REDUCING RISKS AND RECALLS

Safety Assurance Cases For Medical Devices

Sherman Eagles and Fubin Wu

About the Authors

Sherman Eagles is a partner at SoftwareCPR, a consulting and training company specializing in FDA compliance and conformance with international standards. Eagles also is lead instructor for the AAMI Safety Assurance Case course, as well as a former technical fellow at Medtronic. E-mail: seagles@softwarecpr.com

Fubin Wu is cofounder of GessNet. He previously served as quality director and manager with Medtronic, Hospira, and Haemonetics. E-mail: fubin.wu@gessnet.com

Reports of medical device safety-related issues have increased considerably during the previous few years. The U.S. Food and Drug Administration (FDA) reported that Class I recalls have increased more than 100%, from an average of 25 per year before 2008 to 50 in 2011 and 57 in 2012.[1] A Class I recall deals with a situation in which a reasonable probability exists that use or exposure to a medical device will cause serious adverse health consequences or death. In the United Kingdom, the increase in safety-related issues is even more dramatic, with field safety alerts increasing from 62 in 2006 to 757 in 2010—an increase of nearly 1,200%.[2] In addition to safety having serious implications for patients, the economic and legal impact of recalls to manufacturers, user facilities, and users can be substantial or even catastrophic.

A frequent cause of these recalls is that a hazardous scenario is not identified or adequately controlled before the device is available on the market. Demands for increased functionality, such as interoperable medical devices, are increasing the complexity and sophistication of medical technology and healthcare infrastructure. Those demands also are introducing additional hazardous situations, such as cybersecurity vulnerabilities, and adding more difficulties for the industry and regulators. Even a seemingly simple device may not be that simple from a safety perspective, given the complexity of its use environments. Ensuring proper identification and control of hazardous situations and causes has become more critical than ever. We need to challenge the status quo of existing methods and identify new or improved methods to ensure medical device safety in today's environment. Safety assurance cases offer a means to address this critical issue.

Limitations of Medical Device Risk Management Practices

Before turning to safety assurance cases, considering current risk management practices and understanding their limitations might be helpful. Per the standard ANSI/AAMI/ISO 14971, risk management is a systematic life cycle process to identify, control, and evaluate risk, where risk is defined as the combination of severity of the harm (to people, property, or environment) and probability of occurrence of the harm. As a process standard, 14971 defines a general philosophy and process framework and allows the individual organization or company to define and implement the specifics of how to identify, control, and evaluate risks. Different organizations and companies use different methods and practices to implement the standard. The effectiveness of these methods and practices can vary as a result of their inherent limitations. Table 1 summarizes a list of commonly used risk management methods and practices and corresponding limitations.

Ref. no.	Commonly used risk management methods and practices	Limitations
1	Bottom-up analysis methods (e.g., failure mode and effects analysis)	Difficult to identify all system-level hazardous situations. Difficult to identify system or component interaction failures, which can result from design flaws or unsafe interactions among nonfailing systems or components. Difficult to identify an end-to-end causal chain of all contributing factors and conditions that can lead to a hazardous situation.
2	Top-down analysis methods (e.g. hazard analysis, fault tree analysis)	Difficult to identify all the low-level causes, including conditions and events that could contribute to a hazardous situation. Impractical amount of effort to analyze all ways that an undesirable event could be caused by a component failure or component interaction.
3	Top-down and bottom-up analysis performed independently	Difficult to identify the end-to-end causal chain that leads to a hazardous situation. Difficult to identify all possible opportunities for which risk controls can be applied.
4	Risk determination (e.g., risk priority numbers) used as an acceptability criteria when the probability cannot be quantitatively assessed	Difficult to identify objective evidence and rationale that the risk is acceptable. Difficult to manage risk acceptance over the product life cycle as the environmental and use conditions evolve.
5	Risk traceability matrix (e.g., traceability between hazardous situations, causes, risk controls, requirements, testing) used as assurance that risk controls are established	Difficult to ensure that risk controls are implemented correctly and appropriately. The traceability shows the risk control is linked to objective implementation evidence but doesn't provide reviewable information that explains why the implementation is correct and appropriate.
6	Methods that do not document context and assumptions explicitly	Difficult to identify the environmental and use conditions and assumptions that can have a major safety impact.

