Medical Device Recalls, Risk Management, and Safety Assurance Cases

Fubin Wu

Co-founder of GessNet™, a software and consulting company specializing in medical device risk management and safety assurance cases

Introduction

Objectives

- Understand common causes of device recalls in relation to risk management
- Understand common risk management methods & practices and associated limitations through examples
- Understand safety assurance case basics and its relation to risk management
- Understand through a template how risk management and safety assurance case can be integrated
- Understand how safety assurance case can help to address limitations with common risk management methods & practices
- Ask FDA questions about risk management and safety assurance cases

FDA participants are available for questions after the session content has been presented

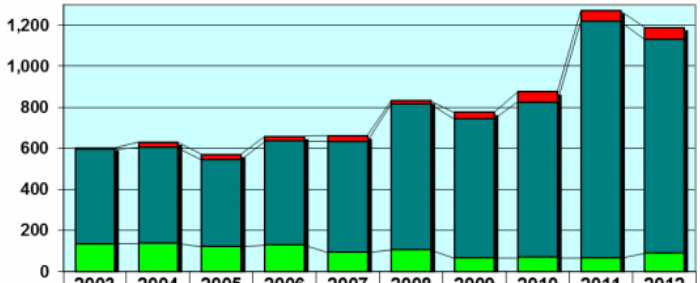
- **Lorie Erikson**, Consumer Safety Officer, Office of Compliance, Cardiovascular Devices Branch, CDRH FDA
- **Ryan McGowan**, ODE reviewer, General Hospital Devices Branch, CDRH FDA
- **Alan Stevens**, Lead Reviewer, General Hospital Devices Branch, ODE CDRH FDA
- **Richard Chapman**, Chief of General Hospital Devices Branch, ODE CDRH FDA

Agenda

- **Medical Device Recalls (**Fubin Wu & Lorie Erikson**)**
  - Most Recent FDA Medical Device Recall Report
  - Recall Example
  - Common causes of recalls and its relation to Risk Management
- **Medical Device Risk Management (**Fubin Wu**)**
  - Common Methods & Practices with Examples – ISO 14971, Hazard Analysis, Fault Tree Analysis, Bottom Up Analysis (e.g. FMEAs), Risk Traceability Matrix
  - Limitations with each of the Common Methods & Practices in reducing device recalls
- **Medical Device Safety Assurance Cases (**Fubin Wu**)**
  - History of Safety Assurance Cases for Medical Devices
  - FDA Safety Assurance Case Pilot Program
  - Safety Assurance Case Fundamentals
  - Structure of Safety Assurance Cases for Medical Devices and its relations to risk management
  - Medical Device Safety Assurance Case Template in integrating with risk management
  - How Safety Assurance Cases can help to address the limitations with common risk management methods & practices
  - Medical Device Safety Assurance Case Example
- **Q & As with FDA**

Medical Device Recalls

(data source: FDA Medical Device Recall Report FY2003~FY2012)



	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Class I	7	24	26	22	26	14	32	49	50	57
Class II	460	467	422	505	540	710	677	753	1,152	1,043
Class III	137	140	124	132	96	108	67	74	69	90
Totals	*604*	*631*	*572*	*659*	*662*	*832*	*776*	*876*	*1,271*	*1,190*

Medical Device Recalls

(data source: FDA Medical Device Recall Report FY2003~FY2012)

Key Observations for Figure 6:

- Overall annual recall counts increased 97%, from 604 recalls in FY 2003 to 1,190 recalls in FY 2012.
- Increases were observed in the annual number of both Class I and II recalls.
  - Class I recalls represented 1% of recalls in FY 2003 (7 recalls), but comprised nearly 5% (57 recalls) in FY 2012.
  - The annual number of Class II recalls more than doubled from FY 2003 to FY 2012.
  - The number of Class III recalls declined by approximately 35% during the study period.

