Effektiv Compliance für Computersoftware in der Produktion herstellen

Mit zunehmender Digitalisierung in der Produktion von Medizinprodukten wächst auch der Bedarf, die Eignung in der Produktion eingesetzter Computersysteme und zugehöriger Software für GxP-relevante Aufgaben nachzuweisen. Die dazu erforderlichen Tätigkeiten werden unter dem Begriff Computersystem-Validierung (CSV) zusammengefasst. Oftmals führen Zeitmangel und Dringlichkeit dazu, dass dafür ein standardisiertes Validierungskonzept ausgewählt wird, welches aber den unternehmensspezifischen Randbedingungen nicht angepasst ist. Effektivere Vorgehensweisen zur CSV bleiben damit eventuell auf der Strecke. Als Folge leidet die Validierungseffizienz erheblich, starre Teststrukturen führen zu zeitaufwändigen Validierungstätigkeiten und Dokumentationsaufgaben. Der folgende Artikel klärt die regulatorischen Grundlagen und beschreibt einen Validierungsansatz, welcher unkompliziert den spezifischen Belangen angepasst werden kann.

1 CSV aus Sicht der Regularien

In der Pharmawelt ist die Validierung von Computersystemen und der zugehörigen Software schon seit langem ein bedeutendes Thema. Bereits 1997 publizierte die FDA im 21 CFR Part 11 regulatorische Anforderungen an die elektronische Datenverarbeitung [1]. Begleitend dazu erschienenen durch die 1980 gegründete International Society for Pharmaceutical Engineering (ISPE) GAMP-Leitfäden (GAMP - Good Automated Manufacturing Practice), welche die Umsetzung der regulatorischen Anforderungen erleichtern sollten. Darunter nimmt der GAMP 5 Guide [2] eine herausragende Stellung ein. Er wurde 2008 als Nachfolger des GAMP 4 Guide erstmalig publiziert und diente der Fachwelt bis 2022 als zuverlässige Anleitung für CSV. Zur Angleichung an die Konzepte und die Terminologien der jüngsten regulatorischen und industriellen Entwicklungen wurde im Juli 2022 die revisionierte zweite Fassung herausgegeben. Die ISPE schreibt dazu [3]:

„ISPE GAMP 5 „A Risk-Based Approach to Compliant GxP Computerized Systems“ (Second Edition) behält die Prinzipien und den Rahmen der ersten Ausgabe bei und aktualisiert deren Anwendung in der modernen Welt, einschließlich der zunehmenden Bedeutung von Dienstleistern, sich entwickelnden Ansätzen zur Softwareentwicklung und dem erweiterten Einsatz von Softwaretools und Automatisierung.“

Inhalt

Stichworte: CSV – Computersystem-Validierung, Computer Software Validation, Computer Software Assurance, 21 CFR Part 11, GAMP 5, risikobasierte Vorgehensweise

Nach wie vor wird eine risikobasierte Vorgehensweise als Grundlage zur Computersystemvalidierung angesehen. Neu berücksichtigt sind Anhänge zu aktuellen Entwicklungen in der Datensicherheit, der Vernetzung von Systemen (wie z.B. dem Cloud-Computing), des Einsatzes von „Machine-Learning“ und der zunehmenden Verwendung von Softwaretools in der Entwicklung. Auch die Anwendung iterativer und agiler Methoden bei der Projektentwicklung in Gegenüberstellung zu dem V-Modell wird stärker diskutiert.

Der Leitfaden enthält auch neue Vorgaben zur Verifizierung von Software-Funktionalitäten. Detaillierte Schritt-für-Schritt-Pläne scheinen zunehmend als zu aufwendig angesehen zu werden, es werden Alternativen in Form von „exploratory testing“ und „unscripted techniques“ vorgestellt.

In der 2. Version des GAMP 5 wird auch verbreitet vom „critical thinking“ gesprochen. Leider fehlt eine abgrenzende Definition, anhand derer der Neuwert dieses Begriffes bewertet werden kann. Inhaltlich scheint es sich dabei um ein „gründliches Nachdenken“ zu handeln. Dies war und ist aber unabhängig von Regularien schon immer angebracht.

