付録 B
リスクマネジメント

ISO 14971 の概念を生産及び品質システムソフトウェアに応用する。

ISO 14971 の" Medical devices —Application of risk management to medical devices（医療機器 － リスクマネジメントの医療機器への応用）" は、生産又は品質システムではなく、医療機器のために作成された規格である。しかし、この規格の最高レベルに位置づけられたリスクマネジメントの概念及びプロセスは、生産・品質システムにも応用できる。

このレポートの主題は生産・品質システムソフトウェアでの検証及びリスクマネジメントだが、ソフトウェアが全体的なプロセスやシステムを構成するコンポーネントの一つであり、故障する可能性があるという点を考慮せずに、ソフトウェアのリスクを徹底的に分析することはできない。医療機器規格の ISO 14971 は、患者又はその他の医療機器ユーザーへの危害のリスク低減に関するものである。生産又は品質システムのコンテクストにおける危害とは大きく異なる。この場合の危害とは、生産される機器への影響（通常、患者への直接的な危害ではない）、全体的な生産プロセスへの危害、品質記録の完全性への危害、規則遵守への危害、又は事業への危害を意味する。

ここで紹介するリスクマネジメントのプロセスは、ソフトウェアで駆動するシステムに固有なタイプの危害を個々に検討するものであり、それがこのレポートのテーマとなっている。そこで、14971 のリスクマネジメントプロセスを、これらの危害発生源のリスクの管理及び予防に応用する。このコンテクストにおける 14971 の参照は、この規格が生産・品質システムソフトウェアに直接適用するという意味ではない。しかし、リスク分析、リスク評価、及びリスクマネジメント（" 危害" の語法に多少修正を加えている）の一般化されたプロセスは、生産・品質システムソフトウェアに適用できるほど一般的なものといえる。新しいプロセスを考案したり、同じプロセスを言い表す言語を変えたりするのではなく、我々は目的のために 14971 からリスクマネジメントプロセスを" 借りる" ことにした。

リスクマネジメントプロセスのフローチャート

下記のソフトウェアリスクモデルのフローチャートは、以下の目的を適切に遂行するために必要なプロセス及びプロセス要素を示している。

- 規制された生産環境でのソフトウェアの使用がもたらす潜在的な影響を特定又は発見する。
- ソフトウェアの故障又は誤用がもたらす潜在的なリスクを評価する。

- ソフトウェアの故障に起因する危害の本質的な重大性を減らすための適切な予防策を通じてリスク低減を適用する。
- 適切なレベルの検証が適用されるようにする。

ソフトウェアの使用がもたらす潜在的な影響を特定又は発見するには、まず最初にソフトウェアの意図する使用を定義し、最初のリスク分析を行う必要がある。この分析の一環として、“もしシステムが故障したら、何が機器の安全性や有効性に影響を及ぼし、生産担当者への潜在的な危害や環境へのダメージを生み出し、生産プロセスや品質システム、又はその両方に悪影響を及ぼすのか”という疑問について考えなければならない。単純な低リスクのソフトウェアの場合（このタイプのソフトウェアを含む例については付録Cを参照）、リスクマネジメント活動を文書化するには、この評価だけでほぼ十分といえるが、高リスクを伴うシステムの場合、リストに記載したすべてのエリアの影響を及ぼす可能性があるため、分野横断的なチームによる非常に綿密な評価が必要となる。

リスク予防策のアプリケーションには、ソフトウェアの設計変更、手順変更、ハードウェア冗長性、セキュリティコントロール、コードレビューなどの静的試験、負荷試験やパス試験などの動的試験、バックアップシステム、モニタリングシステム、アウトプットのマニュアル検査、又は販売業者の検査などが含まれる。これらのリスク予防策は、すぐれたエンジニアリングの問題解決テクニックを応用したものである。予防策を評価・応用するこのプロセスは、システムの危害発生能力が容認可能なレベルにまで低減されたという確信が得られるまで継続される。このTIRでは、リスクを低減するこれらの方法又は理念をリスク予防ツールとして考えることを推奨する。これらのツールを文書化することは、リスク分析及び上記のリスク予防ツールを利用したリスク低減計画の背後にある思考プロセスの共有を促す良い方法の一つといえる。

