraße 3, 79199 Kirchzarten; **E-Mail:** HGutmann@testotis.de



Entscheidungsschema zur Einstufung der Kritikalität von Messmitteln

Bevor die Prüfmittelidentifizierung und die Messtellenrisikoanalyse inklusive der Kalibrierintervallbestimmung vorgenommen werden, sollten vorab Einstufungskriterien für die Bestimmung der Kritikalität der Messmittel festgelegt werden. Mit gut durchdachten Kriterien muss später bei Neuanschaffungen von Messmitteln der Einstufungsprozess nicht jedes Mal neu gestartet werden und der Bearbeitungsaufwand verringert sich. Hierbei ist zu beachten, dass zu grobe Betrachtungen, wie das Auslassen (in der Betrachtung) eines nachgeschalteten Prozesses, zu einer möglicherweise zu „harten“ Eingruppierung (Klasse I statt II) führen könnten, wodurch der wirtschaftliche Vorteil und die Effizienz des Entscheidungsschemas wieder verringert werden würden.

Abbildung 2 zeigt ein mögliches Beispiel für ein solches Einstufungsschema. Hier wird durch Ja/Nein-Fragen die Einordnung in die Kritikalitätsstufen des GAMP herbeigeführt. Dabei werden die Informationen des Herstellers ebenso miteinbezogen wie die Erfahrungshistorie und die Daten aus einer parallelen Überwa-

chungssensorik (Messmittel der Prüfmittelüberwachung aus dem Prüfmittelmanagement, PMÜM). Zudem wird die Prozessorientierung des Messmittels betrachtet.

Best Practice Behälterüberwachung

Betrachtet man das Beispiel aus der Messtellenrisikoanalyse erneut unter diesem Einstufungsschema, kommt man zu folgendem Ergebnis: Beide Sensoren (Temperatur und Druck) sind GMP-relevante Messstellen. Die Temperatur ist im Vergleich zum Druck eine kritische Messstelle, die zusätzlich produktrelevant ist. Eine falsche Temperatur erzeugt eine falsche Materialzusammensetzung bzw. macht das Produkt evtl. unbrauchbar. Der Temperatursensor wird daher in Kategorie I eingestuft. Der Drucksensor erfasst keinen kritischen Prozessparameter, wird jedoch aus Sicherheitsgründen in Kategorie III eingestuft. Eine nicht funktionierende Anzeige suggeriert dem Anwender u. U., er könne einen unter Druck stehenden Tank bedenkenlos öffnen, was schwere Folgen haben könnte. Dies kann durch die Kalibrierung verhindert werden. Zu beachten ist, dass in diesem Fall die nachgeschalteten Prozesse nicht betrachtet werden und der Temperatursensor – anders als in der detaillierten Messtellenrisikoanalyse – in Ka-

tegorie I statt II eingestuft wird. Es ist demnach wichtig, die Einstufungskriterien so praxisnah wie möglich und detailliert wie nötig zu wählen.

