リスク予防策

リスク番号	説明	重大性	予防策	残留リスク
リスク#1		• 高レベル • 中レベル • 低レベル		備考参照
リスク#2		• 高レベル • 中レベル • 低レベル		
リスク#3		• 高レベル • 中レベル • 低レベル		
リスク#4		• 高レベル • 中レベル • 低レベル		
リスク#5		• 高レベル • 中レベル • 低レベル		
リスク#6		• 高レベル • 中レベル • 低レベル		
・ ・ ・ ・		• 高レベル • 中レベル • 低レベル		
リスク#n		• 高レベル • 中レベル • 低レベル		

備考 ― すべてのリスクは最終的に制御され、“許容可能な”レベルに緩和されなければならない。

付録 C
例

この TIR は、品質システムのほか、規制当局への提出、品質システム、生産、及び自動データ処理を意図するデータの作成、測定、評価、又は管理などの生産プロセスの部分を自動化するためのソフトウェアに適用される。その他の意図する使用の例として、自動化された機器からのデータの直接的又は間接的な収集、自動化された機器の操作/制御、及びデータの処理、レポート作成及び保管が挙げられる。これらのさまざまな活動のために、プログラマブルロジックコントローラ（PLC）又はパーソナルコンピュータ（PC）、実験情報管理システム（LIMS）に至るまで、複数の機能を備えた各種のソフトウェアが用意されている。意図する使用の例として、以下のものが挙げられる。

- 製品の合格/不合格を判定するソフトウェア
- 品質システム内でカスタム記録を保存するためのソフトウェア
- 製品サブミッション用のデータ処理・解析ソフトウェア
- 規制当局へのレポート作成用のデータ処理・解析ソフトウェア
- 品質に関する記録を保存するデータベースの記録を作成・修正する規制対象外のソフトウェア
- 規制プロセス用ソフトウェア用のソフトウェア開発ツール又はコンパイラ
- 生命に関わる重要なソフトウェアの認定及び検証の責任を担うソフトウェアツール又は下位ソフトウェアツール
- 品質システム内のコンポーネント、製品、又は患者のトレーサビリティ用ソフトウェア
- 上記の目的で使用される“系統不明のソフトウェア”（ソフトウェアのクオリティ及びロバスト性が不明のもの）

この付録に掲載された例は、医療機器製造業者が遭遇するであろうソフトウェアの実際的かつ現実的な例を提供したいと考えるこのレポートの執筆陣の努力の成果である。作業部会は、これらの例を提示することが、批判的思考のアプローチを体験し、ソフトウェアのタイプ、ソフトウェアのリスク、及び意図する使用の多様性を理解する上で最良の方法であるという意見に賛同する。

注意事項：

- ここで紹介する例は、ソフトウェアが意図した通りに機能するという付加価値と信頼をもたらす検証努力及び厳密さの許容レベルに関するこのTIRの執筆陣の総意を示すものである。この TIR のユーザーには、エンジニアリングの観点から、どんな活動と

努力のレベルが有効かを検討し、規制プロセス用ソフトウェアの主な要因に基づき、要求される厳密性を判定することが強く推奨される。

- 検証努力の妥当性への信頼を確立する方法は常に一つ以上存在する。この TIR で紹介する例は、現時点での考え方と経験に基づく方法ベースのアプローチをもたらしてくれる。
- この TIR のユーザーには、執筆陣の努力を権威的又は規範的なものとして見ないようにすることが強く推奨される。ここで紹介する例は、データの見せ方に関してのみフォーマットが類似しており、批判的思考の応用をデモンストレーションするための主な思考プロセスを網羅している。このレイアウトは、検証のテンプレートとしての使用を意図するものではなく、実際の検証書類に期待されるであろう深みと詳細を含むものでもない。
- ここで紹介する例は、この文書のセクション6で特定された必須プロセスが提示され、正常に機能する状態にあるものと仮定している。例中には必須プロセスの詳細なリファレンスを記載していないが、ソフトウェア及びそれに関連する文書作成や他のインフラなどの部分が変更管理の対象になることを保証するために、これらのプロセスを実施しなければならない。
- 各例の冒頭では、自動化するプロセスの明確な定義を行う。従って、プロセス及びソフトウェアが適用範囲内のものであることは既に決定されている。次に批判的思考の活動を特定し、その概要を作成する。
- ここで紹介する例は、批判的思考のプロセスで使われる決定事項及び決定推進要因に関する情報提供を目的としており、検討中のソフトウェアの包括的な検証を示すものではない。
- ここで紹介する例は、概して、特定のシステムを検証された状態にすることを主旨としている。システムの検証された状態を確立することは非常に重要だが、システムの保守段階で検証された状態を維持し、ソフトウェア及び周辺プロセスの適切なオペレーションを確保することも重要である。保守活動には、初回の検証活動と同じコントロール及び批判的思考が要求される。

例 1：製造装置用プログラマブルロジックコントローラ（PLC）

背景

チュービングサプライカンパニーは主要医療機器製造業者に静脈内投与システム用チューブを供給する契約をしている。この会社は、チューブの特許を取得した形状に形成する要求事項を含むチューブ形成の仕様書を受け取っている。この特殊チューブ形成の要求事項は、チューブ部分の製造工程の一部としてチュービングサプライカンパニーが実施する。

この供給業者は現在このチューブ形成工程を実施する機械を所有していないため、特にこのプロセスに関心がある。この業務を遂行するために、プログラマブルロジックコントローラ（PLC）付のカスタム装置の開発を決定した。医療機器会社の方針に従い、この装置及び内蔵の PCL の意図する仕様の妥当性を確認しなければならない。

プロセスの定義

チュービングサプライカンパニー及び医療機器の製造業者は、チューブの形成プロセスを決定するために会議を行った。会議では、次のプロセスを定義した。

このプロセスでは、プラスチック製チューブに形成を施す温度及び圧力を使用する。このプロセスには次が含まれる。

1. 材料を得る
2. 機械に挿入する
3. 圧力及び熱でチューブを正確な直径に形成する
4. チューブを冷却する
5. 機械からチューブを取り出す
6. 正確な直径を計測する

プロセスリスクの分析

医療機器製造業者は、チュービングサプライカンパニーにリスク分析プロセスで以下の問題及びそれに関連するハザードが判明したことを連絡した。

- 輸液バッグの接続不良のため漏れが生じる。漏れは危険ではないが、介護人が滑るリスクがある。漏れにより治療が遅延する可能性もある。
- 外見上の問題が顧客の受け入れに影響し、治療が遅延する可能性がある。
- チューブ形成プロセスでオペレータが熱傷を負う可能性がある。

