- 文書化：検証レポートに、“ 並列” 試験の結果をまとめる項を加え、結果が等しいことを示す試験の証拠を入れる。

教育訓練

- このシステムのユーザーがシステムの使用方法を完全に理解し、使用の適格性が確認されるよう教育訓練プログラムを作成する。
- ソフトウェアマネージャーは、これが、自動ソフトウェア試験システムが有効かつ安全に使用されるための最も重要な要素のひとつであると感じている。
- 文書化：検証レポートに、システムユーザーに必要な教育訓練の項を加える。

自動試験プロトコルの検証

- システム、ハードウェア、又はソフトウェアリスク/ハザードなどの軽減に設計されたソフトウェアの試験に自動試験システムを使用する場合、自動試験と手動試験の“ 並列” 試験を用いてこれらのプロトコルをひとつずつ検証する。
- 複雑度の低い最終試験に自動試験システムを使用する場合、予測可能なワークフローでこれらのプロトコルのひとつずつが自動試験と手動試験の“ 並列” 試験により検証されたことを確認する。
- 文書化：医療機器のソフトウェア検証レポートに、このカテゴリに該当する試験スクリプト/プロトコルの“ 並列” 試験の証拠を必ず入れる。

構成管理

- 適切で妥当性が確認された自動試験ソフトウェアの版のみをインストールし、使用するようにする。
- 納入業者が自動試験ソフトウェアの新版を作成した場合、新版又は変更の実施を制御し、適当な時期に導入するようにする。
- 自動試験システムの再検証をこれらのすべての更新時点で検討し、システムの再検証を実施、記録するようにする。
- 文書化：検証レポートに、このシステムの構成管理計画に関する項を追加する。

検証レポート

信頼確立活動の結果、ソフトウェアマネージャーは、最終審査及び承認のために検証レポートを提出する。検証レポートには、ソフトウェアマネージャーが自動試験システム使用の結果、開発中の医療機器が誤って故障するというシナリオが発生しないという結論に到達するために実施される付加価値活動の決定に至った思考過程が描かれ

ている。この報告書には、重要と判断される活動はすべて計画通り実施する証拠も含まれている。

検証レポートの内容

- プロセスの定義
- リスク分析
- リスクマネジメント
- 意図する使用
- 納入業者の適当な注意
- 教育訓練
- インストールテスト
- 自動試験システムの意図する使用の検証
- 保守、再検証及び構成管理

検証レポートの審査及び承認

ソフトウェアマネージャーは、プロジェクトマネージャー、プロジェクトソフトウェア品質保証マネージャー及び ソフトウェア試験マネージャーに検証レポートを回覧し、審査及び承認を受ける。

審査をした者はすべて、ソフトウェアマネージャーがこのシステムの意図する使用を明らかに熟慮し、使用によるすべてのリスクを理解していると感じた。審査をした者は、このシステムの使用に必要なレベルの信頼を確立するために必要な活動はすべて実施されたと感じた。審査をした者は計画を承認し、このシステムは“妥当性が確認された”と見なされ、使用された。

例 6：単純なスプレッドシート

背景

検査室の分析担当者らは、分析するすべての製品について文書管理システムから異なる規格のシートを出し、規格と比較する角度数を手で計算することにうんざりしていた。検査室の装置は、受け入れ検査に使用していた。この装置は 3 本の座標の位置を測定し、分析担当者はこれを使用して角度を計算し、仕様と比較した。最近、分析担当者が計算を間違えたことが 3 回あり（彼によれば、入力ミス）、この誤りの再発を防止したい。彼らは、角度計算のスプレッドシートを作成し、彼らが分析する 50 製品すべての仕様をこのスプレッドシート上で統合することにした。彼らが装置で測定した 3 組の座標を入力し、プルダウンメニューから製品名を選択すると合否の結果が出る。また、彼らは、座標を直接スプレッドシートに移す装置のインターフェースについても考えたが、インターフェースのコストにより、この計画の充実は来年に延期した。

プロセスの定義

現行のプロセスには次のステップがある。

1. 装置で部品を計測する。
2. 3 つの座標対を書き取る。
3. 角度を計算する。
4. 文書管理システムから部品の仕様を取り出す。
5. 角度の数値を仕様と比較し、合否を判定する。
6. 合格又は不合格シートを部品に添付し、製品部品の在庫に送る。

新しいプロセスには次のステップがある。

1. 文書管理システムからスプレッドシートを入手する。
2. 装置で部品を測定する。
3. 3 つの座標対をスプレッドシートに入力する。
4. 入力した座標対を装置の数値と目視的に照合する。
5. スプレッドシートの部品番号を選択する。
6. スプレッドシートの“結果を計算”ボタンを押す。
7. 正しい部品番号を選択したかを目視的に確認する。
8. 結果に基づき、合格又は不合格シートを部品に添付し、製品部品の在庫に送る。