Verwaltung der ermittelten Daten

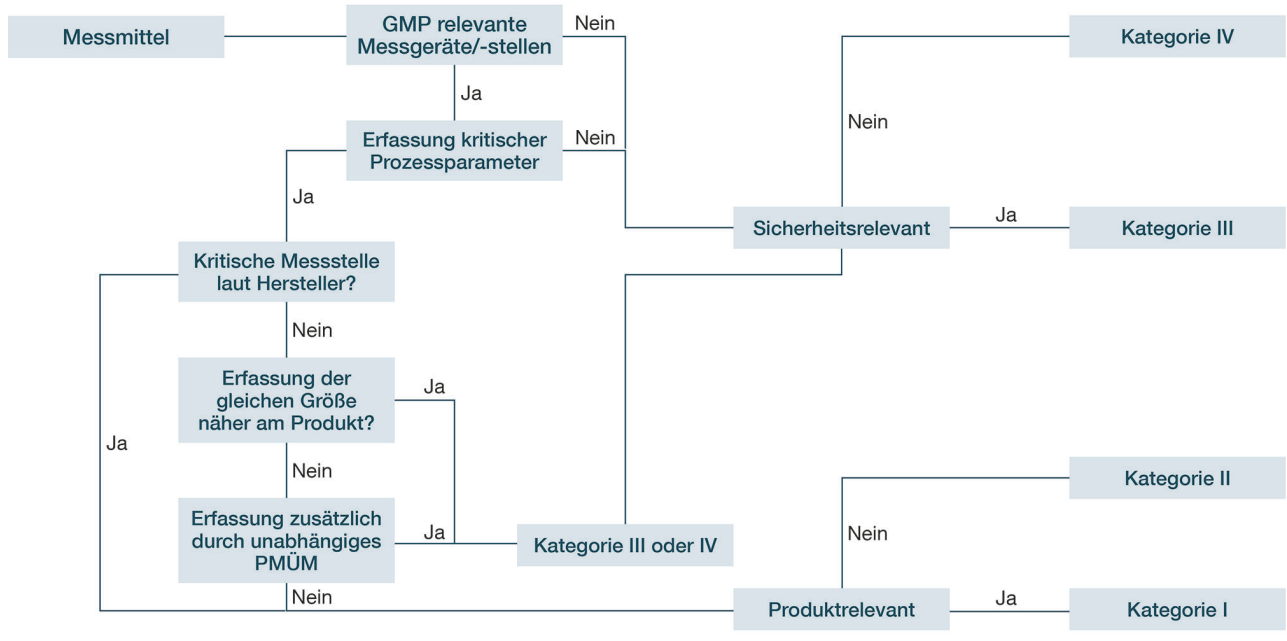
Die Fülle an Informationen zu den einzelnen Messtellen aus dem Kalibriermanagement sollte zur optimalen Prüfmittelverwaltung in ein GxP-konformes, validierfähiges Prüfmittelmanagementsystem überführt werden. Ohne Validierung kann nicht geprüft werden, ob die geforderten Funktionalitäten zur Verfügung stehen, das System geeignet, zuverlässig und effizient ist. Ein solches System kann das praktische Arbeiten deutlich vereinfachen und bietet die Möglichkeit, z. B. Erinnerungen an Kalibrierintervalle automatisch eskalieren zu lassen. Auch Zugriffsrechte für den Anwenderkreis können hier hinterlegt werden und Änderungen an den Messtellendaten sind im System nachvollziehbar. Zentral hierbei sind Datenintegrität und -sicherheit.

Anforderungen an Daten bei der Validierung von automatisierten Prüfmittelmanagementsystemen

Prüfmittelmanagementsysteme dienen zur Verwaltung unterschied-

*) Teil 1 dieses Beitrags ist erschienen in TechnoPharm 12, Nr. 5, 254-258 (2022).

Kritikalitäts-Kategorien



- I. Produktkritisch: Instrumente, deren Genauigkeit bzw. Abweichung einen hohen potentiellen Einfluss auf die Produktqualität oder Patientensicherheit hat.
- II. Prozesskritisch: Instrumente, deren Genauigkeit bzw. Abweichung einen hohen potentiellen Einfluss auf die Prozesseffektivität oder wirtschaftliche Aspekte hat.
- III. Sicherheits-/umweltkritisch: Instrumente, deren Genauigkeit bzw. Abweichung einen hohen potentiellen Einfluss auf die Sicherheit des Betreibers oder auf die Umwelt hat.
- IV. Nichtkritisch: sind Instrumente, deren Genauigkeit bzw. Abweichung keinen hohen potentiellen Einfluss hat.

Abbildung 2: Beispiel einer Kritikalitätseinstufung angelehnt an GAMP „Good Practice Guide: A Risk-Based Approach to Calibration Management“.

lichster Equipments/Messmittel. Neben den funktionalen Eigenschaften der Applikation ist bei der Validierung der Fokus auf die GxP-Anforderungen zu legen, die sich aus Annex 11 [7] und 21 CFR Part 11 [8] ergeben. Die Datenintegrität ist daher zentraler Bestandteil der Validierung und muss durch entsprechende Maßnahmen, die im Folgenden erläutert werden, sichergestellt werden.