リスク予防策の適用により新たな意図しないリスクが全体的なシステムに入り込む可能性を評価するためには、上記の質問プロセスを繰り返し実施しなければならない。リスク評価に基づき、検証努力に適切なレベルの厳密性を割り当てる。

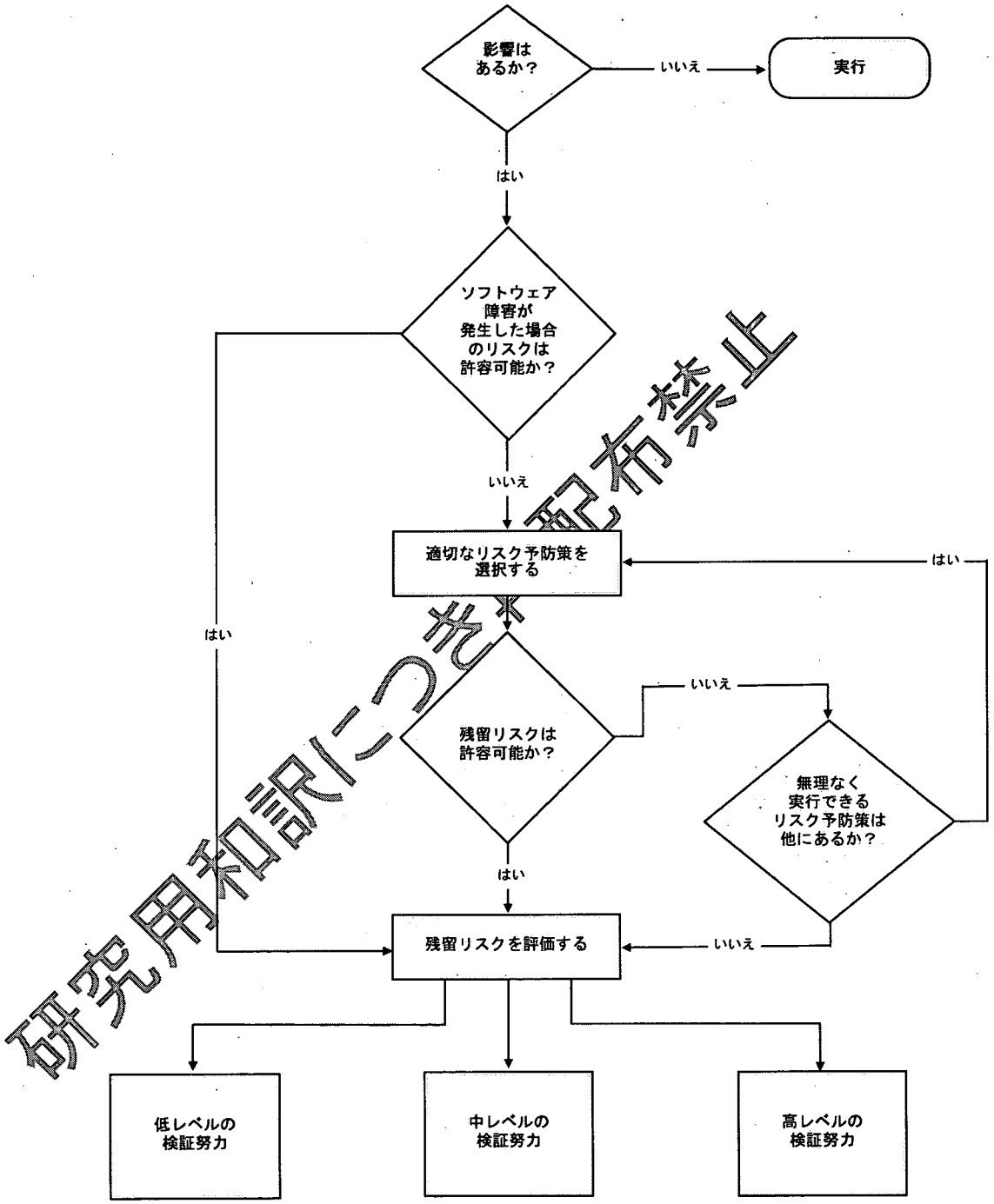

図 **B1** ― リスクマネジメントモデル（**ISO 14971** に基づき翻案）

リスクマネジメント用語の生産・品質システムへの応用

ISO 14971 にあるようなリスクマネジメントの用語及び概念は、手を加えないまま、その大部分を生産・品質システムソフトウェアに応用できる。生産・品質システム（具体的にはそれらのシステム内のソフトウェア）に応用する場合、特殊な意味を持つ用語と概念もいくつかある。