In der Medizintechnik sind nach 21 CFR 820 [4] Eignungsnachweise für in der Produktion eingesetzte Computersysteme und Software ebenfalls zu erbringen:

*„**Automatisierte Prozesse**. Werden Computer oder automatisierte Datenverarbeitungssysteme als Teil der Produktion oder des Qualitätssicherungssystems eingesetzt, muss der Hersteller die Computersoftware für den vorgesehenen Verwendungszweck nach einem festgelegten Protokoll validieren. Alle Software-Änderungen müssen vor der Genehmigung und Herausgabe validiert werden. Diese Validierungsaktivitäten und -ergebnisse sind zu dokumentieren.“*

In 2002 erschien dazu ein Leitfaden der FDA, welcher die allgemeinen Validierungsgrundsätze beschreibt [5].

Ein 2022 herausgegebener Entwurf „Computer Software Assurance for Production and Quality System Software“ [6] wechselt in der Begrifflichkeit von „Computer System Validation“ (CSV) zu „Computer Software Assurance“ (CSA). Inhaltlich wird der risikobasierte Validierungsansatz verstärkt betont. Für diejenigen, welche schon bisher einen risikobasierten Ansatz verfolgt haben, stellt dies aber keine Neuerung dar.

In der zu 21 CFR 820 korrespondierenden europäischen Norm ISO 13485 zu Qualitätsmanagementsystemen für Medizinprodukte enthält erst die Ausgabe von 2016 in Kap. 4.1.6 [7] die dezidierte Anforderung zur Validierung von Computersystemen und deren Software:

„Die Organisation muss Verfahren für die Anwendung der Computersoftware im Qualitätsmanagementsystem dokumentieren. Derartige Softwareanwendungen müssen vor ihrem ersten Einsatz validiert werden sowie, soweit angemessen, nach Änderungen an dieser Software oder ihrer Anwendung.“

Aus sie fordert einen risikobasierten CSV-Ansatz:

„Der spezifische Ansatz und die Tätigkeiten im Zusammenhang mit der Softwarevalidierung und -revalidierung müssen in einem angemessenen Verhältnis zu dem Risiko stehen, das mit dem Einsatz der Software in Verbindung gebracht wird.“

In den letzten Jahren haben sich die grundsätzlichen Compliance-Anforderungen in der Pharma- und der Medizintechnik-Industrie zunehmend angeglichen. Auch auch auf dem Feld der CSV sind entsprechende Entwicklungen zu beobachten. Die im GAMP 5 – Leitfaden beschriebenen Konzepte sind von dem hergestellten Produkt unabhängig einsetzbar. Sie empfehlen sich deshalb auch für die Medizinprodukte-Industrie.

2 Effektive CSV

Je wirksamer (effektiver) ein Ansatz zur Validierung von Computersystemen und der zugehörigen Software ist, desto effizienter, d.h. zeitsparender und kostengünstiger kann eine Validierung durchgeführt werden. Wie im Abschnitt 1 gezeigt, liegt in diesem Zusammenhang der Fokus auf einer risikobasierten Vorgehensweise. Doch wie werden Risiken analysiert und bewertet und darauf abgestimmt die notwendigen Validierungsmaßnahmen festgelegt?

Dazu sollten in der Abfolge Antworten auf die folgenden 3 Fragen gegeben werden:

1.) Ist das System CSV-relevant?
2.) Wie kritisch ist der Einfluss des Systems auf die Sicherheits- und Leistungsanforderungen eines Medizinproduktes?
3.) Welche Komplexität weist das CSV-relevante System auf?

Eine unternehmensspezifische SOP zur Computersystem-Validierung sollte detailliert die Vorgehensweise beschreiben, auf welche Art und Weise Antworten auf die Fragen gefunden werden. Dabei sind die Schulungsbedarfe des involvierten Personenkreises unbedingt zu berücksichtigen, sollen die Prozesse effektiv „gelebt“ werden. Nachfolgend sind wichtige Aspekte zu o.g. Fragen erläutert.

2.1 CSV-Relevanz des Systems bewerten

In einem ersten Schritt ist zu klären, ob das System CSV-Relevanz besitzt. Wenn die in ein System eingegebenen oder durch das System erzeugten Daten die Produktqualität, die Produktdaten, die Produktfreigabe oder dessen Nachverfolgbarkeit beeinflussen, ist das System CSV-relevant, siehe Bild 1. Computersysteme und Software ohne einen derartigen Einfluss müssen keiner CSV unterzogen werden.