ハザード、介護者の滑り、治療の遅延及びオペレータの熱傷のため、軽減前の製品の故障によるリスクは中レベルである。

現在は、次のプロセスリスクコントロール手段を実施している。

- 上流の業務には、チューブが使用に耐えられるかを調べる受け入れ検査及びラインのクリアランスなどがある。
- 下流の検証確認には、装置の誤りを軽減する漏れ検査、工程内検査及び取り付け検査などがある。
- オペレータの負傷を防止する、シールド、独立した温度センサー及び冷却剤噴霧器が設置してある。

この情報を用いて、供給業者は医療機器製造業者と協力し、チューブ形成プロセスの結果生じるチューブ故障の残留リスクは低いと結論づける。

ソフトウェアの目的及び意図の定義

チュービングサプライカンパニーは、ソフトウェアの意図する使用の妥当性を確認するために、意図する使用を定義しなければならないことを知っている。装置が何をするはずであるかについて合意に至るために、チームは一連の質問事項について考え、このシステムの目的及び意図について簡潔であるが使用可能な定義を決定した。最終的に、このチームは次の文章を作成した。

このソフトウェア制御装置は、定義されたプロセスの 2〜6 ステップの自動化を目的とする。このシステムは、施設 B の製造ライン 3 における PN 001 製造での使用を意図する。このシステムは、一般的、無害の溶液送達用の静脈内投与チューブの挿入、形成、除去及び測定を自動化する。

検証プランニング

検証プランニングの第 1 段階は、成果物の厳密さ及び審査の決定である。残留プロセスリスクは低いと決定されたため、次のアプローチをとった。

文書の厳密さ

- このプロジェクトの文書化の厳密さは中等度である。つまり、このケースにおいては成果物が統合される場合があり、実施前に設計を詳細な設計仕様にしない。

検査のレベル

- このプロセスの開発及び実施に責任を有する者（チュービングサプライカンパニーの担当者）及び独立した品質に関する役割を担う者（医療機器会社の担当者）が成果物を審査し、承認する。

- PLC コード並びにあらゆる仕様及び設計を、文書制御システム又は構成制御システムなどの正式な構成管理に入れる。

システムの定義

- プロセス要求事項を作成する。これには、この装置に期待される入力及び出力を含む装置の機能の詳細が記載されたシステム要求事項の仕様を含む（例えば、機能する装置全体の設計制御要素）。
- このグループは、オペレータの観点からシステムを使用するためのオペレータマニュアルを作成する。これに加え、ソフトウェア要求事項を作成し、ソフトウェアの設計を取り扱うのに十分な論理的な機能フローを入れる。

ソフトウェアに対する信頼と制御の確立

チュービングサプライカンパニー又は医療機器製造業者のいずれも、過去にこの PLC プログラミング部品ケージを使用したことはない。この納入業者には、このソフトウェアの能力について信頼を確立できるような経歴がない。しかし、要求事項の審査、構成制御及び試験プロトコルを通じたシステム機能の試験により PCL のプログラミングを制御できる。

ソフトウェアと他のシステムの境界の定義

この装置では PLC が唯一のソフトウェアである。この装置は、他のシステムには接続していない。

ソフトウェアのリスク分析

ソフトウェアが故障し、不適切な形状のチューブが製造ラインに流れたために漏れが生じ、介護者が滑る可能性がある。また、誤作動により過度の熱が発生し、オペレータが熱傷を負う可能性もある。このソフトウェア自体は、まだプロセスリスク分析で把握されていない新たな製品リスクをもたらすわけではない。したがって、グループは、現行の下流プロセスを維持し、ソフトウェアの故障に関するリスク軽減には現行の下流プロセスで十分であると決定する。

検証プランニングの終了

ここで、このグループはソフトウェア及びその使用について十分に理解を深めたので、検証プランニングを終了する。

インプリメンテーションツール

- 装置内には一連のプログラム可能な変数（時間、温度及び圧力）がある。装置内のこれらの変数の好ましい設定及び範囲はすべてソフトウェア要求事項に入っている。したがって、設計の目的にはこの SRS で十分であり、設計活動及び文書化の追加は必要ない。
- このグループは、ソフトウェア要求事項及びそれに関連する試験の間のトレーサビリティマトリックス作成し、トレーサビリティ分析を実施してトレーサビリティを完了する。

試験ツール

- ソフトウェア要求事項及びオペレータマニュアルに基づきソフトウェアシステムを試験する。
- 必要な場合、回帰テストを実施する。

導入ツール

- このシステムのオペレータ及び技術者が作業指示書の明りょう性及び使い勝手を審査する。
- この装置の使用にはオペレータの認証が必要である。

検証プランニングを完了し、その活動を実施した後には、チームはこのシステムが好ましく、かつ定められた出力を一定して支給することに安心していられる。

保守の考慮事項

このプロセスの何らかの部分の変更を考慮する場合、又はソフトウェアの意図する使用が変更される場合、現在の軽減に対する影響はあるか、又は変更により新しいリスクが生じるかを判定するために分析を実施しなければならない。この分析にはチューブ形成装置に関するソフトウェアのリスクの審査も含まれる。

ツールボックスの使用

ツールボックスから次のツールを使用した。

- 開発－定義
  - プロセス要求事項の定義
  - プロセス障害リスク分析
  - 意図する使用
  - 検証プランニング

  - ソフトウェア要求事項の定義
  - 製造プロセス内のリスクコントロール手段の特定
- 開発－インプリメンテーション
  - ソフトウェア故障分析
  - トレーサビリティ分析
- 開発－試験
  - ソフトウェアシステム試験
  - 回帰テスト
- 開発－導入
  - ユーザー手順の審査
  - オペレータの認証

例 2：自動溶接システム

デイブは、新しい製造ラインの全システムについての検証チームの一員である。彼の仕事は、ケースカバーの溶接機の検証である。彼は、このプロジェクトのプロジェクトマネージャーである。

プロセスの記述

チームは、新しい製造ラインを誰が開発し、誰がどの部品の妥当性を確認するかについて長時間議論する。デイブが部品を受け取った時には、既に部品には印がつけられており、材料はすべて検査及び認証を受けていた。部品は上流の妥当性が確認されたシステムによる試験を受けていた。溶接機の据え付けには 3 つのステップがある。