意図する使用の定義

分析担当者は、スプレッドシートの目的と意図を次の通り定義する。

このスプレッドシートは、入力した3つの座標対を用いて角度を計算し、この角度を選択した製品の仕様と比較し、合否を報告する。

リスク分析

分析担当者は、スプレッドシートに関する潜在的なハザードについて考えた。彼らは、誤った結果により仕様を満たさない部品が製品に使用される可能性があると判断した。これらの部品が医療機器の最終ユーザーに到達するまでには少なくとも2回下流で故障が発生しなければならないが、最終ユーザーに対しわずかであるが可能性の低い危害のリスクがある。したがって、仕様を満たさない製品製造によるリスクは低い。しかし、不正な部品が生産に使用され、最初の小組立部品検査まで発見されないと、小組立部品を廃棄することになるため、製造コストが増加する大きなリスクがある。また、不合格という誤った結果が出たら、不良でない部品を廃棄する可能性もあり、廃棄コストも高くなる。したがって、ビジネス上の懸念に対処するため、スプレッドシートの設計、手順管理、文書審査及び検査という形で厳格さを加える。

検証プランニング

仕様外製品生産のリスクは低いため、この検証の取り組みのレベルは低くなる。分析担当者は、スプレッドシートの要求事項及び検証プランニングを同一文書に統合することに決定する。彼らは、設計文書を高レベルテスト計画と統合することも決定する。彼らは、全分析担当者チーム（4名）が品質保証の代表者とともにこれらの文書を審査する計画をする。また、彼らは、計算が意図した通りに機能するという信頼を確立するために、見本となる一組の検査データを作成するために技術専門家への相談を計画する。専門家はこの文書の承認も行う。

リスクコントロール手段

分析担当者は、誤りが生じた場合に不正な結果が発生しうる項目を見る。彼らは、各項目について、リスク軽減方法を特定した。

リスク	軽減方法
不正な数値を入力する。	手順制御で入力した各対の値を装置と照らし合わせて確認する。新プロセスにステップ 4 を追加してこれを行う。
計算が間違っている。	式が正しいかを確認し、意図した正確な結果を出す。
誤った製品が選択される。	手順制御で部品番号を確認する。新プロセスにステップ 7 を追加してこれを行う。
結果を示すマクロが間違っている。	マクロが正しく、意図した通りに作動するか確認する。
スプレッドシートの仕様が間違っている。	スプレッドシートの仕様を 50 個の製品の仕様シートと照らし合わせて確認する。仕様に変更があった場合、スプレッドシートの更新のために、仕様シート変更のプロセスを増加する（これが発生したことはないが、可能性はある）。
計算式又はマクロが検証後に変更される。	妥当性が確認された設定制御付スプレッドシートを文書管理システムにいれ、必要な場合に検索する。設定制御にはパスワード保護及びデータを入力しないすべてのセルのロックなどがある。

検証業務

使用する式は理解されており、開発者はスプレッドシートのマクロ開発の経験がある。

検証では次を確認する。

- 計算
- マクロ
- セルロック機能（ロックしたセルは変更できない）
- データ入力の確認（数値が許容範囲内、適切な製品選択、エラー通知メッセージ）

スプレッドシートはひとつずつ結果を出すため、負荷テスト又は性能テストは必要ない。ひとつのテスト計画及び報告ですべてのテストを実施する。この報告でスプレッドシートの使用を開始し、会社の文書管理システムにおけるスプレッドシートの制御を確認する。

導入

この新しいシステムを導入するには、検査を完了し、製造業者のオペレータの新しいビジョンシステム操作の適格性を確認する。

ツールボックスからのツール

要求事項の定義（検証プランニングに記録）

プロセス障害及びリスク分析（検証プランニングに記録）

意図する使用（検証プランニングに記録）

検証プランニング

テスト計画

オペレータの認証

保守計画（回帰分析が必要）

保守

製品の仕様変更時又は新製品の追加時には、必ずスプレッドシートの保守が必要である。保守検査計画は、新しい項目がスプレッドシートを破壊しないよう、完全な検証検査例の代表的なサブセットを使って作成する。保守計画には、変更したテストケースのサブセットにテストケースを追加する必要があるかをみるための回帰テストが必要である。この計画には、スプレッドシートの更新の仕方も含まれる（セルのロック解除、変更、再ロックなど）。