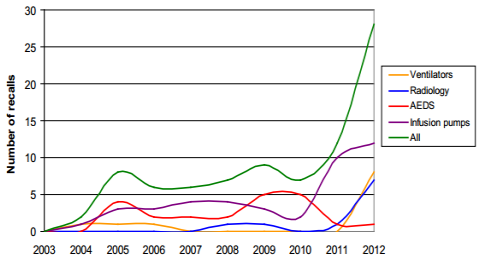
Recall classification is guided by FDA's determination of the risk associated with the device failure.

Class I Recalls

(data source: FDA Medical Device Recall Report FY2003~FY2012)

A class I recall is a situation in which there is a reasonable probability that use, or exposure to, a violative device will cause serious adverse health consequences or death

Figure 12: Class I Recalls for Specific Device Types



Comparison of the Class I to Class II recalls over the study period revealed different distributions by medical specialty. Most of the Class I recalls were in the anesthesia, cardiovascular, chemistry, and general hospital specialties (Figure 13). The radiology, orthopedic, general hospital, and cardiovascular areas had the most Class II recalls.

Impact of medical device recalls

- Patient Safety
- Financial impact
- Legal impact
- Brand/reputation
- …

2011 New York Times: XXX's Profit Falls 12%, Hurt by Series of Recalls

"… The company took an after-tax charge of $922 million for litigation settlements, a recall of poorly fitting xxx hip implants and an increase in its product liability reserve…"

Class I Recall Example

Food & Drug Administration
Center for Devices and Radiological Health
Office of Compliance
Division of Manufacturing and Quality
Lorie Erikson, CSO

2014 Class I Recall

- Device: Class II Guidewire
  - Steerable guidewire with a hydrophilic coating, used to place catheters and other diagnostic devices during invasive medical procedures, which is used in hospitals and other healthcare facilities
- Reason for Recall:
  - Outer polymer jacket of the core wire may be damaged or torn during use, such as when the guidewire is quickly withdrawn through certain delivery catheters

2014 Class I Recall

- Risk to Health:
  - Reduction in or blocked blood flow due to embolization of the torn polymer on the damaged jacket
    - Which can further lead to blood vessel blockage or damage
  - May require surgical intervention to resolve blockages in the blood vessel.

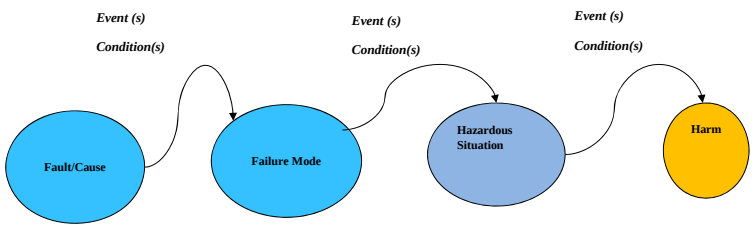
2014 Class I Recall

- Why this example?
  - Damaged or torn **during use**
  - Great example of the need for firm's to understand how the device is being handled by the end user.
  - Not only at the inception or during design activities associated with the device, but during post-market use of the device.

Causes of Recalls

Why recalls?

- a hazardous scenario (risk) is not identified or adequately controlled prior to the device being placed on the market.



Recall Prevention/Reduction - Challenges

Why the risk is not identified or adequately controlled prior to being placed on the market?

- Potential hazardous situations, causes or contributing factors are not completely identified
- Determinations of risk acceptance, risk control effectiveness are made based on incorrect or incomplete "beliefs", context or assumption
- Development process miss it, Manufacturing process miss it, and Review process miss it
- …

Why miss it? too hard

- Complexity of device use environments
- Advanced functionality - integrated with software …
- New technologies/platforms – wireless, drug/device combination products …
- Increased interoperability, system of systems
- Large amount of information/documentation, connecting dots is not easy
- Moving target – continuously evolving use conditions, and contributing factors

Challenge to Risk Management Process

How to effectively assure proper identification and adequate control of hazardous situations and causes prior to the device being placed on the market and throughout the device life?