1. 機械のスイッチを入れる。
2. 部品にバーコードを入れ稼働する。
3. 製造実行システムから部品用プログラムを取る。
4. 装置のマスター記録に照らし合わせてプログラムの版が正確であることを確認する。

ケースカバーの溶接工程には 10 のステップがある。

1. ドアが開く。
2. 部品を搭載する。
3. ドアを閉める。
4. プログラムを開始する。
5. ビジョンシステムが開始点を割り出す。
6. レーザーのスイッチを入れる。
7. 動作制御で部品を移動する– 溶接する。
8. レーザーのスイッチを切る。
9. ドアが開く。
10. 部品を取り出す。

このプロセス終了後に、部品はデイブの管轄外のシステムに移動する。彼は、下流の活動には溶込みの破壊試験、缶の高さ検査、ハーメチックシールの漏れ検査などがあることを知っている。

意図する使用の定義

デイブは、自分のソフトウェアの意図する使用を定義するために情報を収集する。彼は、オペレータの安全を守り、一定した溶込みを得るには、このプロセスにおけるビジョンの精確さ、動作、電力及びスピードが重要だと知っている。

デイブは、まずソフトウェアの目的と意図から開始して、彼の意図する使用を定義する。

ソフトウェアの目的は、作動しているレーザーとの直接接触から機械のオペレータを保護しながらケースカバーを溶接することである。これには、上述のプロセスの記述のステップ 5～8 が含まれる。

リスク分析

デイブは、このプロセスからヒューマンエラーをなくしたいと考えており、レーザー、サーボ及びビジョンの制御がこのプロセスの重要な要素であると知っている。ソフトウェアは、まず、ドアが閉まっているかを確認する。安全上の理由から、ソフトウェアは、ドアが閉まっていることを感知したいと開始しない。ソフトウェアは、レーザーのスイッチが切れていることを確認し、ドアを開けた後に終了する。緊急停止又は予期せずドアが開いた場合、レーザーへの電力が切断する。彼は、このプロセスで得た情報及び溶接が一部であるプロセスの設計の一部として実施された設計リスクマネジメント活動からの情報を使用する。彼は、FMEA を参照し、重要な部品の変数、ハーメチックシール及びユーザーインターフェースの 3 領域に注目する。デイブは、このプロセスに関して多数のハザードを特定した。まず、オペレータはレーザーに接触して熱傷を負う可能性があった。この製品に関しては、このプロセスで不適切な溶接により不良製品が生産され、漏れが生じ、また最終ユーザーが負傷する可能性があった。デイブはこのプロセスのリスクは高いと判断した。

検証プランニング

デイブはツールボックスの定義ツールを見て、このプロジェクトにはソフトウェア要求事項の定義及び保守文書の作成が必要と判断する。彼のソフトウェア要求事項には、ツール用の設定変数、レーザー照射時間及び電力調整が含まれなければならない。また、ソフトウェア とハードウェアのインターフェースも定義しなければならない。特に、デイブはビジョンシステム、レーザー照射時間及び電力の範囲、動作制御の精確さの要求事項及び、レーザーが作動した場合のハードウェアのドアロックとのインターフェースを含めたドアセンサーの安全装置を入れる。

デイブはさらに、オートメーション技術者、製造技術者及び品質技術者が参加する正式なソフトウェア要求事項審査を実施する必要があると判断する。

このシステムのソフトウェアは市販のパッケージであるが、 デイブはカスタム修正が必要であると知っている。彼は、工場の MES システムにインターフェースを追加する必要がある。

リスクコントロール手段

次に、デイブはリスクに注目する。 彼は、下流の漏れ検査及び定期的な破壊試験による溶込みの検査で十分であると確信していたため、溶接深さ及びその他の重要変数の重大さは低いと考えた。同様に、漏れ検査でハーメチックシールが受容可能であるか確認できる。これで、ユーザーインターフェース領域のリスク、特にドア開放時にソフトウェアがレーザー照射を開始するリスクが残る。デイブはソフトウェアがドアの閉鎖を確認することを知っているが、ソフトウェアが意図した操作を実施しない場合のリスクが大きいため、ドア解放時のレーザー作動を防止するために重複してハードウェアのインターロックを追加する。

検証業務

次に、デイブは検証業務に移る。彼が選択したツールの納入業者は広範なプログラミングツールを支給したため、ソフトウェア要求事項の仕様及び先に作成した審査で設計には十分であり、ツールボックスから設計ツール、開発ツールおよび設定ツールを追加する必要はない。

他にデイブがツールボックスの試験セクションから選択した業務は、試験計画書のソフトウェア環境の詳細と予想試験結果が入ったテスト計画などであった。試験計画書は、デイブ以外にオートメーション技術者、製造技術者及び品質技術者が審査し、承認する必要がある。予想結果と比較した実際の試験結果、合否、試験の特定、並びに問題解決の文書化及び故障があった場合の回帰テストを含む試験結果について、デイブは自分以外にオートメーション技術者、製造技術者、品質技術者及びプロジェクト依頼者の承認を求めた。

導入

溶接機の導入について、デイブはツールボックスの導入ツールを見直し、製造オペレータの手順が必要であり、オートメーション技術者、製造技術者及び品質技術者が審査しなければならないと判断した。オペレータが溶接機の操作方法を確実に理解するために、デイブは、試験を含むオペレータの教育訓練及び認証手順を作成した。彼は、

MES システムでは、認証のないオペレータが溶接プログラムをシステムから取り出すことができないことを知っているため、オペレータ損傷のリスクを軽減できると安心している。

保守

デイブは、設定検査ツールがあることを知っているため、この検証において特に保守計画を作成しない。

例 3：自動溶接プロセス制御システム

この例は、本 TIR の図 2 に示されたプロセスを表す。

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	定義				

プロセス要求事項の定義（TIR セクション 4.3.1.1 参照）

デバイスコーポレーションはクラス III の医療機器製造業者である。デバイスコーポレーションは、自動溶接プロセス制御システムを実施することにした。医療機器のケースが適切に溶接されるよう、このプロセスは、パラメトリックリリース決定プロセスに基づいた製品隔離方法を支給する。デバイスコーポレーションは、このプロセスの情報を利用して自社の機器履歴簿を支援することも決定した。