Qualitätsrelevante Daten

Qualitätsrelevante Daten müssen vor unautorisierten Zugriffen und Änderungen geschützt werden. Im

ersten Schritt empfiehlt sich eine Bewertung, welche Daten für den Prozess der Prüfmittelverwaltung qualitätsrelevant sind.

Daten zum Equipment lassen sich z. B. in 3 Kategorien aufteilen (Abb. 3):

1. **Stammdaten:** Daten, die zur Identifizierung des Equipments dienen, z. B. Bezeichnungen, Seriennummer, Hersteller oder das Anschaffungsdatum
2. **Bewegungsdaten:** Daten, die Aufschluss zur Zuordenbarkeit und Vorgängen geben. Darunter fallen der Standort, Kostenstelle, Eigner, aber auch Vorgänge wie

Verleihe, Reparaturen und Kalibrierungen.

3. **Steuerungsdaten:** Daten, die die Kalibrierung oder andere Vorgänge steuern. Hierzu zählen Kalibrierintervalle, Toleranzen und Genauigkeiten, Statusinformationen und Klassifizierungseinstellungen wie Konformitätsaussagen, Freigabefunktionen oder Erinnerungs-/Reportingfunktionen.

Es sind also alle Daten relevant, die zur Verwaltung der Equipments und zur Planung regelmäßiger Maßnahmen wie Kalibrierungen dienen, und alle Aufzeichnungen zu qualitätsrelevanten Ereignissen, wie ge-

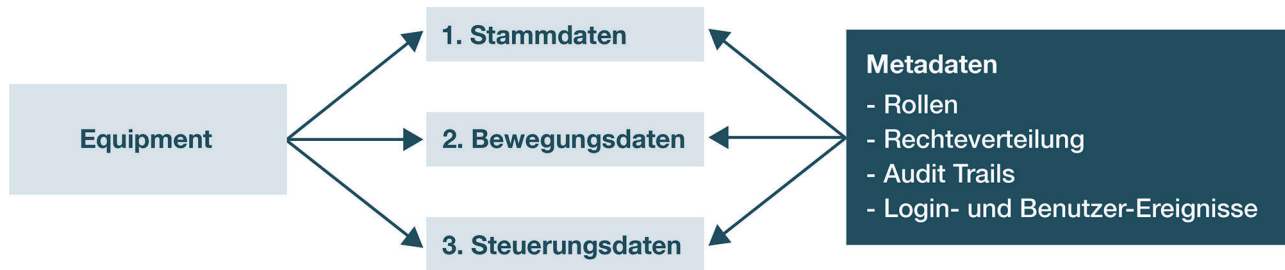


Abbildung 3: Qualitätsrelevante Daten zu einem Equipment in einem Prüfmittelmanagementsystem.

planten Ereignissen (Kalibrierungen/Prüfungen) und ungeplanten Ereignissen (z. B. Reparaturen).

Mitbetrachtet werden sollten auch systemisch vorgenommene Equipment-Freigaben oder Statusänderungen und Dokumentationen zur Kalibrierung (z. B. Kalibrierberichte oder -zertifikate), sofern mit dem Prüfmittelmanagementsystem auch diese Dokumentation verwaltet wird. Darüber hinaus sind solche Daten relevant, die die Integrität der zuvor beschriebenen Equipment-Daten sicherstellen (Metadaten). Dazu gehören Rechteverteilung und Rollen, Audit Trails und Login- und Benutzerereignisse.

Datenerhebung und Zugriffsschutz

Die Verwaltung der Equipments sollte nur durch qualifiziertes und berechtigtes Personal erfolgen. Ein entsprechendes Benutzerkonzept sollte festlegen, wer welche Daten ändern oder einsehen darf. Es ist zu beachten, dass es unterschiedliche Berechtigungsebenen geben sollte: z. B. die Administration (funktional getrennt von der routinemäßigen Anwendung), Prüfmittelverantwortlichkeit und Qualitätssicherung. Weitere Rollen können je nach Prozess hinzukommen. Die Berechtigungen müssen dann den jeweiligen Rollen entsprechend ihrer Tätigkeit in der Applikation zugewiesen werden. Darüber hinaus sind Regelungen zum Zugriffsschutz (z. B. Regeln zu Passwörtern und Benutzernamen) zu implementieren und technisch umzusetzen. Dies ist am einfachsten über eine Anbindung an das Active Direc-