例 7:（あまり）単純（でない）スプレッドシート

ソフトウェアの記述

ソフトウェア開発チームが、クラス III の医療機器に使用されるメッセージ翻訳記録装置の開発にスプレッドシート Microsoft Excel を補助的に使用した。この装置は、最初に米国英語でリリースされた。その後は 7 カ国語でリリースする。このスプレッドシートには 7 列ある。左端の列は、この機器のすべてのメッセージの英語メッセージである。残りの列はそれぞれ支援する言語のひとつを表し、ある列の各行は、その行の左端の英語メッセージの各列の言語への翻訳を表している。

意図する使用

このスプレッドシートは、次の暫定的なニーズを満たす。

- メッセージとその翻訳を目視できるように編成する。
- 翻訳メッセージは、スプレッドシートに直接収集又はスプレッドシートのハードコピーに手書きで収集するために、各国の代表者に送付するスプレッドシートを作成する。
- 翻訳メッセージの暫定的なデータ保存ツールとなる。

翻訳を収集し、機器のソフトウェアに移動した後は、このスプレッドシートを保存又は保守する必要はない。このスプレッドシートには計算したセル又はマクロは入っていない。

適用範囲内であるか？

ここで Excel を使用するのは、回覧用情報の形式をそろえ、機器のメッセージの翻訳を収集するためである。一見、Excel とスプレッドシートの単純なアプリケーションに見え、検証は不要であると早急に結論を出したくなる。

この報告の“ 適用範囲内” の項では、次の質問を尋ねる。

> “ このソフトウェアの故障又は潜在的欠陥は、医療機器の安全性又は医療機器の品質に影響を与えるであろうか”

答えは明らかに“ はい” である。ソフトウェア/スプレッドシートが故障して、保管したメッセージの翻訳が破損する場合、その機器の安全に影響が出る可能性がある。我々は、この“ 単純なアプリケーション” の故障の可能性は低いが、820.70 規則の適用範囲内であると結論づける。

リスクアセスメント

機器のメッセージが正確に翻訳されず、ユーザーの混乱又はメッセージの誤解が生じれば、開発される医療機器を使用した患者に間接的な危害が及ぶ可能性がある。ソフトウェアの故障は検知可能であり、医療機器開発及び検証プロセスには、当該ソフトウェアの故障を検知し、修正するための照合の機会は多数ある。

医療機器のソフトウェアに影響を与えることが想定される故障モードは次の通りである。

- ファイル全体の紛失、個々のメッセージの紛失、メッセージの順序不正による文脈喪失又はランダムロス、文字の置換若しくは転位による個々のメッセージの破損により翻訳される英語メッセージが破損する。
- 地域事務所で準備及び採集した個々の言語の翻訳メッセージが破損する。破損は、ファイル全体の紛失、個々のメッセージの紛失、メッセージの順序不正による文脈喪失又はランダムロス、文字の置換若しくは転位による個々のメッセージの破損による場合がある。英語以外の言語では、フォントが Excel に適切にインストールされていない場合に破損する可能性もある。
- 各訳語が蓄積した結果、スプレッドシートに収集した結果が破損する。破損はファイル全体の紛失、個々のメッセージの紛失、メッセージの順序不正による文脈喪失又はランダムロス、文字の置換若しくは転位による個々のメッセージの破損による場合がある。スプレッドシートの行の順序の間違いに加え、列を間違える可能性もある。その言語のフォント又は文字で列に翻訳メッセージが表示されない場合、ソフトウェア技術者はメッセージをコードに変換したと誤解する。

検証プランニング

ソフトウェア開発技術者は、彼らの新しい医療機器のメッセージが間違っている場合の患者への潜在的リスクを認識した。ソフトウェアの故障の重大さは、高い可能性がある。スプレッドシート内のメッセージは正しい翻訳であるという信頼を獲得するために何らかの措置をとらなければならない。

一方、Excel は情報整理にのみ使用している。Excel をどんなに試験しても、メッセージを破損する故障が明らかになる可能性は低いと考えられる。技術者はこの点についてさらに考え、Excel の単純な応用よりもヒューマンエラーにより間違いが生じる可能性の方が非常に大きいと苦言を呈した。

技術者は、ヒューマンエラーについて考えていて、翻訳の収集方法又はヒューマンエラーの不在の検証方法について十分に定義したプロセスを実施していないことに気づ

いた。技術者は、翻訳メッセージの収集及び検証手順を手書きで作成した。その後、彼らは、彼らのプロセスの障害リスクは何か、それにソフトウェア（Excel スプレッドシート）がどのように関与しているか、そして最後に、スプレッドシートを含むプロセスを検証するために彼らに何ができるかを考えた。