Risk Management Current State

- ISO 14971 - a broadly adopted process standard for compliance purpose
  - a systematic life cycle process to identify, assess/evaluate, and control risk(s)
- As a process standard, ISO 14971 defines a general philosophy and process framework, and let the individual organization or company to define and implement the specifics of how to identify, control and evaluate risks
- Device is Safe because
  - Risk management activities are completed in compliance with ISO 14971
  - Risk analysis report concludes that overall residual risk is acceptable
  - ...
- Don't Forget
  - Different organizations and companies use different methods and practices to implement ISO 14971
  - The effectiveness of these methods and practices vary

Risk Management Current State Common Methods & Practices

I	Bottom Up Analysis Methods (e.g. FMEAs)
II	Top Down Analysis Methods (e.g. Hazard Analysis, Fault Tree Analysis)
III	Top Down and Bottom Up Analysis performed independently
IV	Risk Determination (e.g. RPNs) used as an acceptability criteria when the probability cannot be quantitatively assessed
V	Risk Traceability Matrix (i.e. traceability between hazardous situations, causes, risk controls, requirements, and testing etc.) used as assurance that risk controls are established
VI	Methods that do not explicitly document context and assumptions
VII	Pre-market and post market risk management process (people, activities and results) are not connected or loosely connected

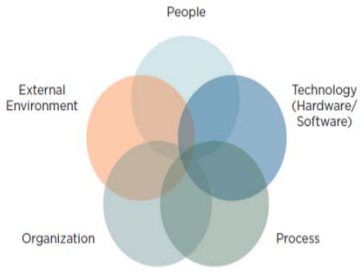
Device Background for some of the examples used

- External infusion pumps are medical devices that deliver fluids, including nutrients and medications such as antibiotics, chemotherapy drugs, and pain relievers, into a patient's body in controlled amounts.
- Clinicians and patients rely on pumps for safe and accurate administration of fluids and medications..
- One of the common hazards is air in line, which can potentially cause air embolism.
- Many pumps have the safety feature to detect air in line situation and generate alarm.

Use Bottom Up Analysis (e.g. FMEAs) as the risk analysis

Causal Chain (Failure Mode, Cause, Control)	Immediate Effect	End Effect	Sev	P1	P2	RPN
Software sub-system						TBD TBD
Hardware sub-system			2 2	2 1	3 3	UN AC
Air Bubble Detector			2 2	2 1	3 3	UN AC
Air detector sensor malfunction	<-| (35301) System fails to detect air in line condition	<-| (35138) Air in line	2 2	2 1	3 3	UN AC
A-Software monitors and detects air bubble and generates alarm			☐	☑	☐	
Pump Hardware			2 2	2 1	3 3	UN AC
Defective wire or wire with errors causing pump not to stop	<-| (35306) System fails to stop infusion when air in line detected	<-| (35138) Air in line	2 2	2 1	3 3	UN AC
A-Wire reliability meets reliability requirement			☐	☑	☐	
I-Manufacturing testing ensures there are no wiring errors			☐	☑	☐	
Calibration Process			2 2			AL AC
Critical to Quality (CtQ)						

Use Bottom Up Analysis (e.g. FMEAs) as the risk analysis - limitations



Source: Sociotechnical System from IOM Report Health IT and Patient Safety: Building Safer Systems for Better Care