デバイスコーポレーションは、自動溶接プロセス制御システムを検証するために新しいプロジェクトマネージャーを選任した。このプロジェクトマネージャーは、21 CFR Part 820 の知識にもとづいて、このシステムは 820.70 (i) 生産及びプロセス制御に従わなければならないことを認識する。したがって、プロジェクトマネージャーは、導入予定の溶接プロセス制御システムには検証が必要であると認識する。

この溶接システムの検証に関する要求事項及びリスクの理解を深めるために、プロジェクトマネージャーは次の通りプロセスを定義する。

1. オペレータは、ロットの最初の部分のロット番号をシステムに入力する。
2. オペレータは、機械の固定具にサブ部品を挿入する。
3. オペレータは、サイクル開始ボタンを押す。固定具は油圧で対応する位置に移動する。
4. 固定されたサブ部品の一定速度の回転とともに溶接サイクルが開始する。
5. 赤外線温度計が、溶接プロセス中の材料の温度をモニタリングする。温度は、各溶接済み部品のロット番号及び部品連続番号とともにファイルに記録する。
6. サイクル終了時に機械が固定具を開く。
7. オペレータは、溶接した部品を取り出し、連続番号に従い、部品をロットトレーの対応する位置に置く。
8. オペレータは、ロットトレーが一杯になるまでステップ 2〜7 を繰り返す。
9. オペレータは、ロット終了ボタンを押す。
10. 機械のオペレータインターフェースは、溶接温度がプロセスの範囲を超えた部品連続番号を表示する。
11. オペレータは、ロットトレーから対応する部品番号を破棄する。
12. オペレータは、拒否する部品リストを印刷し、ロットトレー及び報告書を次のステーションに送付する。
13. オペレータは、ステップ 1 を繰り返して新しいロットを開始する。

プロジェクトマネージャーも、主なオートメーション機能を次の通り認識する。

14. ロット番号の保管
15. 連続部品番号毎の溶接温度の保管
16. 溶接中にプロセスの温度範囲を超えた部品の連続番号の表示
17. ロット拒否報告書の印刷

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	定義				

プロセス障害リスク分析（TIR セクション 4.3.1.2 参照）

プロジェクトマネージャーは、次に現行のプロセスで起こりうる問題について考える。彼は、このプロセスが故障すれば、適切に溶接されていない部品により患者が未滅菌の医療機器に暴露される可能性があると認識する。溶接プロセス制御システムの誤り又はオペレータの誤りで、不良製品の偶発的なリリースが生じうる。

プロジェクトマネージャーは、次に、このリスクを軽減するためにどのようなリスクコントロール手段が実施されているか考える。彼は、このプロセスグループが、次のプロセスステップで溶接オペレータが正確に部品を不合格にしたかを検証する手順を設定していることを知る。さらに、彼はこの溶接システムが、市販の廃製品であることを知る。

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	定義				

ソフトウェア 目的と意図（TIR セクション 4.3.1.4 参照）

ここで、プロジェクトマネージャーは、自動化するプロセスについて基本的に理解したため、溶接プロセス制御システムの目的と意図を作成する準備が整った。

彼は次の通り記載する。

> *この溶接プロセス制御アプリケーションは、溶接したケースの合否について閉鎖ループの品質決定を行う。この決定に基づき、溶接オペレータは、手動で不適合製品を拒否する。*

最後に、プロジェクトマネージャーは、導入予定のシステムが遵守すべき FDA の規制について考える。そこで、彼は、この重要な事実を反映するために、次の文章を追加する。

> *この溶接プロセス制御アプリケーションは、DHR の一部である記録を保管する。したがって、820.80 (d) に従い、このシステムには、最終受入活動の支援に必要な電子記録が含まれる。この従前規則により記録が必要なため、21 CFR 11 の電子記録の要求事項が適用される。*

プロジェクトマネージャーは目的と意図を審査し、このプロセスにおけるソフトウェアの境界を適切に記録する。この審査に基づき、彼は、以下の通り文章の修正を決定する。

> *この溶接プロセス制御アプリケーションは、溶接したケースの合否について閉鎖ループの品質保証決定を行う。この決定に基づき、溶接オペレータは、手動でパラメータが不適合な製品を拒否する。溶接ステーションは、医療機器全体の密封の完全性を制御する唯一のポイントである。*
>
> *この溶接プロセス制御アプリケーションは、DHR の一部である記録を保管する。したがって、このシステムには、820.80 (d) に従い最終受入活動の支援に必要な電子記録が含まれる。この従前規則により記録が必要なため、21 CFR 11 の電子記録の要求事項が適用される。*

プロジェクトマネージャーは、次に、溶接システムとインターフェースする他のシステムがあれば、それは何であるか考える。彼は、このソフトウェアは、IR 温度機器、オペレータインターフェース、プリンター及び機械の PLC I/O に接続した PC で作動する単一のアプリケーションであると判断する。

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	定義				

検証プランニング（TIR セクション 4.3.1.3 参照）

ここで、プロジェクトマネージャーは自動化するプロセスを理解し、新しいシステムの意図する使用を決定したため、高レベルの検証プランニングを計画する準備が整った。

既に、プロジェクトマネージャーは、溶接プロセスは検証不可能なプロセスとして実施するため、このプロセスの残留リスクは高いと判断した。したがってプロジェクトマネージャーは、検証の取り組みの広範な審査が必要であると判断する。彼は、プロセスエンジニアリング、品質エンジニアリング及びオペレーションズプロセストレーナーが主要な承認の役割を担うべきだと決定する。次に、彼は、最終製品受入マネージャーも要求事項を承認すべきだと考える。

プロジェクトマネージャーは、彼の品質システムは、他の検証の成果物又はプロジェクトの成果物が承認される前に高リスクシステムとして承認される検証プランニングを必要とするため、検証プランニングの作成開始を決定する。

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	定義				

ソフトウェア使用の要求事項及びソフトウェア要求事項（TIR セクション 4.3.1.4 参照）

プロジェクトマネージャーは、この検証の取り組みに、高レベルの詳細又は形式を取り入れる必要があると考える。彼は、詳細なプロセス及びソフトウェア要求事項を定義することが重要であると知っている。プロジェクトマネージャーは、ここで、ソフトウェア要求事項を作成する。彼は、ソフトウェアには温度検証の重複及び拒否決定プロセスを入れるべきであると判断する。また、このプロセスには、ラインクリアランス前に拒否報告書を再度印刷するシステムが必要である。

このシステムはパラメトリック値を支援するため、彼は、安全要求事項も、システムアクセスレベルによりどのデータの数値を変更できるかについての詳細なリストとともに入れる。