Auch elektronische Aufzeichnungen und elektronische Unterschriften (ERES – Electronic Records and Electronic Signatures) müssen erst dann validiert werden, wenn sie im o.g. Sinne CSV-relevant sind. Beispiele hierfür sind Zeitstempel für Analyseprotokolle, die elektronische Unterschrift unter ein Freigabeprotokoll oder die Archivierung von Produktionsdaten zu einzelnen Produktionslosen für CSV-relevante Systeme.

Es hat sich bewährt, in die unternehmenseigene SOP zur Computersystem-Validierung die Darstellung einer entsprechenden Fragenkaskade, siehe Bild 1, aufzunehmen.

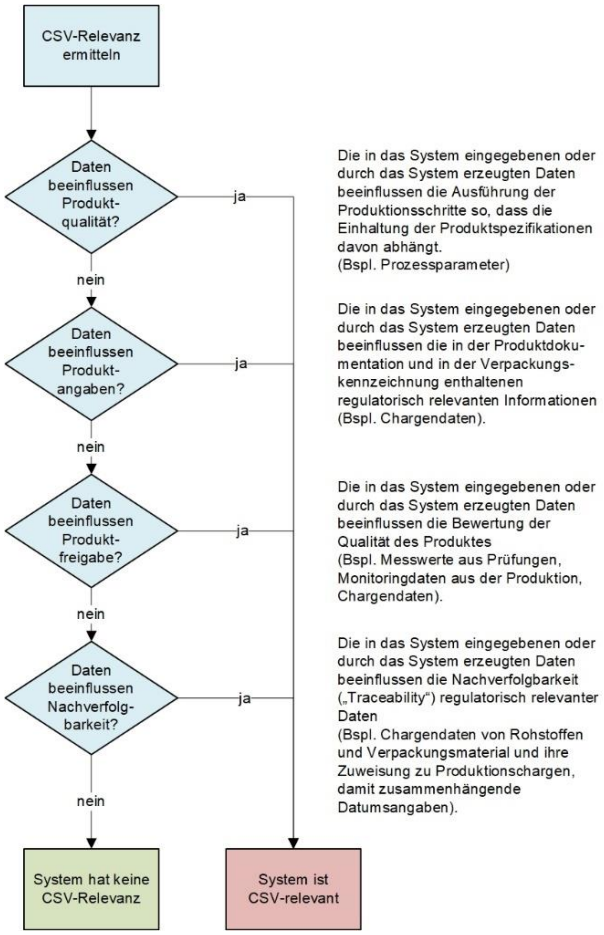

Bild 1: Fragenkaskade zur Ermittlung der CSV-Relevanz

2.2 Kritikalität des Systems bestimmen

In der Bewertung der Kritikalität eines Systems mit CSV-Relevanz liegt ein hohes Potential für eine effiziente Computersystem-Validierung. Je größer der Einfluss auf die GxP-Relevanz (siehe Bild 1), desto höher ist auch die Kritikalität des Produktionssystems. Maßgeblich ist hierfür der Zusammenhang zwischen Prozess- und Produktrisiken.

In [6] werden 5 Beispiele genannt, in denen aufgrund der vorliegenden Prozessrisiken die GxP-Relevanz generell als hoch angesehen wird, das System also kritisch eingestuft wird:

- Prozessparameter (z. B. Temperatur, Druck oder Feuchtigkeit), welche die physikalischen Eigenschaften von Produkten oder von Herstellungsprozessen beeinflussen, die wesentlich für die Sicherheit oder Qualität der Produkte sind.
- Weitgehend automatisierte Messung, Inspektion, Analyse und/oder Freigabe eines Produktes oder Prozesses.
- Weitgehend automatisierte Prozesskorrekturen oder Anpassung von Prozessparametern auf der Grundlage von Monitoringdaten oder automatisierten Rückmeldungen aus anderen Prozessschritten.
- Weitgehend automatisierte Erstellung von Gebrauchsanweisungen oder andere Kennzeichnungen, die für den sicheren Betrieb des Medizinprodukts erforderlich sind.
- Automatisierte Überwachung, Analyse auf Trends oder die Nachverfolgung von Daten, die der Hersteller als wesentlich für die Sicherheit und Qualität des Produkts ansieht.