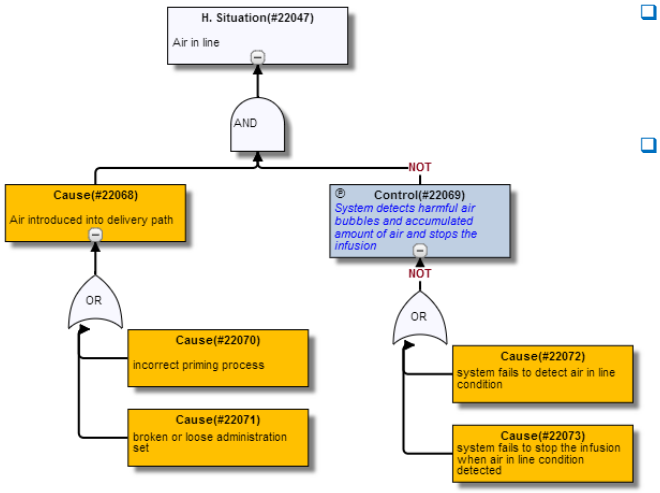
- Difficult to identify all system hazardous situations.
- Difficult to identify system or component interaction failures, which can result from design flaws or unsafe interactions among non-failing systems or components.
- Difficult to identify an end-to-end causal chain of all contributing factors and conditions that can lead to a hazardous situation.

Top Down Analysis Methods (e.g. Preliminary Hazard Analysis)

Safety Asset | Safety Harm | Hazard | Hazardous Situation | Security Asset | Security Harm | Threat | Vulnerability

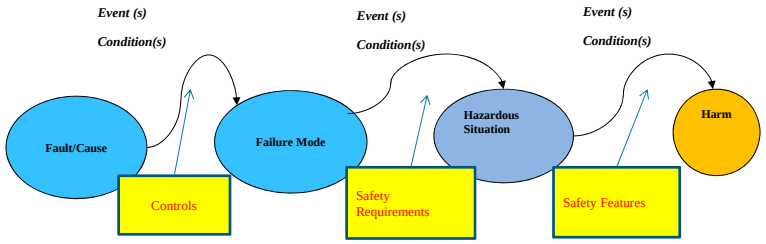
Hazard Causal Chain (Hazard, Failure Mode, Cause, Control)	Harms
Hazards	
Therapeutic	
Under Dose	
Pump infuses less insulin than what user has programmed per pump screen	(31597) Hyperglycemia (Serious)
Over Dose	
Pump infuses more insulin than what user has programmed per pump screen	(31596) Hypoglycemia (Critical)
Delay of Treatment	
User not able to issue remote commands due to non available or degraded wireless communications	(31623) Delay of Insulin Treatment (Minor)
Energetic	
Mechanical Force	
Chemical/biological	

Top Down Analysis Methods (e.g. 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 an undesirable event could be caused by a component failure or component interaction.

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 where risk controls can be applied.

RPNs used as an acceptability criteria while the probability cannot be quantitatively assessed

- Quantitative assessment of risk is very difficult given today's complexity of device functionality (e.g. software controlled) and its use and environmental conditions (e.g. human factors, system of systems)
- Risk acceptability is often evaluated based on probability determination that is the result of team consensus or judgment calls.
- However the qualitative criteria used, the rationale, and the associated objective evidence are not documented.
- This may lead to a situation where the risk acceptance is subjectively determined without support of objective evidence.
- If the criteria used during the initial risk acceptability process are not documented, then it will be difficult to manage risk acceptance and make adjustments and improvements during the rest of the product life cycle
- RPNs - **P**riority **N**umbers are Not Numbers for Risk Acceptance Determination

Use risk traceability matrix as the "assurance" that risk controls are established and effective

Hazard Causal Chain (Hazard, Failure Mode, Cause, Control)	Sev	P1	P2	Ph	Acc	Requirements	Verification	Validation	CAPA	Complaint	SOPs & WIs
Air in line	4 4	3 1	3 3	11 3	UN AC						
A-System detects harmful air bubbles and accumulated amount of air and consequently stops the infusion		☑	☑	☑		Req #123	Test Case #897	Safety Test Report #567			
Air in line detection fails	4 4	3 1	3 3	11 3	UN AC						
Pump doesn't get stopped when needed	4 4										
Software does not command the pump to stop	4 4										
Defective wiring or wiring error causes the pump not to stop	4 4										
A-Wiring reliability meets the reliability requirement		☑	☐	☑		Req #668		Reliability Prediction #36			
I-Manufacturing tests ensure there are no wiring errors		☑	☐	☑							WI1008 RevA
Air introduced into the delivery path	4 4										
Air in due to defective IV set	4 4										
Air in line due to normal operations, foreseeable misuses/use erros	4 4										