		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム
開発	インプリメンテーション／試験／導入				

ソフトウェア障害リスク分析（TIR セクション 4.3.2.1 参照）

プロジェクトマネージャーは、この溶接システムに対する完全な信頼を確立するためにどんなアプローチを使用すべきかを決定する時点にきている。

プロジェクトマネージャーは、この溶接の設計は業界で一般的に使用される COTS システムを必要とすると述べる。彼は、この製品について過去に生じた問題はすべて製造業者が迅速に特定し、公表したことを知る。

プロジェクトマネージャーは、既に、自動化すべき溶接プロセスが高リスクであると判断したが、まだ、ソフトウェア障害のリスクを正式に分析したい。プロジェクトマネージャーは、彼の洞察を確認するために、彼の会社のリスクモデルに関する質問事項を検討する。

1. ソフトウェアが誤作動した場合、製品の安全に潜在的リスクはあるか。*はい*
   a. どのようなものか。*初期設定温度の限界値に基づき、システムが不良な部品を合格とする。停電後、限界値は初期設定に戻る。*
   b. このリスクの制御には何をすべきか。*各ロットの運転前後にオペレータが限界値を検証する必要がある。*
2. ユーザーが間違えば、製品品質（安全リスク以外）に潜在的リスクはあるか。*ある*
   a. どのようなものか。*手動モードでは、両方の部品センサーが 3 秒間作動すると溶接レーザーが発射しうる。*
   b. このリスクの制御には何をすべきか。*自動モードにおいてのみ発射するよう初期設定を変更する。*
3. 記録紛失は規制遵守を示す能力に対する潜在的リスクはあるか。*はい*
   a. どのようなものか。 *デバイスコーボレーションは、使用した溶接変数及びロットの合否に使用した実測データを知らなければならない。*
   b. このリスクの制御には何をすべきか。*プロジェクトマネージャーは、21 CFR Part 11 ソフトウェア要求事項を追加し、ロット報告書の終わりに特定の溶接の限界値を印刷すべきという要求事項も追加する。*

開発	インプリメンテーション／試験／導入	プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

検証プランニング（TIR セクション 4.3.2.2 参照）

プロジェクトマネージャーは、検証を終了するための十分な情報を収集し、ソフトウェア要求事項について理解し、インプリメンテーションアプローチを決定し、ソフトウェアリスクを分析した。この時点で、このシステムについて知っていることすべてを考慮して、この溶接システムがその意図する使用に合うという信頼を確立するにはどのような検証活動が必要かを自問する。

- プロジェクトマネージャーは、第三者がどのようにこのシステムを開発したかを考え、開発者が報告のカスタマイゼーションの要求事項を正確に実施したか懸念する。このシステムは様々なデータ領域に依存するため、開発者の業務の正確性を確認するためにコード審査に検証ステップ活動を追加する。

開発	インプリメンテーション／試験／導入	プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

ソフトウェアのインプリメンテーション（設計/開発/構築/試験セクション 4.3.2.3 参照）

ソフトウェアを内部で開発するのではなく購入するという決定は、コマーシャル・オフ・ザ・シェルフ（COTS）の能力にもとづいて行う。しかし、プロジェクトマネージャーは、意図する使用は高リスクに分類されているため、溶接制御ソフトウェアが妥当性の確認されたソフトウェアの開発ライフサイクルのもとで開発された事をデバイスコーポレーション の品質部門に照明する必要があることを知っている。

彼は、COTS 供給者とこの問題について協議した後、供給者の SDLC プロセスが最近独立監査会社の監査を受けたことを知った。プロジェクトマネージャーは、そこで、COTS 供給者に連絡し、SDLC 査察報告書の写しを購入できた。その結果、品質部門は、COTS 供給者が有効なライフサイクルモデルのもとでこのソフトウェアを開発したと確信した。

開発	インプリメンテーション／試験／導入	プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

検証レポート（TIR セクション 4.3.2.4 参照）

プロジェクトマネージャーは、検証レポートを記入し、承認を得る。

開発	インプリメンテーション／試験／導入	プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

ソフトウェアのリリース（TIR セクション 4.3.2.5 参照）

プロジェクトマネージャーは、彼の正式な構成管理システムのソフトウェアが彼の検証レポートで引用されたソフトウェアと一致することを検証する。

開発		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

変更の分析

プロジェクトマネージャーは、彼の検証プランニングのもとで、検証後の溶接システム変更を管理する正式な変更制御プロセスが彼の会社にあることを検証した。

開発		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

保守のプランニング（TIR セクション 4.4.1 参照）

プロジェクトマネージャーは、システムが引き続きその意図する使用を満たすことを確認するためにどの活動が適切であるかを前もって考える。このシステムは高リスクであるため、彼は、3 ヵ月に 1 回校正を行い、温度の実測値及びロット報告書に印刷された温度が正確かつ厳密であるという承認をしなければならないと決定する。プロジェクトマネージャーは検証プランニングにこれを記録する項を加え、このシステムが生産段階に入ったら 3 ヵ月に 1 回の審査が確実に実施されるように校正/認証手順の開発及び実施を請求する。

開発		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

ソフトウェアの保守

プロジェクトマネージャーは、彼の検証プランニングのもとで、溶接システム及びプロセスがその意図する使用とは異ならないことを保証する定期的審査プロセスが彼の会社にあることを検証した。

開発		プロセス	反復的リスク分析	検証プランニング及びレポート作成	ソフトウェアシステム

ソフトウェアの廃用

プロジェクトマネージャーは、彼の検証プランニングのもとで、溶接システムの廃用を管理する正式なソフトウェア廃用プロセスが彼の会社に存在することを検証した。

ツールボックスの選択:

設計、開発及び設定ツール

- プロセス要求事項の定義
- 正式なソフトウェア要求事項の審査
- 製造/ビジネスプロセス内のリスクコントロール手段の特定
- プロセス開発審査
- トレーサビリティマトリックス（要求事項の仕様に内在）

試験ツール

- テスト計画
- ソフトウェアシステムテスト
- ソフトウェア設定制御

導入ツール

- ユーザー手順の審査
- アプリケーションの内部教育訓練
- 据付時適格性確認
- プロセス検証

例 4：C/C++言語コンパイラ

背景

クラス III の医療機器会社が、組み込みシステムについて自社の OTSS C/C++言語コンパイラの検証をしたい。このコンパイラは DHF（設計履歴ファイル）に入った製品ソフトウェア（ソフトウェアソースコード及び実行可能ソフトウェア）を作成するため、コンパイラは調整されていると判断された。