リスク分析及びリスクマネジメントに関する 14971 などの文書によれば、リスクはハザード、原因及び間接要因の階層構造になっている。このレベルでリスクを取り扱うことは、検証をテーマとするこの TIR の適用範囲外であるが、ソフトウェア故障に伴うリスクのメカニズムとそれを予防する最善策を理解するためにシステムを解体する上で役に立つことは間違いない。

リスク（Risk）

リスクとは、14971 の定義によれば、特定された危険が発生する確率と結果的に生じた危害の重大性を組み合わせたものである。生産・品質システムソフトウェアの障害に起因する危害の重大性は、医療機器そのものに起因する危害の重大性とは微妙に異なる。

危害（具体的にはソフトウェアの障害に起因する危害）が発生する確率というのは難解な概念だが、それは単に、ソフトウェアの障害発生率が予測困難であるという理由による。

まず最初に、自動化プロセスソフトウェア、つまり、コンプライアンスをサポートするために使われるソフトウェア、又は機器の製造や検査プロセスの自動化に使われるソフトウェアを例に挙げ、ソフトウェアという用語を定義してみよう。

自動化プロセスソフトウェアの検証は、通常、患者又は医療機器ユーザーへの危害の直接的な原因にならないという点で、医療機器ソフトウェアと異なる。安全性に関わる（有害な）自動化プロセスソフトウェアの障害は、大抵、使用時に機器が故障した場合にのみ有害となる。自動化プロセスソフトウェアは、通常、患者又は機器ユーザへ*間接的*な危害をもたらすだけである。

生産・品質システムの障害が間接的な危害を及ぼす例として、以下のものが挙げられる。

- 生産滅菌システムの障害が有害又は致命的な感染症を引き起こす。
- 最終試験システムの障害により潜在的な機器の欠陥を発見できない。
- 医療機器にトレーサビリティ機能をもたらす MRP システムの障害により、機器の潜在的なユーザーに安全性に関するリコールを通知できない。

生産・品質システムの障害が直接的な危害を及ぼす例として、以下のものが挙げられる。

- 生産安全性システムの障害がオペレータに危害をもたらす。
- 滅菌システムの障害が原因で環境に有害物質を放出する。

リスクを予防するためのオプションとして、障害の重大性を低減すること、傷害発生の確率を減らすこと、又はその両方が考えられる。

重大性（Severity）

生産・品質システムソフトウェアの障害に起因する危害の重大性が、患者若しくはソフトウェアで製造や品質を管理する医療機器のユーザーに直接的な危害を及ぼすことは滅多にない。この場合の危害は間接的なものである。最終的に患者又は機器ユーザーへの危害の原因となるのは、機器にもたらされる危害である。言うまでもなく、間接的な危害の方が重大性は低い。実際、生産・品質システム障害の方が重大性は高いと考えられる場合もあるが、その理由は単に、それらのシステムに生じた1回の障害が多数の機器の障害につながり、障害が発見される前に、結果として多くの患者が影響を受けるからである。一つの機器に生じたソフトウェアの障害が、一人の患者に1度だけ危害をもたらすこともある。

生産・品質システムの障害が、結果的に直接的な危害と間接的な危害の両方をもたらすこともあり得る。下記に掲載した危害は、相互排他的なものではなく、それぞれが患者及び/又は医療機器ユーザーに間接的な危害を及ぼす可能性を持っている。その例をいくつか紹介する。

- 医療機器への悪影響
  - ○ アラームが臨界許容を生じない。
  - ○ キャリブレーションシステムが薬剤送達装置を正確に較正できない。
  - ○ 滅菌コントローラーが故障して無菌でないコンポーネントが発生する。