リスクコントロール手段

翻訳収集プロセスの定義改良後、このプロセスからメッセージ翻訳に誤りが生じないよう、リスクコントロール手段が特定された。

翻訳収集プロセスを保護するリスクコントロール手段は、ソフトウェアがその意図する使用を逸脱しないようにも保護する。

- 地域事務所が翻訳を提供する場合は、紙媒体（ハードコピー）又はハードコピーと電子媒体で提供しなければならない。地域事務所が電子媒体で提供する場合、マスター翻訳スプレッドシートに転送する際に、スプレッドシートのデータをハードコピーに照らし合わせて検証（及び文書化）する。これにより、転送中のスプレッドシートの破損による結果の誤解又は、翻訳を提供するコンピュータと翻訳を受け取るコンピュータ間のフォントの違いによる結果の誤解を防止できる。
- すべての翻訳を収集し、マスタースプレッドシートに入れたら、確認及び承認のためハードコピーを各地域事務所に送付する。これにより、転送中のスプレッドシートの破損による結果の誤解又は、翻訳を提供するコンピュータと翻訳を受け取るコンピュータ間のフォントの違いによる結果の誤解を防止できる。
- すべての地域事務所、開発及び QA 承認者が承認後、マスタースプレッドシートのハードコピーは、医療機器のソフトウェア開発プロセスの入力になる。さらに、マスタースプレッドシートのハードコピーは、医療機器ソフトウェアの翻訳を検証するテストの予想結果として使用される。

検証業務

上述のリスクコントロール手段に加え、次の検証及び検証業務を完了し、ソフトウェアがその暫定的な意図する使用を適切に満たすことを保証しなければならない。

- 地域事務所から収集した各翻訳について、更新したマスタースプレッドシートのハードコピーを個々の翻訳スプレッドシートのハードコピーと照らし合わせて 1 行ごとに検証する。コンピュータプラットフォーム又はプリンタとのフォントの違いによる誤訳をすべて除外するために、必ずハードコピーとハードコピーを照合しなければならない。

- 版制御プロセスを詳細に文書化する。このプロセスは特に次の責任を負う。
  - 開発中に医療機器の機能性が変化する場合、メッセージ要求事項（英語）を変更
  - 翻訳の提供、地域事務所が更新したマスタースプレッドシートを審査及び修正した場合、マスター文書を変更
- これは非常に単純なスプレッドシートであるが、その使用により現実の版制御リスクがある。
- このスプレッドシートの設定には、スプレッドシート自体の版番号、使用したExcelの版番号、コンピュータプラットフォームの設定、及びスプレッドシートのハードコピー作成に使用したプリンタの設定を入れなければならない。Windows及びOfficeの設定及びプリンタファームウェアの版が異なれば、フォントが異なる場合があるため、これは重要である。翻訳が意図せず変更しないようにする唯一の方法は、スプレッドシート使用時には同一の設定を使用することである。
- 混乱を招く、調整されていない変更を防ぐために、スプレッドシートの設定（操作環境及びバージョニング）を制御する必要がある。設定変更の時期及び変更履歴の記録時期の決定に責任を負う担当者を一名任命した。
- 各スプレッドシートの版は、ハードコピー版で見ることができるようにする。
- 医療機器ソフトウェアの翻訳表には、ハードコピーマスタースプレッドシートのどの版を入力として翻訳したメッセージソフトウェアに使用したかが示されている。
- 個々の翻訳検証業務には次が含まれる。
  - スプレッドシートのマスターと翻訳版の英語メッセージの1行ごとの検証。これにより、地域事務所への転送時から地域事務所からの受領時までスプレッドシートのあらゆる破損（メッセージの破損又は紛失）が防止できる。
  - マスタースプレッドシートへの翻訳挿入（手動又はExcelのカット&ペースト機能使用のいずれか）後、改訂後のマスタースプレッドシートのハードコピーの1行ごとの検証を翻訳スプレッドシートのハードコピーと照らし合わせる。
  - 医療機器のソフトウェアのメッセージ実行をテストする場合、テストの手順には、マスタースプレッドシートの最新版のハードコピーを使用し（さらに版番号を参照し）、実行されたメッセージと意図したメッセージを比較しなければならない。

以上の検証業務はすべて、このプロセス及びExcelスプレッドシートの検証の客観的証拠として文書化し、収集する。

この検証アプローチは、ソフトウェアの入力と出力を 100%検証することになる。これ以上スプレッドシートのテストは計画しなかった。伝統的なテストはなかったが、技術者は、このプロセスに自信を持っており、この検証の論理的根拠は貴重な経験であったと感じた。彼らは、このソフトウェアの故障はすべて検知でき、彼らにはこのプロセスの適当な時点で収集及び記録したハードコピーを使用した回復経路があると結論づけた。ハードコピー及び1行ごとに検証した文書は、この活動の証拠文書となった。