Use risk traceability matrix as the "assurance that risk controls are established and effective

- This method is effective to ensure risk controls are implemented.
- The limitation is that this traceability is not comprehensive for assuring the adequacy and correctness of the risk controls implementation.
- From a reviewer perspective, the traceability matrix is very useful to identify which objective implementation evidence to look at, but there is not enough information for the reviewer to evaluate whether the implementation is correct and appropriate.

Limitations of methods that do not explicitly document context and assumptions

- Environmental conditions and use conditions for a device can be critical to safety
- The underlying context and assumptions for safety related design decisions are critical information that should be documented and communicated
- Also having these factors documented is needed for effective design reviews and continuously building knowledge for improvements
- Current risk management documentation typically does not explicitly capture the context and assumptions associated to risk analysis.

Disconnection or loose connection between pre-market and post-market risk management

Different groups (different activities, methods) making product safety (risk) determinations, but not necessarily leveraging or sharing and continuously building the body of knowledge on device safety

- Pre-production: Product Development – Hazard Analysis, Fault Tree Analysis, design FMEAs, Risk Analysis Document for Regulatory Submissions
- Production: Manufacturing/Operations – Process FMEAs, risk assessment for NCMRs
- Post-production
  - Complaints handling - risk assessment for MDR (Medical Device Reporting) reportability determination
  - Correction & Removals (recalls) – risk assessment for recall notifications to FDA
  - CAPA – risk assessment of product or process issues to determine proper actions and timeline

Potential Issues

- Conflicting information, wrong or inconsistent safety determinations
- Delay in detecting risks and taking proper actions timely
- Extremely valuable design input information lost in the silos

Why ?

- People don't want to share? probably not
- …
- Lacking of a centralized common information platform that is comprehensive to risk management participants/stakeholders even with different background

Summary of Limitations with Current State Risk Management Practices

Ref. #	Commonly used risk management methods and practices	Limitations
I	Bottom Up Analysis Methods (e.g. FMEAs)	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 non-failing 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.
II	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 an undesirable event could be caused by a component failure or component interaction.
III	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 where risk controls can be applied.
IV	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.
V	Risk Traceability Matrix (i.e. traceability between hazardous situations, causes, risk controls, requirements, and testing etc.) used as assurance that risk controls are established	Difficult to assure 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.
VI	Methods that do not explicitly document context and assumptions	Difficult to identify the environmental and use conditions and assumptions that can have a significant safety impact.

What can we do about it?

- To assure medical device safety in today's environment, we should challenge the status quo of existing methods and identify new or improved methods
- Safety assurance cases offer a means to address this.