  生産プロセスへの悪影響
  - ○ 自動化プロセスの障害に伴ってマニュアルの問題回避策が講じられ、生産が減速する。
  - ○ ソフトウェア制御のプロセス障害により規格外部品の割合が増加する。
- 規則遵守への悪影響
  - ○ 苦情処理システムが間違った故障統計データを出力し、現場報告された欠陥が未確認のまま放置される。
  - ○ 機器サービス/修理システムが故障し、それまで見つけられなかった欠陥を指摘できたかも知れない問題の動向を浮き彫りにすることができない。
  - ○ インプラントに関するデータベースの完全性が損なわれる。
  - ○ 製品の安全性チェックに関連する品質管理記録の消失。
  - ○ コンプライアンスデータの消失。
  - ○ 機器検証データの消失。

- 製造された機器のソフトウェア構成を管理・報告することができない。
- トレーサビリティ機能をもたらすMRPシステムの障害により、機器の潜在的なユーザーに機器の安全性に関するリコールを通知できない。

- 生産担当者又は環境への危害。
  - オペレーターの傷害又は有害物質の漏出。

生産・品質システムを自動化するソフトウェアに関連するリスクを分析する際、あらゆるカテゴリーの危害を考慮しなければならない。それぞれの危害の重大性は、具体的なアプリケーション、及びその危害に対する機器製造業者の許容力に依存する。製造業者が採点法を利用して危害の重大性をランク付けしたり、許容可能/許容不可能の二者択一で判定を行うことも多い。危害そのものが特定されるまで、重大性を予測できない場合が多い。そのような場合、最も重大な危害をリストの最上部、あまり重大でないものをリストの最下部に配置した相対的なスケールを使って危害の重大性をランク付けすると役に立つこともある。ランク付けしたリストをチェックすれば、どのレベルが許容可能で、どれが不可能かを明確にすることもできる。

尤度（Likelihood）

自動化プロセスソフトウェアの障害に起因する潜在的な危害発生の尤度に影響を及ぼす可能性がある要因として、以下の例が挙げられる。

- 障害の結果を察知する能力。
- 障害を改善又は障害に起因する危害を緩和する下流のリスク予防策の有無及び有効性。
- 二次的または同時に発生して危害を生じるイベントの数（相乗的蓋然性 ）。
- 二次的なイベントの尤度。
- 危害をもたらす可能性がある二次的なイベントの平行パスの数（相加的因果性 ）

障害の尤度は、障害の確率に関連するか、それと同じである。学術研究の多くは、ソフトウェア障害の確率を予測するための数量モデルや、残された欠陥数の数量化に重点を置いてきた。これらの推定法に関わるパラメータの数は多く、その大半は主観的な尺度に基づいている。

ソフトウェア検証のリスク評価に利用できる比較的単純な方法として、相対語でのみ尤度を考える方法が挙げられる。例えば、ほとんどの人は、複雑なソフトウェアの方が単純なソフトウェアよりも障害の発生率が高く、試験を経たソフトウェアの方が未試験のソフトウェアよりも障害の発生率が低いと考えるだろう。尤度又は確率がどの程度減少するかを数値化する試みがどれほど有意義なものかは、議論の余地がある。

これを数学的に判定してくれる絶対確実な科学は存在しない。ソフトウェア検証及び設計・開発の優良実施の作業は、障害の確率を上昇させるソフトウェアの属性を減らし、障害の確率を低下させる属性を増やすことに重点を置かなければならない。

つまり、この文書のコンテクストでは、障害が結果的に直接的又は間接的な危害をもたらす場合に限り、障害の蓋然性は興味深いものになる。ビジネスのリスク、規制のリスク、又はその両方について検討が行われていれば、それらのカテゴリーで危害を生み出す障害も興味深いものになる。

自動化プロセスソフトウェアの障害尤度を取り扱うアプローチの一つとして、ソフトウェアが障害を起こすのを当然とみなすことが挙げられる。自動化プロセスソフトウェアの障害に起因する危害は、医療機器を介して間接的な影響を及ぼすことが多いため、下流で障害を見つけたり、リスクを予防する機会は数多く存在する。それらの機会をリスク予防策に利用することもできるし、障害に起因する危害のポテンシャルを減らす目的で既に利用している例もある。

また、ソフトウェア障害の後又はそれと同時に他の何らかのイベントが発生した場合、危害はソフトウェア障害に起因するものだけになる。因果連鎖におけるこれらのイベントの尤度は、ソフトウェアと障害が危害をもたらす尤度に影響を及ぼす。