保守

スプレッドシートは暫定的に必要なため使用した。スプレッドシートは、翻訳メッセージがコードに組み込まれたら廃用する。保守計画は作成していない。

考察

このスプレッドシートの意図する使用及び初回リスク分析は、スプレッドシートにさらに検証が必要かを決定するために重要であった。同じスプレッドシートでも、意図する使用状況が異なる場合、このスプレッドシートは低リスクで明らかに複雑性も低いという結論になった可能性がある。意図する使用が単に翻訳収集の進捗状況の追跡（スプレッドシートの翻訳を活動実施の設計に使用しない）であれば、医療機器の完全性に対するリスクはほとんどなく、事実、これはビジネス管理ツールであり、この規制の適応範囲に該当することもないと判断されたであろう。

このソフトウェアが“自動化している”“プロセス”は、医療機器用のデータ収集、書式設定、及びメッセージ翻訳の保管一部であった。これは、いくつかの観点から興味深い例である。

- 検証では、ソフトウェア使用の妥当性を確認するためのソフトウェアのテストの必要性があったとしても、非常に小さかった。ソフトウェア（Excel及びスプレッドシート）は、使用全般に対してではなく、この特定の使用について妥当性が確認されたことに注目することが重要である。チームは、テストによりこのソフトウェアの欠陥が明らかになる可能性は低いが、このソフトウェアが予想しない形で故障した場合に医療機器が脆弱になると感じた。
- 検証は、スプレッドシートの出力の100%検証であった。ハードコピー版を“黄金律”として頼った。これらは承認後にDHFで使用され、この後に発生したソフトウェアの故障は重要ではなかった。承認前のソフトウェアの故障はすべて、審査及び承認プロセスで検知されるであろう。
- この“プロセス”は、スプレッドシートソフトウェアのいかなる故障の影響も受けないよう修正された。

- 人的故障の可能性は、このアプリケーションにおけるソフトウェア故障の可能性よりも非常に大きかった（大きく見えた）。人間は、誤字、シートの間違った版の使用などをする可能性がある。この例における“ソフトウェア検証”により、プロセスがさらにヒューマンエラーの影響を受けにくくなった。
- この例は、日常的に使用するオフィス生産性ツールでさえもいかに構成管理が重要かを強調している。

注 – これは、あまりうまく処理されなかった実例にもとづいている。事実、スプレッドシートのバージョニングにヒューマンエラーがあった。予期せず、複数の PC の Excel 設定が異なり、それに連動したフォントの版が問題となり、ハードコピーの結果が同一にならなかった（プリンタのフォントもプリンタが異なると問題になりうる）。検証は不要であるとほとんど看過される一見単純なスプレッドシートが、実際には、メッセージ翻訳の破損で問題となった。

例 8：パラメトリック滅菌装置

メアリーは、彼女の勤めるオールウェイズセーフ・メディカルデバイスカンパニー 用にカスタム開発される新しい自動滅菌システムの検証の取り組みを率いる業務を行ってきた。

プロセスの定義

メアリーは、まず、彼女の会社の工場に導入しようとしているこの 100%ETO（エチレンオキサイド）滅菌プロセスについて彼女が知っていることの定義及び文書化を開始する。

- 医療機器を手動で滅菌装置に入れる。
- シリアルナンバー、バッチ情報及び滅菌サイクル情報を DHR に転送する。
- このプロセスには、パラメトリックリリースのための滅菌サイクル変数評価が含まれている。
- 自動滅菌システムのソフトウェアは、滅菌サイクル活動を制御する。
- サイクル完了後、医療機器を手動で取り出し、脱気室に移動する。

プロセスリスクの分析

メアリーは、このプロセスのリスクを非常に懸念している。このプロセスが故障すれば、次のような重大な結果が生じうる。

1. 医療機器の滅菌不良。この故障の結果、未滅菌製品の使用による感染症のため、重大な損傷又は死亡が発生する可能性がある。
2. 医療機器の履歴情報及び製品のトレーサビリティ紛失。
3. 製造施設若しくは環境、又はその両方への有害化学物質の放出。この故障の結果、滅菌装置のオペレータ又は近隣住民の重大な損傷又は死亡が発生する可能性がある。