Table 1. Limitations of Common Risk Management Methods and Practices

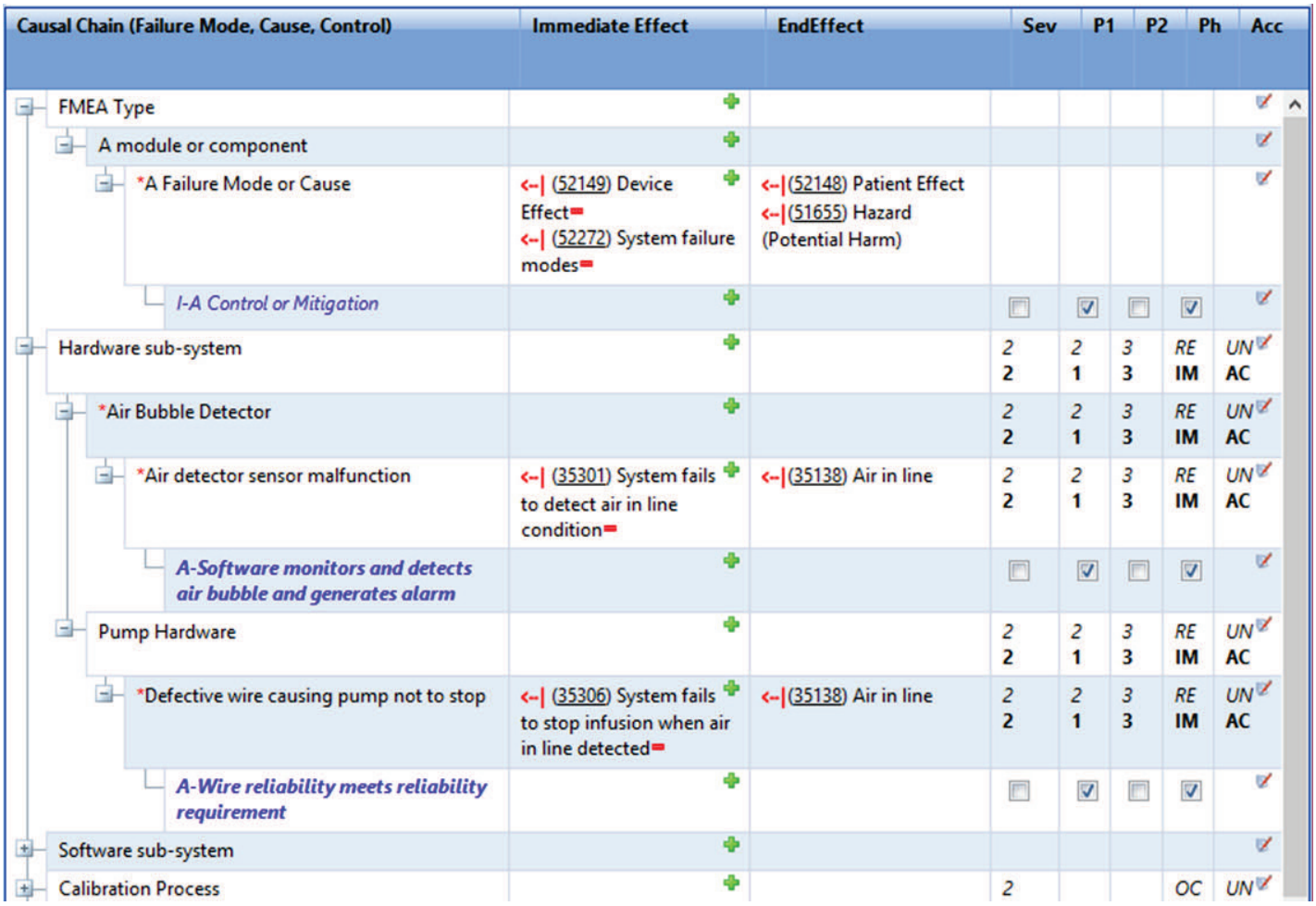

Figure 1. Example of Bottom-Up Analysis: Failure Mode and Effect Analysis (courtesy of GessNet[3])

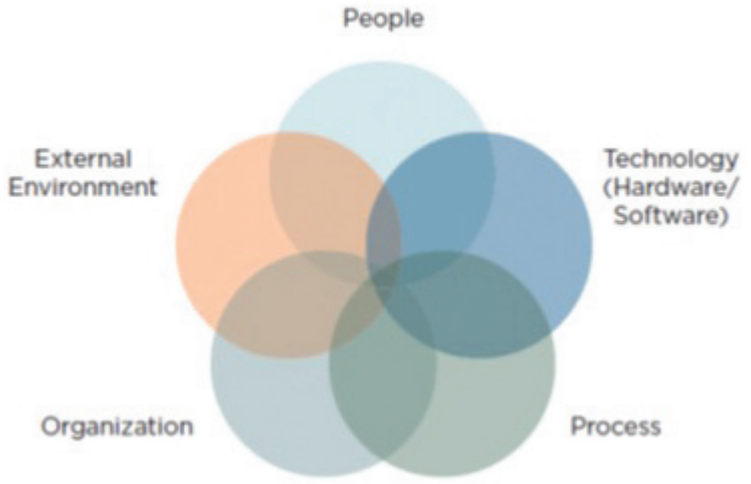

Figure 2. Sociotechnical System Underlying Health Information Technology–Related Adverse Events (courtesy of IOM[4])

Limitations of Bottom-Up Analysis

Bottom-up (e.g., subsystem or component failure mode and effects analysis) risk analysis (illustrated in Figure 1)[3] has been used for medical devices for several decades. Initially, it was used to identify potential hardware component failures (single faults) and predict the possible consequences and likelihood of these failures. Bottom-up risk analysis has made many devices safer and continues to make a valuable contribution to device safety. However, as medical devices and the environments in which they are used become more complex, taking component and subsystem interactions into consideration when specifying failure modes and their consequences becomes increasingly important.