Systeme mit oben genannten Prozessrisiken generell als kritisch hinsichtlich CSV-Relevanz zu klassifizieren ist nicht falsch aber wenig effizient. Es lohnt sich eine differenziertere Betrachtungsweise. Sie muss das Prozessrisiko in Kontext zum Produktrisiko stellen.

Die Kritikalität in der Produktion eingesetzter Computersysteme und zugehöriger Software ist nur dann hoch, wenn davon

a.) kritische Qualitätsattribute (CQA) beeinflusst werden (→ hoher Schaden) UND
b.) von der Software unabhängige Vermeidungsmaßnahmen im Produkt- oder Prozessdesign die Auftretenswahrscheinlichkeit nicht auf Null (→ A > 0%) reduzieren ODER
c.) die Entdeckungswahrscheinlichkeit für die Abweichung in der CQA-Spezifikation in nachfolgenden Prozessschritten nicht sicher (→ E < 100%) ist.

Erst dann ergibt sich aus einem hohen Prozessrisiko ein hohes Produktrisiko. Im Umkehrschluss gilt, dass ein System, welches aufgrund eines Prozessfehlers eine Spezifikationsabweichung in einem CQA erzeugt, nicht als kritisch angesehen werden muss, wenn der Fehler in nachfolgenden Herstellschritten sicher entdeckt wird und das Fehlteil z.B. ausgeschleust werden kann, siehe Bild 2. Trotz hohem Prozessrisikos wäre in diesem Falle das Produktrisiko vernachlässigbar. Nähere Einzelheiten zur Vorgehensweise sind in [8] beschrieben.

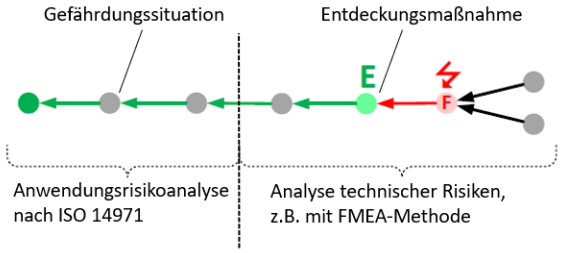

Bild 2: technischer Fehler: Das Eintreten der Gefährdungssituation wird deshalb vermieden, weil ein auftretender Fehler in der Ereigniskette rechtzeitig entdeckt und durch Reaktionsmaßnahmen beherrscht wird.

Das Hauptaugenmerk bei der Bestimmung der Kritikalität eines Systems mit CSV-Relevanz muss also auf dem möglichen Produktrisiko liegen. Es empfiehlt sich, die beschriebene differenzierte Betrachtung der Risiken in die unternehmenseigene SOP zur Computersystem-Validierung aufzunehmen und damit Systeme mit CSV-Relevanz unabhängig von den Prozessrisiken bei zuverlässiger nachfolgender Entdeckung der produzierten Fehler in der Kritikalität herunterstufen zu können. Nachfolgend sind einige Beispiele aufgeführt.

Beispiel 1: Eine automatisierte Montageeinheit verpresst zugelieferte Komponenten. Es besteht CSV-Relevanz, da die Verpressung softwaretechnisch gesteuert wird und damit die Prozessdaten die Produktqualität beeinflussen (siehe Bild 1). Das Produkt ist jedoch als Ergebnis einer Risikoanalyse so optimiert, dass bis zu einem designtechnisch vorgegebenen Einrastpunkt verpresst wird und bei fehlerhafter Verpressung die Komponenten auseinanderfallen. Damit ist die Auftretenswahrscheinlichkeit für fehlerhaft verpresste Endprodukte in der Auslieferung Null, das System besitzt eine niedrige Kritikalität hinsichtlich CSV.

Beispiel 2: Eine Fertigungszelle produziert automatisiert dem individuellen Patienten angepasste Medizinprodukte-Komponenten, deren kritische Abmessungen in einer nachgeschalteten Prüfstation mit Hilfe einer Kamera vermessen werden. Es besteht CSV-Relevanz, da die Produktionsdaten die Produktqualität beeinflussen (siehe Bild 1). Obwohl die Produktionsparameter großen Einfluss auf die Maßhaltigkeit der Komponenten haben, ist jedoch die Kritikalität der Fertigungszelle niedrig, da jede Abweichung in den kritischen Qualitätsattributen nachfolgend sicher erkannt wird. Die Prüfstation mit integrierter Bildverarbeitungssoftware ist CSV-relevant, da deren Daten die Produktfreigabe beeinflussen. Sie ist jedoch im Gegensatz zur Fertigungszelle hinsichtlich CSV als kritisch einzustufen, da von deren Eignung die sichere Entdeckung aller Produktionsfehler abhängt.