そこで、メアリーは、このようなリスクを軽減するためにどのリスクコントロール手段を設定し、検証しなければならないかを考える。メアリーは、正確な温度及び相対湿度で適量のガスが、適当な時間使用されるパラメトリック滅菌技法を使用して、リスクを制御できると考えた。さらに、滅菌装置のデータの適切なパラメトリック値を手動で確認して、独自に滅菌が十分であるかを確認する。最後に、彼女は、施設への化学物質の漏れを制御するために、二重安全装置のシャットダウン及び密封構造を採用しなければならないと考えた。

これらのリスクコントロールを実施しても、複数のシステム故障が同時に発生し、医療機器が滅菌されない可能性がある。しかし、これが発生した場合の影響は大きいため、メアリーはこのプロセスの残留リスクは高いと考える。彼女は、このリスクは大きなリスクに変わるため、厳格な検証が適当と考える。

ソフトウェアの目的と意図の定義

メアリーは、このシステムでソフトウェアをどのように使用するのかを詳しく理解したい。まず、彼女は、このソフトウェアが何をすべきかを考える。この場合、ソフトウェアは、DHR に入力する情報の記録及びパラメトリックリリースのための滅菌値の分析など、100% ETO 滅菌槽を用いた医療機器滅菌プロセスを制御する。この新しい滅菌装置は、現行のシステムより大きなバッチを収容できるために購入した。この点は、現在の製品の需要を満たすためには非常に重要である。滅菌のオペレータが QA とともにこのシステムを使用し、医療機器のリリースの受容可能性を判定する。メアリーは、これは、滅菌サイクル中の滅菌槽のリアルタイム制御及び監視並びにデータベースへの情報保管を通じて実行されることを理解する。メアリーは、このシステムが滅菌施設の中に設置され、システムに必要な保守のために使用しないのは通常週 1 日だと知り喜んでいる。

メアリーは、このソフトウェアは、医療機器を手動で滅菌槽に入れる点から手動で滅菌槽から取り出す点までのすべての側面を自動化すると判断する。

メアリーは、目的と意図を次の通り記録する。

この滅菌ソフトウェアは、滅菌プロセスを制御及び監視し、データをプロセスから滅菌済み医療機器の DHR へ転送し、パラメトリックリリースの滅菌サイクル変数を評価する。

検証プランニング

ここで、メアリーは、ソフトウェアが何をするのかを理解したため、高レベルの検証プランニングを作成する準備が整った。彼女は、後で詳細を付け加える必要があることを知っているが、今、検証プランニングを開始し、十分に情報を得た状態でソフトウェアの障害リスクを特定し、それを使用して計画を完了したい。

初期に高い残留リスクが特定されたため、メアリーは検証の取り組みにおいて詳細及び形式を準備する必要があると考える。彼女は、詳細の文書化には高レベルの厳格さを適用し、小規模の取り組みでよくあるように文書を統合するのではなく、ほとんどの文書を独立した文書にしたいと考える。このシステムは高リスクであるため、医療機器のソフトウェア開発と同程度の厳格さで開発することを決定する。その結果、彼

女は、ライフサイクル制御法として、医療機器のソフトウェアに、つまりソフトウェアライフサイクルプロセス（IEC 62304:2006）に従うことを決定し、ソフトウェアリスクマネジメントの指針としてAAMI TIR32：医療機器ソフトウェアリスクマネジメントを参照する。さらに、開発の取り組みにソフトウェア障害の木分析の適用を決定し、すべての危害の原因を考慮するようにする。また、彼女は、ユーザービジネスプロセス要求事項及びソフトウェア要求事項を正式に定義及び文書化することも決定する。特に懸念となる機能は特別に識別する。さらにメアリーは正式なソフトウェア要求事項の審査も計画する。QA、滅菌技術者及び滅菌マネージャーの承認が必要である。このシステムの重大度及びリスクから考えて、検証レポートの最終承認には、上級管理職のメンバーも加える。

ソフトウェア要求事項の定義

ここでメアリーは、ソフトウェア要求事項の定義を作成する。彼女は、ソフトウェア要求事項では、警告、エラーの取り扱い及びメッセージ、変数設定の確認、DHR システムのインターフェース、センサー制御及び監視、動作制御及び監視を取り扱わなければならないと決定する。

このシステムは電子データを管理するため、メアリーは、21 CFR 11 の文言から標準的要求事項文書も含める。

信頼の確立及びソフトウェアの制御

すべてを内部で実施するために納入業者の活動が発生する必要がないため、オールウェイズセーフの内部開発制御手順をもとに、メアリーは開発ライフサイクルを通じて内部制御を使用する。

ソフトウェアと他のシステムとの境界の定義

メアリーは、次に、他にどのシステムが新しい滅菌装置とインターフェースする必要があるかを考える。彼女は、唯一のインターフェースは、滅菌サイクル中に発生したデータを保管するオールウェイズセーフの既存の DHR データベースシステムであると判断する。