リスク低減努力の優先順位を決定するには、患者、ユーザー又は環境への潜在的な危害の重大性とその危害の原因が発生する尤度を組み合わせて検討しなければならない。

リスク又は残留リスクの容認性

おそらくリスクマネジメントで最も困難な活動は、リスクの許容可能レベルを決定することだろう。これは、潜在的な危害の重大性に大きく依存する。各製造業者は、リスクの容認性を定義・文書化するための基準を設定し、それらの基準に適合した評価を可能にするようなフォーマットであらゆるリスクを特定する必要がある。一般的に、ある人が同僚や管理職、監査担当者に無理なく妥当性を証明できるレベルにまでリスクの許容可能レベルを下げることができれば、それは適切なレベルと考えられる。

容認性の閾値を提案するのはこの文書の守備範囲外だが、そのレベル設定プロセスについて、いくつかの案を紹介するのは構わないだろう。

- 具体的にする。“ できる限り低く” とか、“ 他の製品と同じくらい安全” などといった許容基準は役に立たない、許容基準は、許容基準を満たしていることを客観的に判断できるように、試験用の仕様書と同様に文書化されなければならない。
- 早い段階で許容基準を特定する。危害の潜在的なリスクが特定されたら、早急に目標又は使用を決定する。リスク予防策を講じる前に、許容性に関する

目標を設定することが重要である。リスク予防策を講じた後、容認性の認識はより高レベルのリスクへと向かう場合が多い。許容基準を事前に文書化し、プロセスが逸脱しないようにすること。

- リスクの許容決定を裏付ける根拠を文書化する。これは、将来的に自動化プロセスの保守を行い、思考プロセスを規制当局の調査官に伝達する上で有用である。

リスク予防策

リスク予防策とは、システム内で特定された危害に起因するリスクを低減する対策のことである。このレポートの主旨に関連があるのは、ソフトウェア障害に起因する危害のリスク予防策である。

リスク予防策の形式はさまざまだが、常に全体的な生産又は品質システムのコンテクストで考慮されなければならない。すべてのリスク予防策が同じようにリスク低減に効果的とは限らない。結果的に生じた危害の重大性、又は危害の発生率を低下させることで、リスクを低減できることを忘れてはならない。

ソフトウェア障害に対するリスク予防策は、ソフトウェア本体の外側で履行されることが多い（ウォッチドッグタイマー、スレーブプロセッサー、又はトランザクションロギング）。生産システムの場合、ソフトウェア障害に起因する生産上の欠陥リスクは、生産された部品の下流での適切な検査を要求することで予防できる場合が多い。

下流の検証

組み込まれた生産プロセスソフトウェアは、アクセスが困難で、製造業者から詳細な情報を入手できない場合が多い。よくある例として、マシンツールに組み込まれたソフトウェアが医療機器の製造に使われることがある。ソフトウェアをスタンドアロンの単位で検証する場合、このタイプのソフトウェアを意図する使用について検証するのは困難なこともある。

このような状況で特に効果的なリスク予防策は、ソフトウェアのアウトプット、又はそのソフトウェアが制御する機器のアウトプットを下流で検証する方法である。つまり、ソフトウェアによって自動化されたプロセスのアウトプットを監視して潜在的に有害な欠陥をチェックすれば、ソフトウェアが意図する使用に適合していることを直接判定できる。こうすれば、ライフサイクルコントロールの手法を採用して、ソフトウェアが意図する使用に適合していることを証明する代わりとなる。この手法は、パーツ単位、又は統計的に決定されたパーツのサンプリングごとにチェック可能で、ごく少数の重要な操作を自動化しているプロセスにのみ有効である。検証技師は、下流

での検証を代用した根拠、及び継続的な検証ではなく、サンプリングによる検証を選択したことを正当化するために利用した前提について詳しく説明し、それらの前提を検証しなければならない。

下流での検証は、他のリスク予防策と同様に文書化しなければならない。後のコスト削減措置で排除されることがないよう、検証プロセスがリスク予防策の一つである旨を文書化することが特に重要である。また、規則によって検証の“客観的な証拠の用意”が求められており、その確認が検証の大部分の代わりになることから、下流での検証の結果を文書化する必要もある。製品の進化に伴い、ソフトウェアによって自動化されるプロセスの意図する使用も進化する。その一例として、当初は医療機器のコンポーネントで一つの重要なオペレーションを実行していたマシンツールについて考えてみよう。後に、医療機器の設計がわずかに変更され、ソフトウェアで動作するそのマシンツールに二つの重要なオペレーションが要求されるようになった。このマシンツールの意図する使用が変更された結果（安全上重要なオペレーションが一つから二つに増加）、下流での検証も両方のオペレーションをチェックするように変更されなければならない。