2.3 Komplexität des Systems analysieren

Neben der Kritikalität beeinflusst die Komplexität eines CSV-relevanten Systems maßgeblich den Umfang an benötigten Validierungsnachweisen. Die Komplexität wurde in der Vergangenheit hauptsächlich durch folgende Kategorien definiert:

Kategorie 1 – Software und Softwaretools für die IT-Infrastruktur (z.B. Betriebssysteme, Datenbanken, Programmiersprachen, Statistikprogramme, Überwachungssoftware, Antivirus-Software)

Kategorie 2 – nicht mehr verwendet, in GAMP 4 bis 2008 für Firmware vorbehalten.

Kategorie 3 – Standardsoftware (nicht anwenderspezifisch, nicht konfigurierbar oder mit Standardeinstellungen betrieben, weit verbreitet)

Kategorie 4 – Konfigurierbare Software (Entsprechend vorbereitete Module von Standardsoftware, welche anwenderspezifisch konfiguriert werden)

Kategorie 5 – Kundenspezifische Programmierlösungen

Mit dieser Kategorisierung wird der Tatsache Rechnung getragen, dass mit zunehmendem Einfluss individueller Kundenvorgaben das Auftreten softwarespezifischer Fehler wahrscheinlicher wird und die erforderlichen Validierungsnachweise an Komplexität und Umfang zunehmen.

Heutige Softwaresysteme für Produktion und Qualitätssicherung bestehen oftmals aus einer Kombination mehrerer Softwarekomponenten, welche unterschiedlichen Kategorien angehören. Ein Beispiel wäre die Rechnereinheit einer Produktionsanlage, auf der neben der Software zur Maschinensteuerung (Kategorie 4) zugleich eine Bildauswertessoftware zur Qualitätssicherung (Kategorie 4 od. 5), ein Batchmanager für Serialnummern (Kategorie 3), sowie eine Datenbank für den Audittrail und für die Formatdaten (jeweils Kategorie 3 oder 4) installiert

ist. Ein weiteres Beispiel ist in Bild 3 dargestellt. Konfigurierbare Softwaremodule der Kategorie 4 sind zudem für etliche Funktionen vorbereitet, welche im konkreten Anwendungsfall gar nicht benötigt werden und dementsprechend auch nicht getestet werden müssen. Darüber hinaus ist die Kategorie eines Softwaremoduls nur ein Aspekt der Komplexität. Etliche Standardprogramme für Messaufgaben sind darauf ausgelegt, nur in wenigen Parametern konfiguriert zu werden, gehören aber deshalb der Kategorie 4 an. Software für Maschinensteuerungen oder für ein SCADA-System kann derselben Kategorie zugeordnet werden, ist aber wegen der Vielzahl von abzubildenden Funktionen und Prozessen erheblich komplexer.

Eine effiziente risikobasierte Vorgehensweise fokussiert sich deshalb unabhängig von der Softwarekategorie auf die GxP-relevanten Funktionen des Produktes, welche die Software in der Produktion und in der Qualitätssicherung sicherstellen sollen. Sie leitet aus der Risikoanalyse die erforderlichen risikomindernden Validierungsmaßnahmen ab. Die Software-Kategorie einzelner Module ist dabei ein unterstützender Aspekt, um den Validierungsansatz zu systematisieren und anerkannte Validierungsmaßnahmen entsprechend der Kategorie zuzuordnen.

Je komplexer die zu untersuchenden Softwarearchitekturen dabei sind, desto bedeutsamer wird, zu Beginn der Risikobetrachtung das zu untersuchende System abzugrenzen und die Schnittstellen zwischen dem System und der Umgebung vollständig zu erfassen sowie zu beschreiben, siehe Beispiel in Bild 3

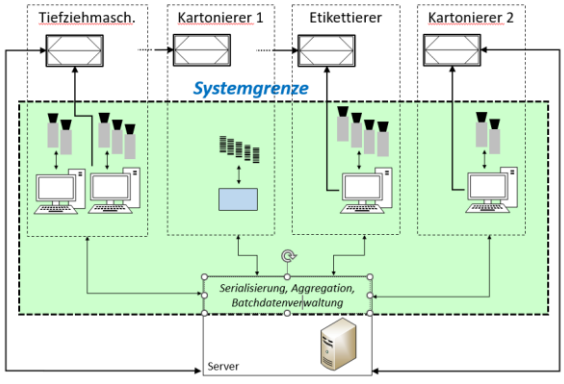

Bild 3: Systemgrenze eines aus mehreren Modulen bestehenden Systems zur Serialisierung, Aggregation und Batchdatenverwaltung.