品質システムプロセスの記述

このケーススタディには、2 つの品質システムプロセスがある。一つ目は、クラス III の医療機器ソフトウェアインプリメンテーション全体の品質システムプロセスである（図 1 参照）。二つ目は、ソフトウェアの設計を実施し、OTSS C/C++言語コンパイラを含むすべてのソフトウェア要求事項を満たすプロセスである。（図 1 の“ソフトウェアのインプリメンテーション”の項参照）

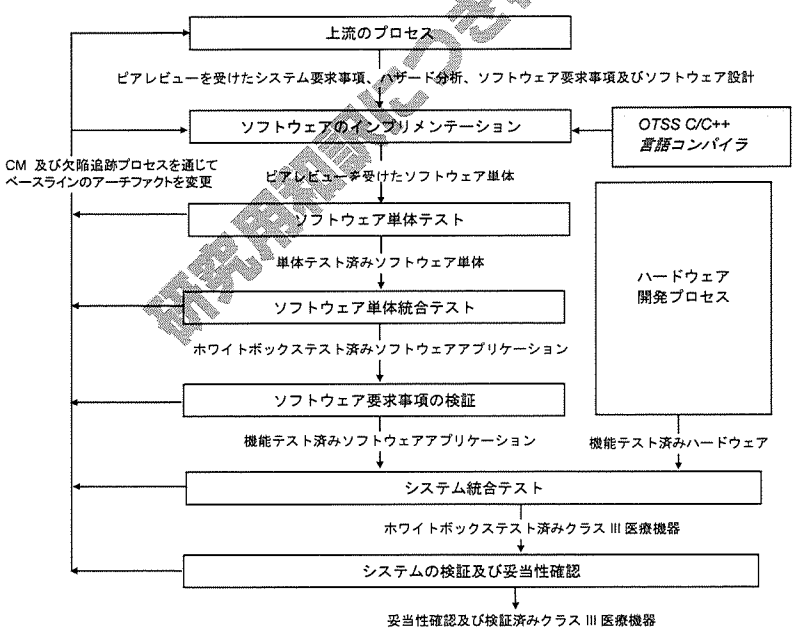

図 C1－クラス III 医療機器ソフトウェアのインプリメンテーション

上流のプロセス

ソフトウェアインプリメンテーションの上流プロセスには、開発する医療機器を特徴付けるシステムレベル文書（要求事項、設計、ハザード分析など）の開発プロセスがある。次に、ソフトウェアに実装したシステムの部分について、ソフトウェア要求事項、ソフトウェア設計及び他のソフトウェア文書又は計画の開発プロセスを通じて特徴を付与する。ソフトウェアの開発と並行して、医療機器ハードウェア開発のためにも追加プロセスが実施される。

ソフトウェアインプリメンテーションプロセス

使用した正式なソフトウェア言語はC/C++ソフトウェア言語である。OTSS C/C++言語コンパイラを使用して高レベルのソフトウェアステートメントを実行可能なマシンコードにコンパイルする。ソフトウェアインプリメンテーションプロセスの出力は、他の技術担当者が完全性及び正確性をピアレビューしたベースラインのソフトウェア単体である。ソフトウェア単体をピアレビューするには、ソフトウェア単体は、最高のコンパイラレベルで誤りなくコンパイルされ、コンパイラの警告はすべてピアレビューで説明しなければならない。

下流の検査プロセス

ソフトウェア単体は、次の通り、複数の試験プロセスで試験又は検証する。

- ソフトウェア単体テスト。個々のソフトウェア単体の論理的正当性及び境界条件を試験する。この試験は、開発システム又は標的システム（医療機器のハードウェア）で実施する場合がある。単純なソフトウェア単体については、コードのピアレビューが単体の論理的な誤り検知に十分であると判断された場合にはこの検査を実施しなくてもよい。
- ソフトウェア単体統合テスト。ソフトウェア単体を統合及び試験し、ソフトウェアの設計が正しく実装され、設計がテストされたことに関する境界条件が試験されたことを保証する。この試験は標的システムで実施する。
- ソフトウェア要求事項の検証。完全な一組のソフトウェア要求事項に照らし合わせて、完全にソフトウェアアプリケーションを検証する。検証は標的システムで実施する。
- システム統合テスト。医療機器のソフトウェア及びハードウェアをテストし、システムの設計が正しく実装され、システムの設計が試験されたことに関する境界条件が試験されたことを保証する。
- システムの検証及び妥当性確認。医療機器は、システム要求事項レベルで検証し、また、その意図する使用の妥当性を確認する。

プロセス障害リスク分析

このプロジェクトは、自社のプロセスリスクアセスメント手順に従った。クラス III 医療機器ソフトウェアインプリメンテーションの全体の品質システムプロセス（図1のすべてのプロセスを含む）は、クラス III 医療機器内で機能するソフトウェアを作成するため、本質的に高リスクである。

ソフトウェアインプリメンテーションプロセスの一部であるOTSS C/C++言語コンパイラは、次に基づき低リスクと評価された。

- 患者、オペレータ又は第三者に対する直接重大な損傷又は死亡原因にはならない。
- ツール（例えば、ソフトウェア単体テスト、ソフトウェア単体統合テスト、ソフトウェア要求事項の検証、システム統合テスト、システムの検証及び妥当性確認）の出力（ソフトウェアソースコード及び実行可能なソフトウェア）の下流での検証。

意図する使用の定義

上述のソフトウェアインプリメンテーションプロセス内のOTSS C/C++言語コンパイラの目的と意図は、組み込みシステムソースコードを作成し、コンピレーションプロセスを実行して、クラス III 医療機器の実行可能なソフトウェアを作成することである。

ソフトウェア使用の要求事項

1. ツールは、C 及び C++コードをクロスコンパイルして、選択した納入業者のオペレーティングシステムを用いたRISCプロセッサで作動しなければならない。
2. コンパイラにはソースコードデバッガがなければならない。
3. コンパイラは、ANSI C 及び C++対応でなければならない。
4. コンパイラは、様々な承認された業界標準の統合開発環境（IDE）を統合しなければならない。
5. 納入業者は、検索可能な既知のバグリストを公表しなければならない。このリストは、必要に応じて相談の参照として使用しなければならない。
6. 納入業者は、規制産業内に大規模なユーザー基盤が必要である。