The Institute of Medicine (IOM) has characterized the complex environment in hospitals as a sociotechnical system (Figure 2).[4]

The bottom-up analysis focuses on identifying device component failures. It would be difficult for this method to identify all the causes, including interactions among environmental conditions, use conditions. and nonfailing components that can lead or contribute to a hazardous situation or harm (Figure 3).[3]

*Limitations of Top-Down Analysis**

Top-down analysis (e.g., system fault tree analysis) provides another method for identifying causes of an undesirable event. It starts by assuming that harm has occurred and identifying the hazardous situations (i.e., the circumstance in which people, property, or the environment are exposed to one or more of the hazards that could have caused the harm). Further analysis is conducted to determine the system-level factors (device faults, use conditions, or events) that could cause or contribute to the hazardous situation, followed by the subcauses from subsystems or components that could lead to the system-level faults. Figure 3 illustrates the results of a top-down analysis.[3]

Top-down analyses are limited in that identifying all the low-level causes, conditions, and events that contribute to an unintended event is difficult. For example, a fault tree analysis is not efficient at identifying all possible causes of hazardous situations from every subsystem and component, and it likely is impractical when a large number of subsystems and components are in play.

Limitations of Independent Top-Down and Bottom-Up Analyses

Choosing how to control the evolution of a causal chain so that harm is prevented is called risk control analysis in 14971.[5] Referring

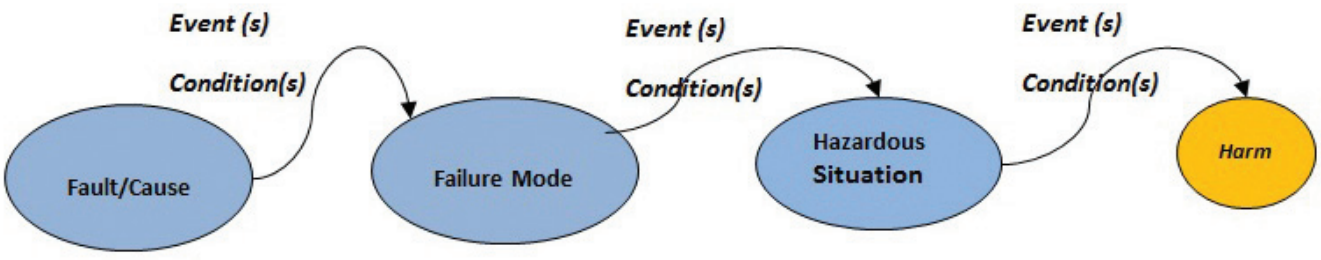

Figure 3. An End-to-End Causal Chain for a Hazard (courtesy of GessNet[3])

* Different organizations and companies use different methods and practices to implement the standard. Their effectiveness can vary.