Hinsichtlich der methodischen Vorgehensweise in der Risikobetrachtung haben sich u.a. Systematiken bewährt, welche im Sinne einer Gapanalyse die geforderten Inhalte des 21 CFR Part 11 [1] und darauf aufbauend des GAMP 5 [2] erfragen. Die Systematiken sollten so eingerichtet sein, dass nichtzutreffende Bereiche im Verlauf der Gapanalyse ausgegraut werden. Für das in Kap. 2.2 beschriebene zweite Beispiel ergäbe die Gapanalyse mit einer bei der Grünewald GmbH im Einsatz befindlichen CSV-Checkliste zu der Frage „Werden Fehlfunktionen, die während des Einsatzes des Systems auftreten, in allen Fällen in einem nachfolgenden Prozessschritt entdeckt?“, dass alle weiteren Fragen ausgegraut würden. Es erschiene der Hinweis „Jede Fehlfunktion des Systems wird entdeckt. Alle weiteren Fragen können entfallen, wenn sichergestellt ist, dass die Methoden zur Fehlerentdeckung valide sind. Es ist nur ein Systemsteckbrief zu erstellen.“

3 Spezifische Themen aus der CSV-Praxis

3.1 „Alte“ Steuerungen validieren

Vielerorts laufen langjährig im Einsatz befindliche Produktionsanlagen oder Testssysteme mit Steuerungssoftware auf veralteten Betriebssystemen. Da die Anlagen in der Regel stabil funktionieren und zudem eine technische Aufrüstung nur mit größerem Aufwand zu realisieren ist, empfiehlt es sich oftmals, die Anlagen in dem Zustand zu belassen, auch wenn heutige regulatorische Anforderungen nur teilweise erfüllt werden. Ein Beispiel wäre eine veraltete Benutzerverwaltung, welche mit „Administrator“ und „Operator“ nur 2 Benutzerebenen anstelle der Mindestanforderung von 3 Benutzerebenen zulässt oder aber nur über einen eingeschränkten Audittrail verfügt.

Eine risikobasierte Betrachtung des Herstell- und/oder Prüfprozesses kann für das Beibehalten des Status Quo die notwendige Begründung liefern. Bei langjährigem Einsatz sollten ausreichend Daten vorliegen, um aufgetretene Fehler zu GxP-relevanten Funktionen vollständig zu erfassen und deren Auftretenshäufigkeit bewerten zu können. Ergibt sich daraus, dass das Risiko entsprechend den firmeninternen Vorgaben zum Risikomanagement beherrscht wird, wie z.B. im o.g. Fall das Risiko eines unberechtigten Zugriffs auf Steuerungsparameter, dann sind keine weiteren Maßnahmen zur Risikominderung erforderlich.

3.2 Neuronale Netzwerke validieren

Neuronale Netzwerke werden auch in der Produktion und Qualitätssicherung von Medizinprodukten zunehmend eingesetzt. Es handelt sich um Strukturen, welche durch maschinengestützte Lernprozesse befähigt werden, Muster und Strukturen zu erkennen und daraus Entscheidungen abzuleiten. Ein typi-

sches Beispiel ist die automatisierte Erkennung visueller Defekte, wie Oberflächenveränderungen, Glasbruch oder Einschlüsse in Spritzgussteilen.

In der Regel handelt es sich um kundenspezifische Lösungen. Sie sind hinsichtlich Komplexität der Kategorie 5, siehe Kap. 2.3, zuzurechnen. Doch im Gegensatz zu herkömmlichen Softwarelösungen, deren Funktionalität im Source Code begründet ist, handelt es sich hierbei um Systeme, deren Eignung für die gewünschte Funktion durch den maschinellen Lernprozess hergestellt wird. Dies setzt in der Regel umfangreiche Datensätze mit entsprechenden Gut- und Schlechtmustern zum Anlernen voraus, die Güte des maschinellen Anlernprozesses bestimmt die Prozesseignung des neuronalen Netzwerks. Das System kann zu einem bestimmten Reifepunkt im Anlernprozess „eingefroren" werden oder so eingesetzt werden, dass es im Einsatz fortlaufend weiterlernt und seine Reife verbessert.