ソフトウェアの障害リスク分析

このOTSS C/C++言語コンパイラのリスク分析から、誤りがあった場合に次が発生しうることがわかった。

- リスク_1：OTSS納入業者は、技術の明らかな特徴及び機能に加え、適切なビジネスプロセス、開発方法及びサポートを提供できない。
- 軽減_1：納入業者選択プロセス。（下の項参照）
- リスク_2：間違った実行可能な文章を作成する。
- 軽減_2：検証プランニング（下の項参照）
- リスク_3：ユーザーによる誤使用。最も厳格なレベルのエラーチェックを実施していない。
- 軽減_3：教育訓練及び手順/作業指示書

納入業者選択プロセス

このプロジェクトは自社の納入業者選択承認に関する品質システム手順に従い、この情報はプロジェクトのDHFに保管する。この手順には、納入業者のSDLCに関する方針、手順、業務及び活動を審査するオンサイトでの評価が含まれた。OTSS納入業者のC/C++言語コンパイラの能力は、上記のソフトウェア使用の要求事項を満たすことが検証された。

検証プランニング

このOTSS C/C++言語コンパイラでは、下流の検証アプローチを選択した。納入業者の選択プロセスで、この納入業者がすべての文書化されたソフトウェア使用の要求事項を満たすと判断された。このコンパイラは、納入業者において重要なランタイムがあり、このプロジェクトで実施するデバッグ及び試験でも重要なランタイムがある。コンパイラの出力は、下流のプロセスにおける次の動的テストを受ける。

- ソフトウェア単体テスト
- ソフトウェア単体統合テスト
- ソフトウェア要求事項検証テスト
- システム統合テスト
- システムの検証及び妥当性確認

検証レポート

検証レポートの内容

- OTSSの記述
- ソフトウェア使用の要求事項
  - ハードウェア要求事項
  - ソフトウェア要求事項
  - パッチ
- リスクアセスメント/ハザード分析
- 納入業者選択
- インストール活動
- 検証
  - ソフトウェア使用の要求事項テストケース/結果
- 既知のバグリスト
- 設定制御
  - 教育訓練
  - インストール位置
  - 保守
  - 廃用プロセス

ツールボックスの選択

- 定義:
  - 意図する使用
  - 検証プランニング
  - リスクマネジメント計画（リスクアセスメント）
- インプリメンテーション:
  - リスクコントロール手段
  - 納入業者監査
- 導入
  - 据付時適格性確認
  - アプリケーションの内部教育訓練
  - 最終受入試験
- 保守段階
  - 保守計画
  - 既知の問題の分析

例 5： 自動ソフトウェア試験システム

背景

この例では、製造業者はクラスⅡの医療機器製造業者である。この製造業者が製造した医療機器はソフトウェアで制御する。そのソフトウェアは、アーキテクチャ上、オペレータコンソール及びリアルタイム組み込み制御ソフトウェアという2つの重要な要素で構成される。オペレータコンソールは、このシステムへの主なヒューマンインターフェースである。リアルタイム組み込み制御ソフトウェアは、電気機械制御、データ収集、タイミングなどすべてを実施するソフトウェアである。オペレータコンソールソフトウェア（業界の標準オペレーティングシステム及びデータベース搭載 PC に内蔵）及びリアルタイム組み込みソフトウェア（オンボード組み込み CPU カードに内蔵）は、標準 TCP/IP ハードウェア及びプロトコルインターフェースを用いてインターフェースしている。

このプロジェクトのソフトウェアマネージャーは、ソフトウェアの自動試験を導入してソフトウェアの開発・試験プロセスを改善することは価値があると判断した。ソフトウェアマネージャーは、まず、オペレータコンソールソフトウェアの自動ソフトウェア試験のみを実施することにした。自動ソフトウェア試験は、統合テスト及びソフトウェアシステムテストの両方の時点で実施する。

ソフトウェアが調整されているかの判断

自動試験ソフトウェアは、この製造業者のソフトウェア開発手順に必要な試験を実施するために使用し、統合テスト及びシステムテスト時点の回帰テストに必要な証拠を提供するため、開発プロセスの一部を自動化し、21 CFR 820.70（i）–生産及びプロセス制御–自動プロセスの検証要求事項の対象であったことがわかった。

プロセスの定義

オペレータコンソールの自動ソフトウェア試験導入の要求事項及びリスクの理解を深めるために、ソフトウェアマネージャーは、ソフトウェア開発プロセスにおける自動試験ソフトウェアの使用を次の通り定義する。

医療機器のソフトウェア開発中に、様々な時点でシステムソフトウェアに様々なモジュールの統合を予定している。また、既にシステムに統合されているモジュールは、欠陥修正及び要求事項の修正のために変更される。自動試験システムは、統合システムソフトウェアの回帰テスト及びシステム中の特定のモジュールの最終試験への使用が計画されている。このソフトウェアプロジェクト計画では、週に 2～3 回のモジュ

ール統合又は更新が必要になる。自動試験は、このような各統合ポイントで実施し、新しい機能が正常に作動し、それまでの機能に追加したコード又はあるビルドで変更したコードが悪影響を及ぼしていないことを確認する。自動試験は、検証、そして最終的には顧客への最終リリースの候補であるビルドのソフトウェアシステム試験レベルで実施する。また、自動試験は、予定の手動試験を保管する回帰テストレベルを提供するための修正が必要な最終開発段階で欠陥が発見された場合にも使用される。

リスクの分析

ソフトウェアマネージャーは、ここで分析プロセスに進み、自動試験ソフトウェアについて問題が生じた場合の影響を判断する。

まず、ソフトウェアマネージャーは、自動試験プロセスの故障、自動試験ソフトウェアの故障、又は自動試験ソフトウェアユーザーによる誤りが最終的に医療機器の故障になり、患者、オペレータ、第三者、サービス担当者又は環境への潜在的危害が生じるかどうかを評価する。

- ソフトウェアマネージャーの最大の関心は、自動ソフトウェア試験システムが、検査中のオペレータコンソールソフトウェアに対して実際には欠陥があるのに正常に作動しているという誤った指示を与える可能性があるということである。
- 検出されない欠陥がソフトウェアの重要な部分にあった場合、医療機器が誤作動し、危害が生じうる。
- ソフトウェアマネージャーは、この潜在的リスクは、自動試験ソフトウェアの誤った管理又は誤った自動試験ソフトウェア使用、若しくは自動試験ソフトウェア自体の故障により発生しうると理解する。
- ソフトウェアマネージャーは、自動ソフトウェア試験システム使用時期、及び使用目的に境界条件を設定し、ソフトウェア開発・試験チームがこのシステムに過度に依存しないようにすることが重要であると判断する。
- 自動試験ソフトウェアの設定、プログラミング及び操作に関わる者は、その役割について教育訓練を受ける必要がある。
- ソフトウェアマネージャーは、これらの要素を制御することで、関連する潜在的リスクを受容可能なレベルにまで軽減できると感じる。