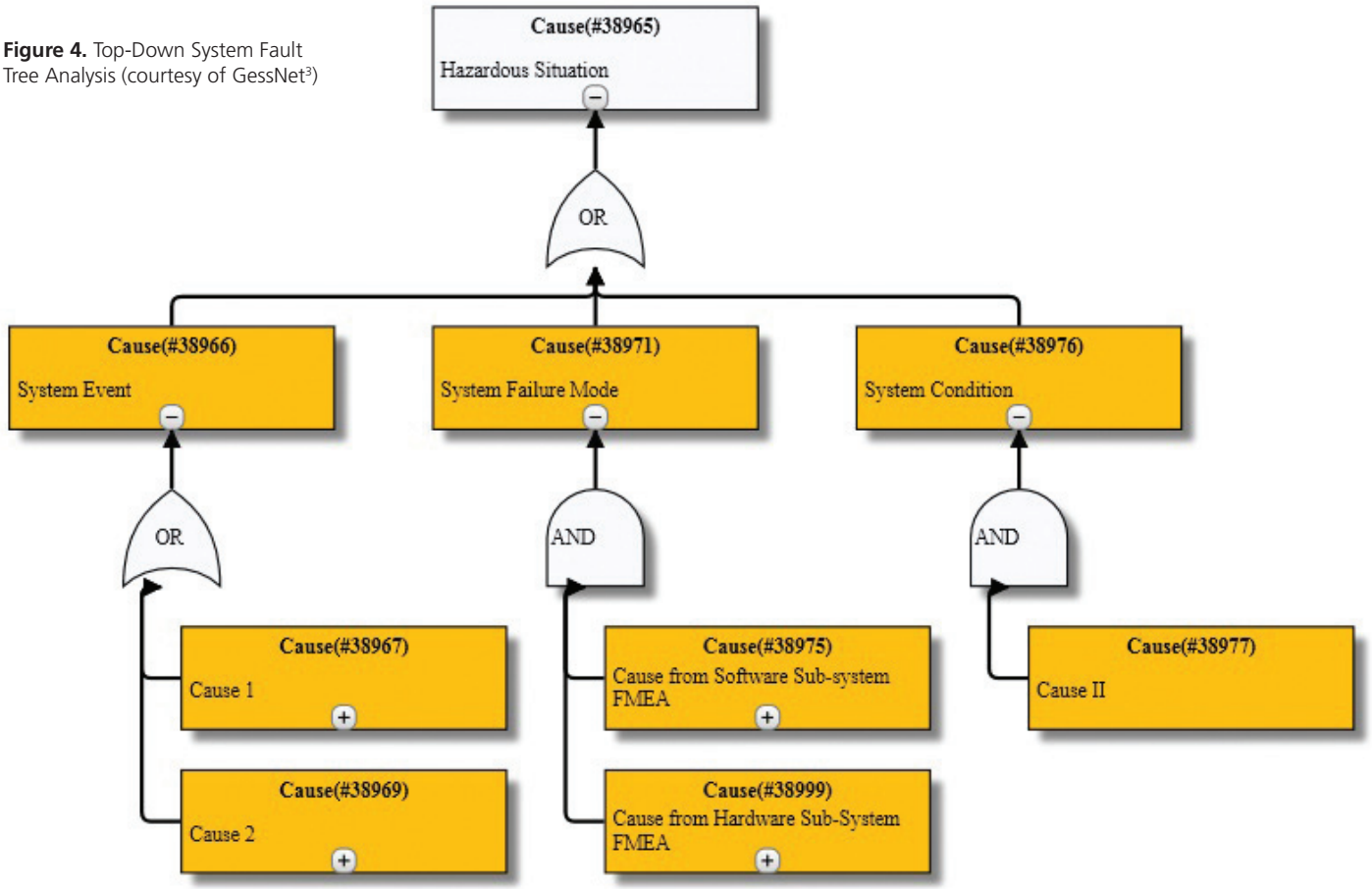

Figure 4. Top-Down System Fault Tree Analysis (courtesy of GessNet[3])

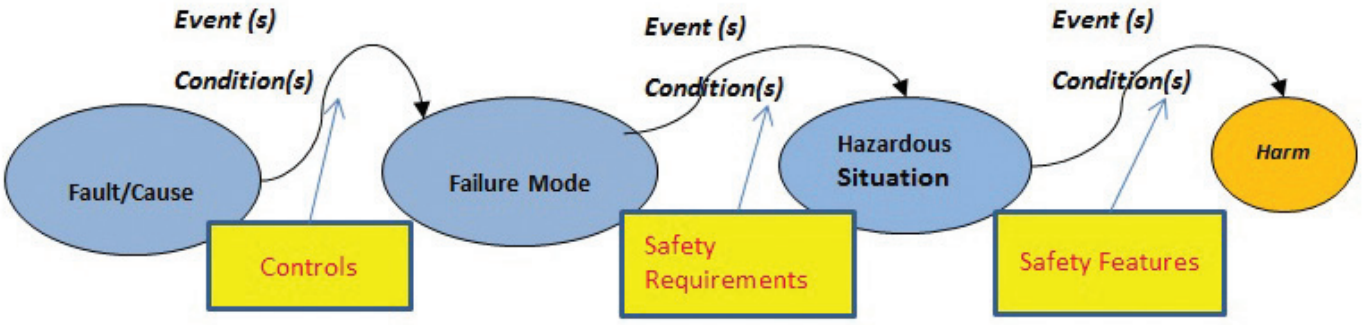

Figure 5. Location of Risk Control Measures in a Causal Chain (courtesy of GessNet[3])

again to the causal chain diagram, identifying risk control measures at multiple stages of the causal chain is possible (Figures 5 and 6).[3]

To effectively apply risk control measures at different stages, the causal chain (Figure 5) should be identified explicitly. If the end-to-end causal chain is not defined, opportunities to apply risk controls at multiple stages are likely to be missed. Performing top-down and bottom-up risk analysis methods independently does not ensure that the effects identified during bottom-up analysis are linked properly to the system failures or hazardous situations identified during the top-down risk analysis. Therefore, an end-to-end causal chain may not be identified completely.

Limitations of Risk Determination Methods Used as Acceptability Criteria

Per 14971, risk is the combination of severity of potential harm and probability of the harm occurrence. Because practical methods for quantitatively estimating the probability of design flaws (e.g., software defects) and use conditions and event occurrence (e.g. user,