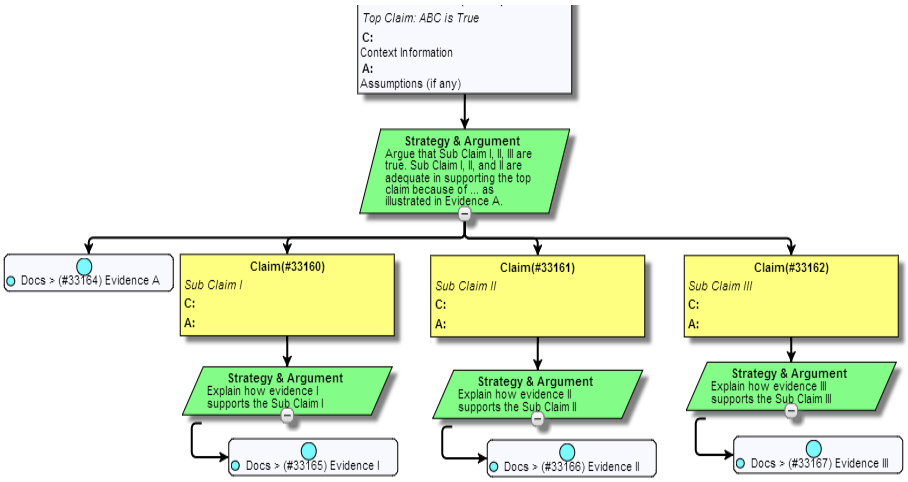
Introduction of (Safety) Assurance Case

A (safety) assurance case is a method for demonstrating the validity of a (safety) claim by providing a convincing argument together with supporting evidence

Elements	**Claim** Statement (assertion) about property of system; need include Context and Assumptions as applicable	**Strategy/Argument** Explanation to connect a claim to evidence or sub-claims in demonstrating validity	**Evidence** Objective evidence to support the claim, strategy/argument …
Rules	• Must have at least 1 child argument • Can have zero or more subsidiary child claims • Must have no child evidence	• Must have a parent claim • Must have one or more child evidence • Can have zero or more child claims	• Must have one or more parent arguments • Must have no child evidence, child claims or child arguments

"Safety Assurance Case" is also called "Safety Case"

Graphical Format Assurance Case



"Assurance Case" way of thinking is already rooted in our education system

- *"The Common Core emphasizes using **evidence** from texts to present careful analyses, well-defended **claims**, and clear information..."*
- *"The reading standards focus on students' ability to read carefully and grasp information, **arguments**, ideas, and details based on **evidence** in the text..."*
- *"Though the standards still expect narrative writing throughout the grades, they also expect a command of sequence and detail that are essential for effective **argumentative** and informative writing."*
- *"The standards' focus on **evidence-based writing** along with the ability to inform and persuade is a significant shift from current practice."*

Safety Assurance Cases - History of Use

- Regulations for safety have generally followed accidents that cause loss of life
- Even after prescriptive safety requirements were put in place, serious accidents continued
- Beginning with the nuclear industry, a new approach began to be used, requiring that the safety of critical systems be justified
- This goal-based regulatory model requires the creation of a safety assurance case
- This approach spread to other types of safety critical systems such as:
  - Defense
  - Civil aeronautics
  - Chemical processing plants
  - Rail transport
- A safety assurance case is now required for these in Europe

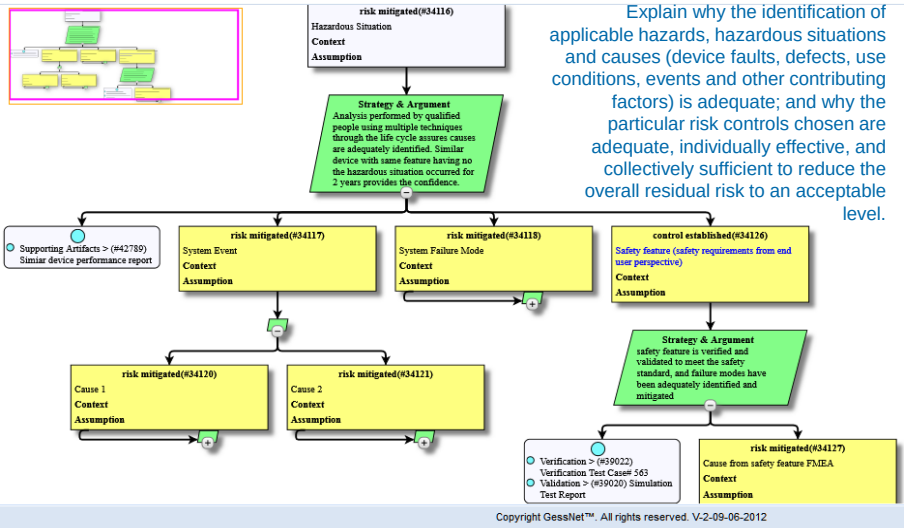
History - Application of Safety Assurance Cases for Medical Devices