tory zu erreichen, sofern die Applikation dies zulässt. Es ist sinnvoll, dass qualitätskritische Datenänderungen/Ereignisse über Signaturen der dafür berechtigten Anwender bestätigt werden. Aus der elektronischen Unterschrift müssen in diesem Fall der Klurname, Datum und Uhrzeit sowie die Bedeutung der Unterschrift [8] hervorgehen.

Um den Zugriffsschutz zu gewährleisten, sind neben dem Berechtigungskonzept Überwachungsprozesse notwendig. So sind die vergebenen Berechtigungen regelmäßig zu überprüfen, um auszuschließen, dass nicht mehr berechtigte Nutzer weiterhin Zugang zu qualitätskritischen Dateneingaben/-änderungen haben. Zusätzlich kann ein regelmäßiger Review über auffällige Benutzerereignisse wie Login-Ereignisse bzw. fehlgeschlagene Logins oder Signaturen – je nach Kritikalität – sinnvoll sein.

Datenablage und -aufbewahrung

Zur Sicherstellung der Datenintegrität müssen Datenflüsse bekannt sein. Zur Dokumentation dienen z. B. Datenflussdiagramme. Sollten Daten in andere Systeme transferiert werden – wie z. B. in ein Datensicherungssystem – muss sichergestellt werden, dass die jeweiligen Systeme ebenfalls validiert sind und die Schnittstellen im Rahmen der Validierung betrachtet werden. Zur Datensicherung erfolgen regelmäßige Backups der erzeugten Daten, welche in einem wiederherstellbaren und lesbaren Format sicher aufbewahrt werden müssen. Datensi-

cherungs- und Wiederherstellungs-tests sind daher ein notwendiger Bestandteil der Validierung. Darüber hinaus müssen Aufbewahrungsfristen geregelt sein. Zur Aufrechterhaltung des validierten Zustands muss das Datensicherungs- und Wiederherstellungsverfahren regelmäßig überprüft werden. Um das Intervall für die regelmäßige Überprüfung festzulegen, ist es zweckmäßig, die Kritikalität des Prozesses zu bewerten.

Kontrollen

Zur Sicherstellung der Datenintegrität gehört, dass alles, was mit dem Equipment passiert, nachvollziehbar ist und dass dies kontrolliert bzw. überprüft wird. Bei der manuellen Eingabe besonders kritischer Daten ist es daher sinnvoll, einen Kontrollprozess zu etablieren, um Fehler auszuschließen (z. B. 4-Augen-Prinzip). Darüber hinaus sind alle Änderungen und Vorgänge systemisch in Audit Trails aufzuzeichnen. Notwendig für die Zuordenbarkeit und Nachvollziehbarkeit sind Angaben zu Bearbeiter, Datum, Uhrzeit und Vorgang – im Idealfall mit einer Begründung bei Änderungen. Vorher- und Nachher-Werte müssen bei Änderungen relevanter Daten nachvollziehbar sein. Solche Funktionalitäten sollten über Validierungstests sichergestellt werden. Um Vorgänge zu Equipments zu kontrollieren, sollten Regelungen zum Review und Monitoring getroffen werden:

- In einem Review-Konzept für Audit Trails werden relevante Ereignisse im Audit Trail definiert und je nach Kritikalität der Daten ein

Review-Intervall festgelegt. Hierbei kann eine Unterscheidung sinnvoll sein zwischen einem administrativen Review, das sich auf administrative Vorgänge in der Applikation bezieht, und einem operativen Review, das sich auf die operativen Daten zu den Equipments bezieht.

- Für ein regelmäßiges Monitoring des Kalibrierstatus, bestimmter Aktivitäten oder anstehender Kalibrierungen kann ein regelmäßiges Reporting eingerichtet werden. Im Idealfall sind solche Reports in der Applikation konfigurierbar. Diese Konfigurationen sind zudem Bestandteil von Verifizierungstests.