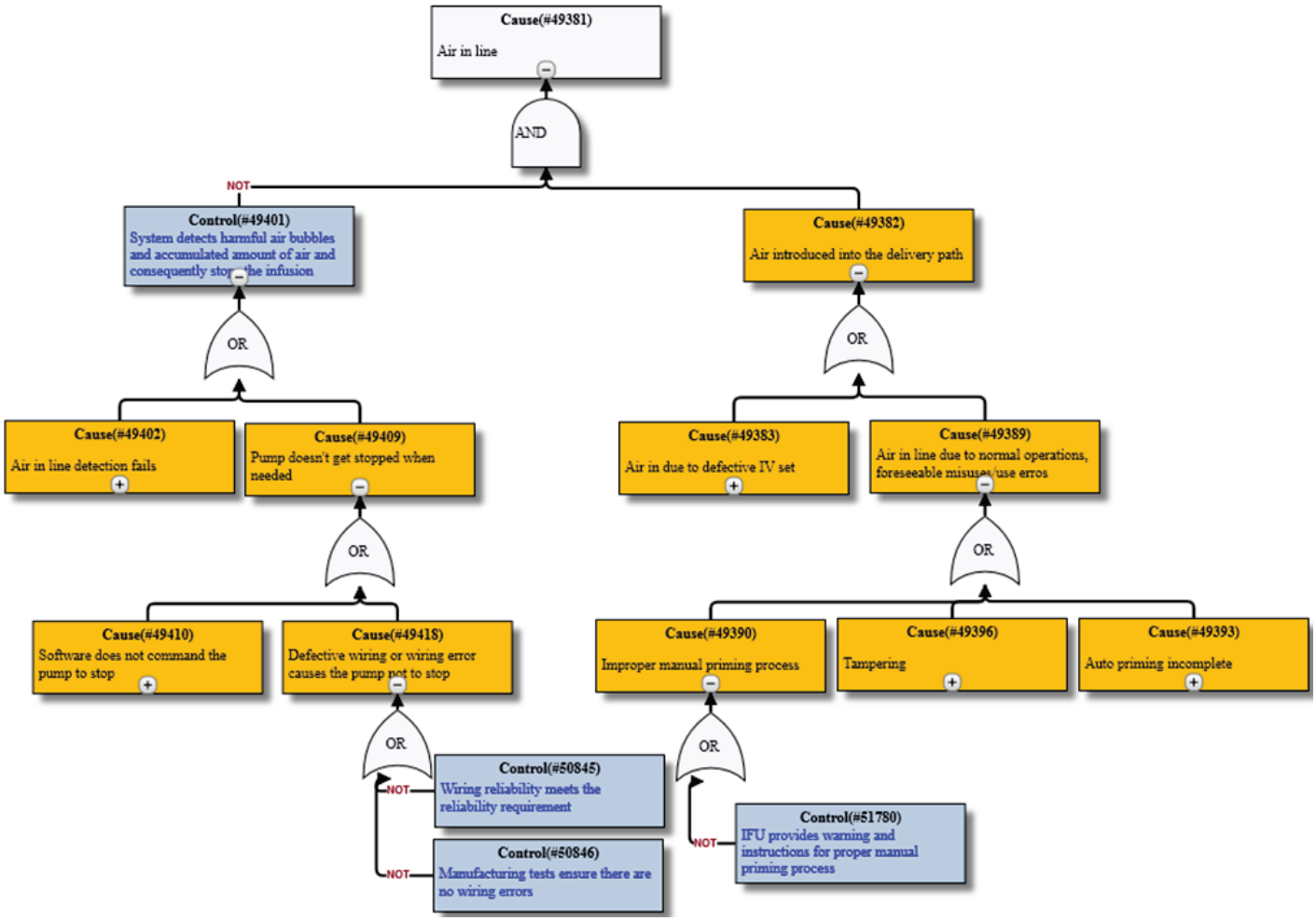

Figure 6. Location of Risk Control Measures (in blue) in a Causal Tree (courtesy of GessNet[3])

environmental, and system interactions) do not exist, risk acceptability often is evaluated based on probability determination resulting from team consensus or judgment calls. In other words, for a known severity, the risk acceptance is based on probability that is a qualitative (nonquantitative) estimate. However, in many cases, the qualitative criteria used, the rationale, and the associated objective evidence are not documented. This may lead to a situation in which the risk acceptance is determined subjectively without support of objective evidence. In addition, risk management is a product life cycle process. The qualitative criteria that are adequate at one time may not be adequate over a product's life time. If the criteria used during the initial risk acceptability process are not documented, then managing risk acceptance and making adjustments and improvements during the remainder of the product life cycle will be difficult.

Limitations with Risk Traceability Matrix. As shown in Figure 7, a risk traceability matrix is a common method to ensure that risk controls are traceable to objective implementation evidence such as product requirements, design, verification and validation, and standard operating procedures.

This method is effective to ensure that risk controls are implemented. The limitation is that this traceability is not comprehensive for ensuring the adequacy and correctness of the risk controls implementation. From a reviewer (internal or external) perspective, the traceability matrix is useful in identifying objective implementation evidence for which one should be cognizant; however, it does is not provide sufficient information for the reviewer to evaluate whether the implementation is correct and appropriate.

Hazard Causal Chain (Hazard, Failure Mode, Cause, Control)	Sev	P1	P2	Ph	Acc	Requirements	Verification	Validation	CAPAs	Complaints	SOPs
Air in line	2 2	3 1	3 3	OC IM	UN AC						
*Air introduced into the delivery path.	2 2	3 2	2 2	RE IM	AL AC						
I-System detects air, generates alarm and stops infusion	☐	☑	☐	☑		Req #234	TC #001	Val #02			
System fails to detect air in line condition											
*Air detector sensor malfunction	2 2	2 1	3 3	RE IM	UN AC				#668	#3689	
A-Software monitors and detects air bubble and generates alarm	☐	☑	☐	☑		Req #8679	TC #003	Val #03			
Inaccurate reference used	2 2			OC IM	UN AC						
System fails to stop infusion when air in line detected											
*Defective wire causing pump not to stop	2 2	2 1	3 3	RE IM	UN AC						

Figure 7. Risk Traceability Matrix Example (courtesy of GessNet[3])

Limitations of Methods that Do Not Explicitly Document Context and Assumptions.