Bei der CSV von neuronalen Netzwerken sollten je nach GMP-Kritikalität des Systems zwei Aspekte im Fokus stehen.

Der erste Aspekt betrifft das Lieferantenmanagement. Es ist sich zu vergewissern, in wie weit der Lieferant die Fähigkeit besitzt, Systeme, welche auf neuronalen Netzwerkstrukturen basieren, zu entwickeln und maschinell anzulernen. Zu berücksichtigen ist dabei, wie der Lieferant sicherstellt, dass die Compliance-Anforderungen der Medizintechnikbranche nachweislich erfüllt werden.

Der zweite Aspekt betrifft das einzusetzende System an sich. Im Rahmen der CSV ist hier nachzuweisen, dass maschinelle Lernergebnis geeignet ist, dauerhaft und sicher die gewünschten Entscheidungen zu treffen. In der Regel erfolgt dies durch „Einfrieren" des angelernten Systems und Anwendung eines repräsentativen Mustersatzes aus Gut- und Schlechtteilen, welcher in dem Datensatz des Anlernprozesses nicht enthalten sein durfte.

Systeme mit neuronalen Netzwerkstrukturen, welche fortlaufend weiterlernen sollen, sind hinsichtlich CSV komplexer. Auch hier empfiehlt sich ein „Einfrieren" zu einem bestimmten Zeitpunkt und das Validieren dieses Zustandes mit einem Mustersatz. Ist die Eignung nachgewiesen, könnte man das maschinelle Lernen reaktivieren. Hier sollte allerdings anhand einer Risikobetrachtung eine Antwort darauf gefunden werden, wie hoch das Risiko ist, dass bei weiterem Anlernen die Prozessgüte negativ beeinflusst wird, wie z.B. durch eine veränderte Wichtung von Fehlerbildern durch deren Auftretenshäufigkeit. Schließlich ist auch zu klären, welche Gründe dafürsprechen, ein nachweislich geeignetes (validiertes) System weiter verbessern zu müssen. Wenn bisher die als Beispiel oben genannten visuellen Defekte sicher erkannt werden, ist erst einmal kein Anlass zu einer undefiniert verlaufenden Prozessverbesserung durch weiteres maschinelles Lernen gegeben. Umgekehrt müssen weiterlernende Systeme im Lebenszyklus regelmäßig einer Revalidierung unterworfen werden, um ihre Eignung fortlaufend nachzuweisen. Der Umfang der Revalidierungsmaßnahmen wird auch hier aus einer risikobasierten Betrachtung abgeleitet.

4 Fazit

Einer risikobasierten Betrachtungsweise kommt eine zentrale Bedeutung zu, will man effektiv und effizient in der Produktion eingesetzte Computersysteme und zugehörige Software validieren. Sie unterstützt dabei, an den GxP-relevanten Funktionen des Produktes orientiert die CSV-Kritikalität und die CSV-Komplexität der Systeme zu analysieren und auf die Bedeutung der Risiken abgestimmte Maßnahmen zur Risikominderung einzuleiten. Dazu zählen auch Maßnahmen zur Computersystem-Validierung, welche deren Eignung nachweisen.

Wesentlich ist bei der risikobasierten Betrachtungsweise auch, den größeren Systemzusammenhang zu sehen. Die CSV-Kritikalität eines Produktionssystems mag für sich betrachtet hoch sein. Wenn aber eventuelle Fehlteile nachfolgend identifiziert und ausgeschleust werden, bevor das Medizinprodukt zur Auslieferung kommt, kann das System in seiner CSV-Kritikalität heruntergestuft werden.

Die Güte einer risikobasierten Betrachtungsweise hängt auch von den fachlichen und methodischen Kompetenzen des involvierten Personenkreises ab. Während dies in fachlicher Hinsicht unbestritten ist, werden die methodischen Aspekte oftmals mehr oder weniger vernachlässigt. Die Folge sind hohe Streuungen in der Qualität der Risiko- und Validierungsdokumentation, welche nur durch entsprechende Qualifizierung und beständiges Anwenden verringert werden können.