Risikobasierter Ansatz für die Validierung

Prüfmittelmanagementsysteme im GxP-Bereich sind qualitätsrelevant und unterliegen daher einer Validierungspflicht. Für den risikobasierten Ansatz, der in Annex 11 [8] und DIN EN ISO 13485 [2] gefordert wird, empfiehlt sich eine Orientierung an GAMP 5 [5].

Sofern die Software nicht spezifisch für den Kunden/Prozesseigner programmiert wurde, sondern lediglich spezifische Konfigurationen einer Standardsoftware für das Prüfmittelmanagement notwendig sind, kann die Software in die Kategorie 4 gemäß GAMP 5 klassifiziert werden. Die Validierung erfolgt nach dem V-Modell. Teil der Validierung sind die in den vorherigen Abschnitten beschriebenen Anforderungen an die

Daten und an die Kontrolle der Daten. Risikobasiert werden Verifizierungstests festgelegt, um nachzuweisen, dass die Anforderungen an das System und insbesondere an die Datenintegrität erfüllt sind und dass das System für das Prüfmittelmanagement des Anwenders geeignet ist.

Der validierte Zustand muss über den gesamten Lebenszyklus hinweg aufrechterhalten werden. Das bedeutet, auch das Risikomanagement muss sich gemäß GAMP 5 und Annex 11 am Lebenszyklus orientieren. Ein Änderungs- und Konfigurationsmanagement [7] werden im Rahmen der Validierung etabliert, d. h., geplante Änderungen müssen risikobasiert und kontrolliert durchgeführt werden und die Konfigurationen unterliegen hierbei der Änderungskontrolle.

Darüber hinaus schreibt der Annex 11 eine periodische Evaluierung des Systems vor, die nachweisen soll, dass sich das System in einem validen Zustand befindet. Auch dies sollte gemäß eines geregelten Verfahrens durchgeführt werden. Das Intervall der Evaluierung kann risikobasiert festgelegt werden.

Fazit

Ein GxP-konformes Prüfmittelmanagement, das den Anforderungen aus dem Qualitätsmanagement voll gerecht werden soll, lässt sich am besten dadurch erreichen, dass zusätzlich zum Kalibriermanagement die Verwaltung der Prüfmittel auto-

matisiert erfolgt. Als erfolgreich erwiesen hat sich ein risikobasierter Ansatz gemäß GAMP [6] zur Bestimmung der Kriterien für eine korrekte Kalibrierung von Messmitteln (nach geeigneten Verfahren).

Planung und Durchführung der Kalibrierungen lassen sich optimalerweise über ein Prüfmittelmanagementsystem abwickeln, welches selbst validiert ist. Auch hier bildet ein risikobasiertes Vorgehen zur Validierung gemäß GAMP 5 [9] die Basis, um die Prozesssicherheit, Datenintegrität und Datensicherheit über den gesamten Lebenszyklus des Systems hinweg zu gewährleisten und damit alle Voraussetzung für die Konformität des Prüfmittelmanagements zu erfüllen.

Literatur

- [1] DIN EN ISO 9001:2015 – Qualitätsmanagement, 2015
- [2] DIN EN ISO 13485:2016 – Medizinprodukte: Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke, 2016
- [3] EudraLex: EU-GMP-Leitfaden, Teil 1
- [4] „Code of Federal Regulations“ 21 CFR 820: „Food and Drugs“, Abschnitt 72, Apr. 2016
- [5] PIC/S Good Practices for Computerised Systems in Regulated “GXP” Environments (PI 011-3) Sept. 2007, Anhänge 15.22 und 15.36
- [6] ISPE: GAMP Good Practice Guide: A Risk-Based Approach to Calibration Management, Second Edition, 2010
- [7] EudraLex: EU-GMP-Leitfaden, Annex 11 – Computergestützte Systeme, 2011
- [8] FDA: 21 CFR Part 11 – Electronic Records, Electronic Signatures, 1997
- [9] ISPE: GAMP 5, Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme, 2008