As illustrated in Figure 3, many factors are related to the safe use of medical devices. These factors define the external environmental conditions and use conditions for a device, which can be critical to safety. For example, a patient's lifestyle can have a major impact on the reliability (and therefore safety) of an implantable cardiac defibrillator lead. Similarly, a hospital's protocols and workflow can affect the safe operation of a device (e.g., infusion pump) considerably. The underlying context and assumptions for safety-related design decisions are critical information that should be documented and communicated. These factors also change over time as the healthcare system evolves. Documenting these factors is essential for effective design reviews and continuously building knowledge for improvements. Although some of this knowledge may be documented in the design or requirement documents, risk management documentation typically does not explicitly capture the context and assumptions associated with risk analysis.

Addressing Shortcomings in Common Risk Management Methods

Safety assurance cases for medical devices have been described by researchers,[6,7] have been recommended in an IOM study,[8] and now are included in the FDA draft guidance for 510(k) submissions of infusion devices.[9] A safety assurance case is a method for demonstrating the validity of a safety claim by providing a convincing argument together with supporting evidence (Figure 8). This body of argument explains why the identification of applicable hazards, hazardous situations, and causes (device faults, defects, use conditions, events, and other contributing factors) is adequate and why the particular risk controls chosen are adequate, individually effective, and collectively sufficient to reduce the overall residual risk to an acceptable level.

A safety assurance case for a medical device is argued in a hierarchical fashion with a top-level claim (e.g., declaring an infusion pump to be reasonably safe) and multiple layers of subclaims (e.g., stating that the risk of an overdose hazard is mitigated to an acceptable level) (Figure 9). Each subclaim is supported by an appropriate argument (and objective evidence, if applicable), and at the lowest level, each subclaim also is supported by objective evidence. The architecture of the safety assurance case is to lay out a logical structure of subclaims that support the top claim that the device is safe for its intended use, as shown in the "claims" column of Figure 9.

The underlying context and assumptions for safety-related design decisions are critical information that should be documented and communicated. These factors also change over time as the healthcare system evolves.