ソフトウェアの障害リスク分析

メアリーは、既に自動化するビジネスプロセスは高リスクであると判断したが、まだ、ソフトウェアの障害のリスクを分析する必要がある。メアリーは、AAMI TIR を参照

してこの活動に定量的リスクモデルを選択する。彼女は新しいシステムに次の通り順位をつけた。

- このシステムの障害により死亡又は重大な損傷が生じうるため、メアリーは“重大さ”を高い（10）と評価する。
- ソフトウェア自体が滅菌の受容可能性を決定しているため、ソフトウェア自体の障害が危害をもたらす可能性があり、彼女は“可能性”を高い（10）と評価する。
- 彼女はリスクスコアを20と計算し、これは高リスクに分類される。

高リスク分類には、厳格な検証方法が適用される。滅菌装置自体が医療機器であるかのように厳格かつ包括的にこの方法を遵守する。

この自動システムの残留リスクは、軽減により合理的に達成可能なできるだけ低い（ALARP）。このシステムによる危害の重大さにより、滅菌は本質的に高リスクのプロセスである。AAMI TIR 32を使用したリスクに関する追加活動も実施する。

検証プランニングの終了

ここで、メアリーはソフトウェア要求事項の定義を完了し、実施アプローチを決定し、ソフトウェアのリスクを分析したため、検証プランニング終了に十分な情報を得ている。

検証プランニングの初稿で、メアリーは既にリスクマネジメントに対する厳格なアプローチを採用すべきと決定し、既に検証の取り組みを高度に正式な方法で取り扱う計画を立てていた。

したがって、彼女は使用予定のAAMI TIR32:2004で特定されるリスクマネジメントツールを説明する。

リスクマネジメントツール

- ソフトウェア障害の木分析
- リスクマネジメント計画
- 製造/ビジネスプロセスにおけるリスクコントロール手段の特定
- ソフトウェアの障害分析（リスク分析）

メアリーは、次に、ソフトウェアの設計、開発及び設定段階でどのようにソフトウェアに対する信頼を確立するかを考える。彼女は、既に、ライフサイクル制御にIEC 62304規格の採用を決定している。彼女はここで、このソフトウェアが設計、開発及び設定段階で適切に開発されたことを示す他の関連するツールを特定する。

設計、開発及び設定ツール

- IEC 62304：2006
- アーキテクチャの文書化及び審査
- 設計仕様
- ソフトウェアの詳細の設計及び審査
- ソフトウェアコーディング規約
- トレーサビリティマトリックス
- ソフトウェアシステム設計におけるリスクコントロール手段の特定
- コード審査/コード検証
- 開発及び設計審査

メアリーは、この新しいシステムを広範に検査する必要があると確信している。まず、彼女は、通常の単体テスト、統合テスト及びインターフェーステスト活動以外に正式な試験計画活動が必要と判断する。しかし、このシステムは、最終医療機器をリアルタイムでリリースするため、負荷テスト、性能テスト、及び入力テストを広範に組み合わせて可能な限り多くの操作状況を作り出して、システムの制限を広げなければならないと判断する。

検査ツール

- テスト計画
- 単体テスト
- 統合テスト
- インターフェーステスト
- 回帰テスト（必要な場合）
- ソフトウェアシステムテスト
- 頑健性（負荷）テスト
- 入力テストの組み合わせ
- 性能テスト

最後に、このシステムは、生産環境において完全に実施されるまで完了しないため、メアリーは、導入段階で検討したい検証活動に関心を移す。彼女は、システムの適切な文書化及びユーザーに対する正確な使用についての十分な教育訓練を確実にしたい。また、システムを意図通りに確実に設置したい。そこで、彼女は導入段階の検証プランニングに次の計画を追加する。

導入ツール

- 使用手順の審査
- 内部教育訓練
- 据付時適格性確認
- 操作及び性能の適格性確認
- オペレータの認証

保守計画

メアリーは、残留リスクリスクが高いため、保守について懸念している。彼女は、システム導入以後にソフトウェアの品質を保証するために、ユーザーの教育訓練、システム監視手法、システム出力の正確さの確認及び欠陥の報告の評価などいくつかの保守活動を計画する。また、彼女は、ソフトウェア保守活動に加え、校正など、ハードウェアの保守活動が実施されていることを確認する。

廃用活動

旧システムで作成したデータを DHR 用に記録保管する必要があるが、新しい形式とは互換性がなかったため、メアリーは旧システムの廃用に苦労した。このシステムは、普遍的なデータ形式を採用しており、新システムへの世代交代時に残存データの移動を柔軟に実施できる。