ソフトウェアの意図する使用の定義

ここで、ソフトウェアマネージャーは自動試験ソフトウェアの使用の可能性を分析し、関連するリスクについて理解したため、自動ソフトウェア試験システムの目的と意図を作成する準備が整った。

- 自動試験システムは、開発プロセスにおける統合テスト時点のソフトウェアのビルドを試験するために使用する。
- 自動試験システムは、ソフトウェアのシステムテスト時点で検証と候補のリリースビルドを試験するために使用する。
- 自動試験システムは、システムの回帰テストを行い、新たに導入したソフトウェア又は変更したソフトウェアによりワークフローに悪影響が出ていないかを確認する。
- 自動試験システムの一般的な役割は、実施される手動試験を保管する回帰テストの実施である。
- 複雑度が低く、予測可能なワークフローには、特定のプロトコルが、相当する手動試験と同等であると検証されている場合、自動試験システムをソフトウェアの正確性の最終決定要因として使用できる。
- 自動試験システムは、ソフトウェアシステム又は医療機器全体の安全装置（リスク軽減）を提供するソフトウェアを実行する。

検証プランニング

ソフトウェアマネージャーは、自動化すべきプロセス、特定の自動試験システムの意図する使用、及び関連する潜在的リスクを明確に理解している。彼は既にこのソフトウェアの使用に関して何らかの制御を設置すべきと判断した。彼は、自動ソフトウェア試験システムが適当な制御とともに使用された場合、使用によるリスクは受容可能レベルになると判断した。

この場合、彼は、“適切に使用した”場合、この自動ソフトウェアシステムが原因で医療機器が故障するリスクはほとんどない、又は全くないと判断した。彼は、“適切に使用した”場合とは、ソフトウェア開発・試験チームがソフトウェアの正確さの判定に際しこの自動試験システムに過度に依存しないことと定義した。彼が低リスクと判断したため、ソフトウェアマネージャーは、このシステムの検証の要求事項は、ソフトウェア試験システムに関しては最低のレベル及び厳格さとなると判断した。

検証の文書化 –“検証レポートアプローチ”

ソフトウェアマネージャーが採用を決定したアプローチは、システムに必要なレベルの信頼を獲得するためのすべての活動の要約を含む自動ソフトウェア試験システムのソフトウェア検証レポートの作成である。

批判的思考

ソフトウェアマネージャーは、ここで、システムが適切に使用され、医療機器の深刻な欠陥の原因とならない必要な信頼レベルの最良の獲得方法を決定するプロセスに移る。

彼は、システムに必要レベルの信頼を獲得するために最も重要な要素のひとつは次の通りであると判断する。

適当な意図する使用の厳格な遵守

- ソフトウェアの開発及び試験に関わる要員すべてがシステムの境界条件及び適当な意図する使用を確実に理解するようにする。
- 文書化：検証レポートに、特定の意図する使用及び特定のプロジェクトのソフトウェア開発計画を通したその連絡方法を記述する項を加える。

適当な注意

- その企業の試験システムが同レベルの重要度又はより重要度の高いアプリケーションに使用されている信頼できる納入業者から、業界標準の自動ソフトウェア試験システムを購入する。
- システムの意図する使用を納入業者とともに審査し、その意図する使用が適切かを判断する。
- 市販前にその納入業者のソフトウェアの検証の方法に関する情報を入手する。納入業者の QA 組織から、市販のソフトウェアが納入業者による検証を受けていることを確認する文書を入手する。これにより、自動ソフトウェア試験システムが納入業者により適切に試験されたという信頼を獲得し、その後にソフトウェアマネージャー及び彼のチームが実施する追加的活動の基盤ができる。
- 納入業者との関係を構築し、ソフトウェアマネージャー及び彼のチームが使用する試験ソフトウェアの版についての既知の問題及び欠陥に気づくようにする。
- 納入業者の今後のソフトウェアの更新計画を理解し、新版のソフトウェアへの移行計画及び再検証活動を予測する。

- 文書化：検証レポートに、納入業者の自動ソフトウェア試験システムの検証情報、納入業者の欠陥（バグ）リストへのアクセス方法及び新版のソフトウェアへの移行計画など、納入業者の適当な注意についての活動の結果に関する項を加える。

インストールテスト

- コンピュータの計算環境が納入業者の仕様に適合することを確認する。
- ソフトウェアが正確にインストールされたことを確認するために、最初の高レベルプロトコルを確立する。
- 文書化：検証レポートに、インストール確認活動結果に関する項を加える。

リスクマネジメント

- ソフトウェアマネージャーがソフトウェアの目的と意図で定義した通りにのみシステムが使用されるようにする。
- 自動試験システムを使用するプロジェクトのソフトウェア開発計画に特定の自動試験システムの受入可能境界条件を入れる。
- 手動試験で自動ソフトウェア試験システムが取り扱わない領域を取り扱うよう、試験システムの正確な適用領域を特定するために分析を実施する。
- 文書化：検証レポートに、初回リスク分析で特定されたリスクに関する項を加え、これらのリスクがどのように軽減されるかを示す。

ソフトウェア使用の要求事項

- ソフトウェア開発チーム及びソフトウェア試験チームと協力するソフトウェアマネージャーは、使用しようとする自動試験システムの機能性のリストを作成する。
- このリストを、使用する機能を表す“ソフトウェア使用の要求事項”リストと呼ぶ。
- 文書化：検証レポートに、“ソフトウェア使用の要求事項”リスト及び各ソフトウェア使用の要求事項の記述の項を加える。

自動試験システムの検証

- “ソフトウェア使用の要求事項”に基づき、ソフトウェアマネージャーは、初回自動試験スクリプト/プロトコルを 3 つ選び、同一のプロトコルによる手動試験の“並列”試験を実施し、必要レベルの信頼を獲得できると判断した。
- 3 つの初回試験スクリプト/プロトコルは、チームが使用するすべての機能性を実行する。

- 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届いたら、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。