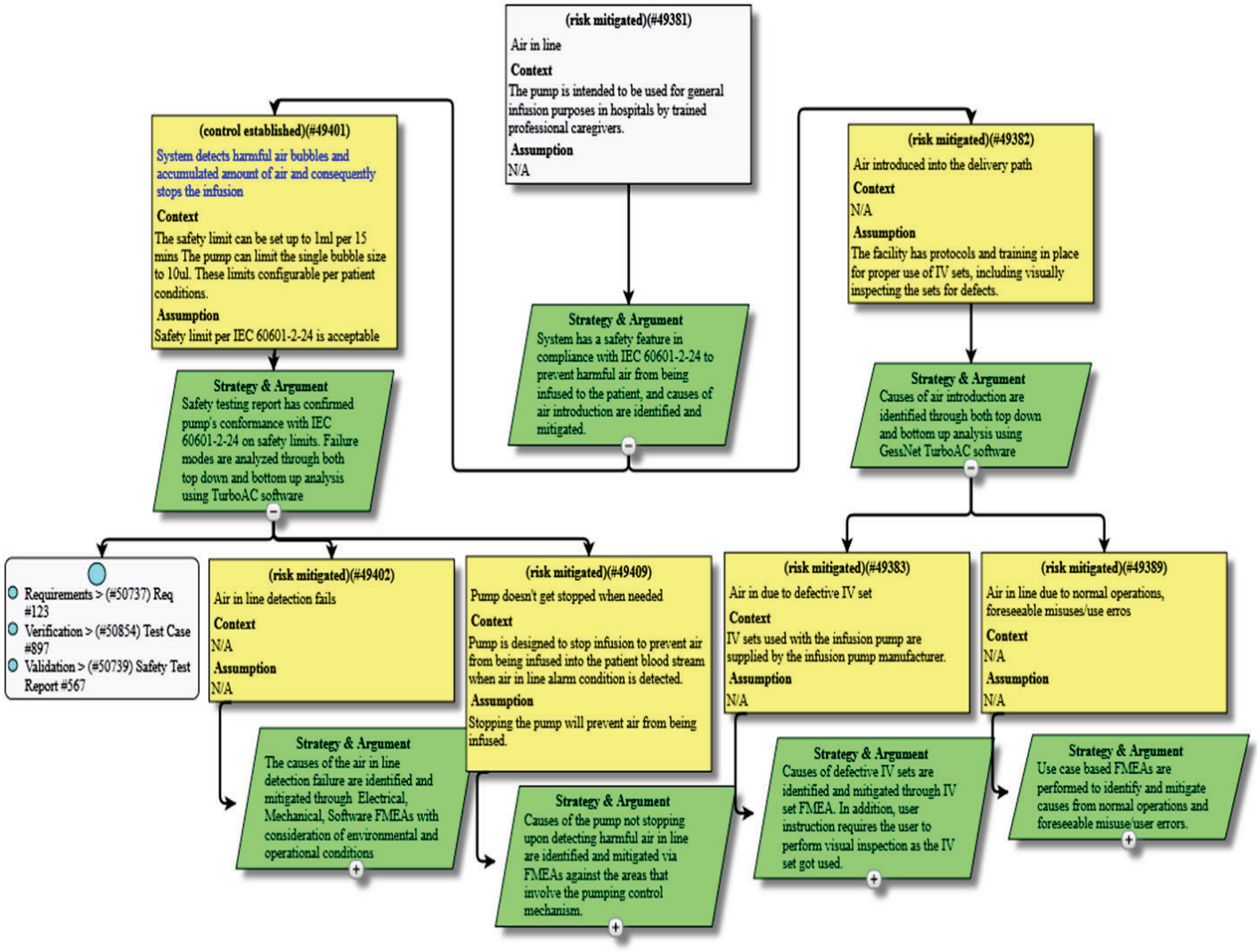

Figure 8. Safety Assurance Case Graphic Example (courtesy of GessNet[3])

This requires proper identification of hazardous situations and possible cause and effect chains (i.e. causal chains) that can lead to the hazardous situations, as illustrated by Figure 7. Without systematically understanding the top-level hazardous situations and associated causal chains, identifying the subclaims that are cohesive to formalize a convincing safety assurance case architecture would be impossible. The architecture of a safety assurance case exercises a top-down analysis to support the top claim. This addresses the limitations of the bottom-up analysis methods, as discussed above (Table 1, ref. 1).

Two critical elements of a safety assurance case are "argument" and "evidence."

Argument addresses the limitations for a number of risk management methods. First, each claim that has subclaims of "risk is mitigated" for a hazardous situation or a cause should have an argument to explain why its subclaims are sufficient to support it as the parent claim. Developing an argument for the parent claim requires critical thinking of why its decomposition into subclaims is complete and correct. This critical thinking stimulates the identification of hazardous situations, causes, or subcauses, including low-level causes that can be more efficiently identified using a bottom-up analysis. This confirms that the bottom-up analysis needs to be performed adequately and that it needs to be connected logically to the top-down analysis. As such, the limitations with top-down analysis methods (Table 1, ref. 2) and the limitations with independent top-down and bottom-up analyses are addressed (Table 1, ref. 3).

Second, each claim of "risk is mitigated" that has "risk control is established" as subclaims should have an argument to explain why the risk controls collectively reduce the risk to an acceptable level. This argument should refer to valid quantitative assessment results or valid (i.e., justifiable) qualitative criteria as objective evidence. This argumentation addresses the limitations with the risk determination method (i.e., the objective evidence is not always documented) (Table 1, ref. 4).

Claims		Strategy & Argument
Top Claim	ABC Medical Device is safe for its intended use	Argue that all applicable hazards are identified and mitigated. Confidence argument on why hazards are identified correctly, completely and appropriately
⇓ **Top Sub-Claims**	Sources of **Harm** (Top Hazards) are Mitigated	Argue that hazardous situations are identified and mitigated. Confidence argument on why hazardous situations are identified correctly, completely and appropriately
⇓⇓ **Sub- Claims**	Risk of **Hazardous Situations** is Mitigated	Argue that causes are identified and mitigated. Confidence argument on why causes are identified correctly, completely and appropriately
⇓⇓⇓ **Sub-Claims**	Risks of **Causes** are Mitigated	Argue that sub-causes are identified and mitigated. Confidence argument on why sub-causes are identified correctly, completely and appropriately
⇓⇓⇓⇓ **Sub-Claims**	Risks of **Sub-Causes** are Mitigated	Argue that controls are established. Confidence argument on why control (s) are collectively sufficient to reduce the risk (severity or probability) to be at acceptable level
⇓⇓⇓⇓⇓ **Sub-Claims**	**Risk Controls** are established	Argument on why control implementation is correct, complete and appropriate

Figure 9. Medical Device Safety Assurance Case Structure (courtesy of GessNet3)

Third, each claim of "control is established" is supported by implementation evidence, such as requirements, procedures, and verification, and by an argument of how and why the evidence supports the claim that risk control implementation is adequate and correct. This addresses the limitation with the risk traceability matrix (Table 1, ref. 5).

A safety assurance case structure requires context and assumption as part of the default template for every claim. Explicitly documenting the context and assumptions stimulates critical thinking and captures knowledge that otherwise may not be documented anywhere (Table 1, ref. 6).

In summary, a safety assurance case achieves the following criteria:

- Provides a framework and a vehicle to stimulate critical thinking
- Ensures the completeness of risk identification and risk controls
- Provides rationale for the validity of risk acceptance
- Logically documents and connects safety critical information in an easily understandable manner
- Communicates safety critical information effectively to internal and external stakeholders

For example, the structured documentation provided by a safety assurance case can help an independent reviewer evaluate the rationale and evidence for safety efficiently and effectively, without requiring the same level of familiarity with the device as a member of the development team. These benefits ultimately help ensure the safety of medical devices.