例 9：不適合材料報告システム（NCMRS）– システム全体のアップグレード

アドバンスドメディカルスペシャリティーズコーポレーション（架空の企業）は、不適合材料報告システム（NCMRS）のソフトウェアをアップグレードしている。これは市販のソフトウェア部品ケージであるが、アドバンスドメディカルは、過去の大規模なリリース時にアップグレード をしなかったため、大規模なリリース 2 回分の遅れがある。この会社では現在第 2 版を使用しているが、最新の第 4 版がリリースされている。現行のソフトウェア保守契約を維持するために、アドバンスドメディカルはアップグレードしなければならない。NCMRS-Pro（ソフトウェア）の第 4 版は、現在使用している V2 に比べ大きく変化している。特に、その製品は、通常のクライアント/サーバーアプリケーションからウェブベースのアプリケーションにプラットフォームを変更した。新しいソフトウェアには重大な特性及び機能も入っている。ビジネスプロセスオーナー兼プロジェクトマネージャーはフランクである。フランクは、既存のソフトウェア及びプロセスについて、新しい要求事項はないが、新しいソフトウェアの特性を利用したいと考えている。

フランクは、規制グループに相談し、ERP システムと NCMRS システム間の現行のインターフェースには変更がなく、そのままであると判断したが、新版では ERP システムにデータを書き戻すことができ、この拡大インターフェースを検証時に詳細に調べなければならないと認識する。フランク、製造品質技術者及び規制チームが検証の取り組みの適用範囲決定を検討し始める。

プロセスの定義

フランクは、現行の手動プロセスを分析し、新しいソフトウェアによりワークフローのどの要素を自動化するかを決定する。

1) 不適合材料又は製品が発生する可能性を認識（適用範囲外）
2) 不適合材料及びその発見にまつわる状況に関する情報を入力（適用範囲内）
3) その材料の適切な識別、評価、調査及び処分を可能にする情報の経路選択（適用範囲内）
4) 重要な利害関係者並びに財務、購入、計画及び日程計画を適切に取り扱うための他のコンピュータシステムに情報を伝達（適用範囲内）.
5) その材料の物理的処分（適用範囲外）。ただし、処分に関するデータはこのシステムに記録する。

プロセスリスクの分析

フランクは、このプロセス及び補助となるソフトウェア にリスクがあると気づいている。このプロセスで故障が発生すれば、次のような深刻な結果が生じる可能性がある。

- 不注意により不適合材料が製造フロアにリリースされる。
- 不注意により不適合材料が市場にリリースされる。
- スクラップ、作り直しなどによりコスト又は製造が増加するなど。

フランクとチームは、以上のリスクを軽減するためにどのリスクコントロール手段が実施されているかを考える。

- 不適合材料の検知、隔離、制御及び修正の手順制御
- プロセスが適切に制御されていない可能性があるという開発の傾向を特定するための、SPC データ及びその他の手段の管理及び品質審査
- 手順の遵守に関するオペレータの継続的訓練
- 製造プロセス特有でない問題があることを示す材料の使用を特定するための財務報告書

以上のリスクコントロールを実施しても、複数のシステム障害が同時に発生すると、不適合材料又は製品を適切に制御できなくなる。しかし、この種類の障害が発生した場合、品質、規制及び財政上の影響が出る可能性があるため、フランクは、プロセスリスクのために厳格な信頼確立活動を実施し、ソフトウェアの正確な作動及び意図する使用の適合を確実にする必要があると判断する。

ソフトウェアの目的と意図の定義

フランクは、ソフトウェアのアップグレードがどのように彼の会社のユーザー及び組織に影響を与えるかについて詳細に理解したい。フランクは、このソフトウェアは基本的には自動問題追跡及び管理ツールだと結論づける。規格のツール、装置及びその他の手段を用いて業務を行う製造要員は、不適合材料及び製品を認識し、隔離する責任を負う。問題が認識されたら、その状況の詳細をソフトウェアに入力する。次に、ソフトウェアは、ワークフロー、割り当て及び通知を管理し問題を解決し、材料及び製品の処分に必要な様々な活動を記録する。ソフトウェアのアップグレードは、このプロセスを簡素化、効率化するとともに、品質チームに対しより強力なデータ分析及び動向のツールを提供し、品質の問題を見極められるようにしなければならない。フランクは、アップグレードが必要なプロセスの変更は主にワークフロー及び情報伝達であると理解する。ソフトウェア自体は財務上の決定を行わず、他の結果を独自で決定しないが、システムと相互にかかわる人間による決定を受け、記録する。