下流での検証プロセスを確認する

下流での検証はマニュアル又はその他の人的なオペレーションによって遂行される。その例として、エッジの仕上げや機械的整合性の目視検査、又は機械的誤差や電気的導通のマニュアル測定などが挙げられる試験のタイプに関係なく、もしそれがソフトウェアによって自動化されたプロセスの下流検証で、その自動化プロセスのためのリスク予防策として利用されているのなら、検証試験を文書化しなければならない。試験官のための試験手順を明記し、試験項目ごとに結果の許容範囲を明確に定義する。試験官もまた、自動化プロセスのアウトプットをテストするための手順を実行したことを証明する文書を提出しなければならない。

リスク予防策としてのソフトウェア検証

ソフトウェア検証は、ソフトウェア障害の尤度を低減させることから、リスク予防策の一つといえる。残念ながら、その尤度がどの程度下がるのかは、今のところ判明していない。従って、ソフトウェア検証はリスク予防の最後の手段と考えるべきである。なぜなら、ソフトウェアコンポーネント以外のリスク予防策は、重大性のみならず、確率さえも軽減すると考えられ、それによって危害の尤度を大幅に低減できるからである。

より付加価値の高い検証活動を利用して開発と試験が行われたソフトウェアは、ほとんど検証活動が行われずに開発と試験が行われたソフトウェアよりも、故障する確率

が少ない。もしリスクマネジメントがソフトウェア検証活動に大きく依存するのであれば、リスク（重大性に重点を置く）が高いと認識してもらえるように、より深く詳細な客観的証拠を用意することがますます重要になっているといえる。客観的証拠は、ソフトウェアの開発と試験が優良実施規則に基づいて行われたことを明記した文書で構成される。このアプローチは、ソフトウェア障害に起因する危害の重大性又は尤度をコントロールするプロセス又はシステムに計画したリスク予防策を採用する方法ほど望ましいものではない。

リスクモデルの例

下記のリスクモデルは、14971 のリスクモデル（図 B1）で使用したものと同じように、アンケートの結果に基づいてソフトウェアに起因する危害の重大性を高レベル、中レベル及び低レベルに分類したものである。

これはリスクモデルの一例に過ぎないが、プロセスやソフトウェアのリスクを、高中低のレベルに分類する方法は他にもたくさんある。これはあくまでも一つのモデルの一例である。

リスク評価

	リスク評価アンケート	Yes または No で 回答すること Yes の場合はリスク番号を 記入すること （例：リスク#1、リスク#2、 ……リスク#n）
1.1 製品の安全性 （危害）	ソフトウェアが故障した際に懸念される製品安全性への潜在的なリスクは存在するか？ • 患者への危害 • オペレーターへの危害 • 傍観者への危害 • サービス担当者への危害 • 環境への危害	
1.2 製品の安全性 （危害）	ソフトウェアのユーザーがミスを犯した際に懸念される製品安全性への潜在的なリスクは存在するか？ • 患者への危害 • オペレーターへの危害 • 傍観者への危害 • サービス担当者への危害 • 環境への危害	
2.1 製品クオリティ	ソフトウェアが故障した際に懸念される製品クオリティへの潜在的なリスク（安全性のリスクを除く）は存在するか？	
2.2 製品クオリティ	ソフトウェアのユーザーがミスを犯した際に懸念される製品クオリティへの潜在的なリスク（安全性のリスクを除く）は存在するか？	
3.1 記録の完全性	記録を保管するシステムに記録の完全性への潜在的なリスクは存在するか？ • 記録消失 • 記録損傷	
4.1 **FDA/ISO 規格の** **遵守証明**	規格遵守を証明する能力に関する潜在的なリスクは存在するか？ • 記録消失 • 記録損傷 • 規制プロセス要件（マネジメントコントロール、CAPA、サービス及びサポートなど）に対する自動化プロセスの不適合	

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。