Risk Management and Safety Assurance Case Tool Needs

To establish effective risk management practices and safety assurance cases without electronic tools can be very challenging as a result of the need for multiple analysis techniques; the amount of information to be managed; and the needs of organizing, linking, presenting, and maintaining this information through the product life cycle. A tool that can facilitate both top-down and bottom-up analyses, connect the top-down and bottom-up analyses, integrate the safety assurance case method into risk management, and intuitively ensure that limitations with existing risk management methods are addressed can provide substantial benefit. In addition, from a safety assurance case review perspective, the information must be

Explicitly documenting the context and assumptions stimulates critical thinking and captures knowledge that otherwise may not be documented anywhere.

presented in a format that is easy to review. Unfortunately, that which is considered easy to review is subjective and varies among reviewers. Although a narrative format can be used, most reviewers seem to prefer either a graphical (Figure 8) or tabular (Figure 10) presentation of the case. Tools that provide reviewers with interchangeability and seamlessness can provide considerable value for facilitating and accelerating the review process.

Conclusion

Although many medical device manufacturers do a good job complying with the ISO 14971 risk management standard, more safety recalls are occurring in increasingly complex devices and environments. Existing risk management methods and practices in today's complex medical technology environment have limitations. By requiring a holistic body of argument that is logically structured with supporting objective evidence, safety assurance cases connect the dots and propose the right questions for ensuring safety in complex situations. They intuitively guide critical thinking on product safety and push toward complete and effective risk management. Exercising this critical thinking will result in more complete identification of scenarios leading to hazardous situations and more adequate and effective risk controls. Ultimately, it will reduce product recalls by addressing the frequent causes of the recalls. ■

References

1. **Medical Device and Diagnostic Industry.** CDRH 'Puzzled' by Class 1 Recalls Jump. mddionline. December 7, 2012. Available at: www.mddionline.com/article/cdrh-%E2%80%98puzzled%E2%80%99-class-1-recalls-jump. Accessed Nov. 11, 2013.
2. **Heneghan C, Thompson M, Billingsley M, et al.** Medical-device recalls in the UK and the device-regulation process: retrospective review of safety notices and alerts. BMJ Open. 2011;1(1):e000155.
3. **GessNet.** GessNet TurboAC Risk Management and Assurance Case Software White Paper. Available at: http://gessnet.com/files/GessNet_TurboAC_White_Paper_July.pdf. Accessed Nov. 10, 2013.
4. **Institute of Medicine.** *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, DC: National Academies Press; 2012.
5. **International Organization for Standardization.** ISO 14971:2007: Medical Devices–Application of Risk Management to Medical Devices. Geneva: International Organization for Standardization; 2007.
6. **Weinstock C, Goodenough J.** *Towards an Assurance Case Practice for Medical Devices.* Arlington, VA: Software Engineering Institute: 2009.
7. **Ray A.** Assurance Cases: Their Use Today and the Challenges Ahead. *BI&T.* 2012;46(3):195-200.
8. **Institute of Medicine.** *Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years.* Washington, DC: National Academies Press' 2011.
9. **Food and Drug Administration.** Guidance for Industry and FDA Staff: Total Product Life Cycle: Infusion Pump: Premarket Notification [510(k)] Submissions. Available at: www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm. Accessed Nov. 10, 2013.

Figure 10. Tabular Format Safety Assurance Case (courtesy of GessNet3)

Claim: risk of [Air in line] is mitigated	Context & Assumption	Strategy & Argument	Evidence & Reference
Air in line	Context: The pump is intended to be used for general infusion purposes in hospitals by trained professional caregivers. Assumption: N/A	System has a safety feature in compliance with IEC 60601-2-24 to prevent harmful air from being infused to the patient, and causes of air introduction are identified and mitigated.	
A-System detects harmful air bubbles and accumulated amount of air and consequently stops the infusion	Context: The safety limit can be set up to 1ml per 15 mins The pump can limit the single bubble size to 10ul. These limits are configurable per patient conditions. Assumption: Safety limit per IEC 60601-2-24 is acceptable	Safety testing report has confirmed pump's conformance with IEC 60601-2-24 on safety limits. Failure modes are analyzed through both top down and bottom up analysis using TurboAC software	Requirements > Req #123 Verification > Test Case #897 Validation > Safety Test Report #567
Air in line detection fails	Context: N/A Assumption: N/A	The causes of the air in line detection failure are identified and mitigated through Electrical, Mechanical, Software FMEAs with consideration of environmental and operational conditions	
Pump doesn't get stopped when needed	Context: Pump is designed to stop infusion to prevent air from being infused into the patient blood stream when air in line alarm condition is detected. Assumption: Stopping the pump will prevent air from being infused.	Causes of the pump not stopping upon detecting harmful air in line are identified and mitigated via FMEAs against the areas that involve the pumping control mechanism.	
Air introduced into the delivery path	Context: N/A Assumption: The facility has protocols and training in place for proper use of IV sets, including visually inspecting the sets for defects.	Causes of air introduction are identified through both top down and bottom up analysis using GessNet TurboAC software	
Air in due to defective IV set	Context: IV sets used with the infusion pump are supplied by the infusion pump manufacturer. Assumption: N/A	Causes of defective IV sets are identified and mitigated through IV set FMEA. In addition, user instruction requires the user to perform visual inspection as the IV set got used.	
Air in line due to normal operations, foreseeable misuses/use erros	Context: N/A Assumption: N/A	Use case based FMEAs are performed to identify and mitigate causes from normal operations and foreseeable misuse/user errors.	