5 Grünewald-Leistungen zur CSV

Die Grünewald GmbH kann auf eine langjährige Erfahrung in Compliance-Dienstleistungen zur Computersystem-Validierung zurückblicken. Zu den Leistungen zählen:

- Analyse des CSV-Bedarfs von Produktionsequipment: Wir analysieren Ihnen effizient CSV-Relevanz, CSV-Kritikalität und CSV-Komplexität Ihrer in der Produktion und Qualitätssicherung

eingesetzten Softwarelösungen und leiten daraus die erforderlichen Validierungsmaßnahmen ab. Dies kann entweder retrospektiv für bereits vorhandenes Equipment oder prospektiv für Neuinstallation durchgeführt werden. Das Ergebnis ist ein equipmentspezifischer Validierungsplan für CSV-Compliance.

- Validierungsprojekte CSV: Wir leiten und führen Projekte zur Computersystem-Validierung im Herstellbereich durch. Dies kann auch im Verbund mit der Qualifizierung und Validierung des Produktionsequipments (Hardware) erfolgen. Je nach Ergebnis einer Bestandsaufnahme können die Projekte auf Werkvertrags- oder Zeitvertragsbasis durchgeführt werden.
- Deckung einmalig anfallender CSV-Bedarfe: Für mittel- bis langfristig anfallende Bedarfsspitzen in der CSV stehen Ihnen unsere Spezialisten nach Klärung der terminlichen Verfügbarkeit zur Verfügung. Unsere Mitarbeiter sind mit den regulatorischen Anforderung an CSV vertraut und besitzen das fachliche und methodische Rüstzeug, um Sie zügig wirksam zu unterstützen.
- Konzeption von CSV-Prozeduren: Wir analysieren Ihren Bedarf an Entwicklung und Verbesserung von Prozessen zur Computersystem-Validierung und unterstützen Sie dabei, den Reifegrad dieser Prozesse zu erhöhen. Im Anschluss an eine Gapanalyse unterbreiten wir Ihnen einen Vorschlag für einen Projektplan, welcher mit Ihnen in Inhalt und Ausführung abgestimmt wird. Die vorgeschlagenen Maßnahmen sollen in Ihrem Hause eine breite Akzeptanz erfahren, es muss ein gelebtes System entstehen, welches von Ihnen anschließend selbstständig im Reifegrad weiterentwickelt werden kann.
- CSV-Schulungen: Wir bieten individuell auf Ihre Bedürfnisse angepasste Schulungen zu den CSV-Regularien und deren praktische Umsetzung an. Die Schulungen können entweder in unserem Hause oder bei Ihnen Vorort durchgeführt werden. Entsprechende, auf Ihre Anwendungsfälle abgestimmte Übungen sichern den Lernerfolg.

6 Literatur

Ref.	Titel
[1]	Code of Federal Regulations (CFR) Title 21 Part 11 “Electronic Records, Electronic Signatures”, Federal Register, Vol. 62 No. 54, 20.03.1997
[2]	GAMP 5 Guide: „A Risk-Based Approach to Compliant GxP Computerized Systems“, 2nd edition, Juli 2022
[3]	https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition
[4]	FDA 21 CFR §820.70 „Production and process controls”
[5]	“General Principles of Software Validation, Guidance for Industry and FDA Staff”, January 2002
[6]	“Computer Software Assurance for Production and Quality System Software”, Draft Guidance for Industry and Food and Drug Administration Staff, Entwurf September 2022
[7]	DIN EN ISO 13485 „Medizinprodukte – Qualitätsmanagementsysteme“, deutsche Fassung EN ISO 14971:2016
[8]	Blog „Wissenswert“ der Grünewald GmbH https://gruenewald-gmbh.de/risikomanagement-fuer-medizinprodukte-nach-iso-14971-wie-sinnvoll-ist-der-einsatz-der-fmea-methode/, April 2022

7 Autoren & Feedback

Dipl.-Ing. Martin Zierau ist Qualitätsmanagementbeauftragter und Senior Compliance Spezialist / Berater bei der Grünewald GmbH. Wir freuen uns über Ihr Feedback an martin.zierau@gruenewald-gmbh.de.