- In October 2009, CME Software Engineering Institute TECHNICAL NOTE CMU/SEI-2009-TN-018 "**Towards an Assurance Case Practice for Medical Devices**"
- In April of 2010, FDA issued **"Draft Guidance for industry and FDA staff – Total product life cycle: infusion pump – premarket Notification [510(k)] Submissions"**
- In the IOM report on the 510(k) process, released in July of 2011, **the IOM recommended that a safety assurance case be used for all software in medical devices.**
- After gathering comments on their 510(k) proposals, **the FDA stated that they would use the infusion pump safety assurance case as a pilot study and assess its results before expanding the safety assurance case requirements.**
- **The pilot has been a success**
  - "Safety assurance cases document safety critical information in organized and logical fashion that makes a large amount of information more understandable"
  - "Safety assurance reports have been beneficial in communicating with the FDA. It helps as a communication tool internally as well"
  - "Safety assurance cases intuitively ask critical questions to stimulate critical thinking and drive for evidence based decisions and rationale"
  - "It makes sense once you understand it …"
  - "I can see this is becoming the industry standard …"
- AAMI BI&T Journal Article (Jan/Feb 2014) **"Reducing Risks and Recalls: Safety Assurance Cases for Medical Devices"**

Medical Device Safety Assurance Cases

- The manufacturers make a **Claim** the device is reasonably safe for its intended use
- They argue that the device is acceptably safe from different hazards. The **Argument** provides a rationale that
  - Why that hazardous situations (including causes) are adequately identified, and
  - What was done makes the device acceptably safe with regard to each hazardous situation (including causes)
    - Risk control measures (mitigations) are chosen, and
    - The rationale (reasoning) for why the risk control measures are adequate to make the hazardous situation acceptably safe
    - The rationale (reasoning) for why the each risk control measure is effective
- **Evidence** is provided to support the argument that the risks are identified adequately, risk control measure is implemented correctly and mitigates the hazardous situation

Medical Device Safety Assurance Case – a body of argument



Explain 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.

Safety Assurance Case Structure for Medical Devices

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

Safety Assurance Case Tabular Format Template

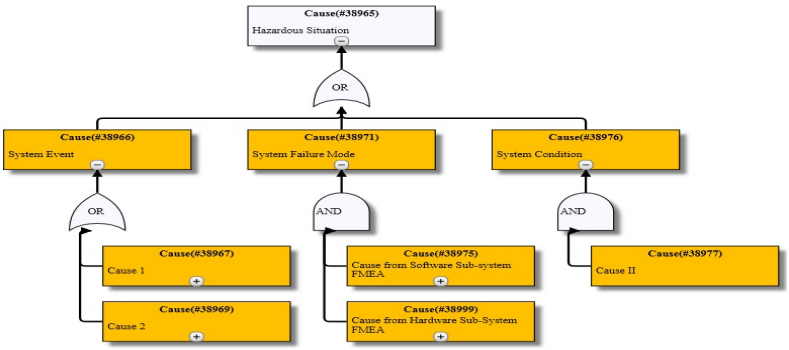
Claims		Context & Assumption	Strategy & Argument	Evidence & Reference
Top Claim	ABC Medical Device is safe for its intended use	Refer to intended use. "Safe" and "Mitigated" means residual risk is acceptable per 21 CFR 860.7(d)(1)	Argue that all applicable hazards are identified and mitigated. Confidence argument on why hazards are identified completely	Intended use, safety policy Evidence to support strategy or argument as applicable
Top Sub-Claims	Sources of **Harm** (Top Hazards) are Mitigated	Explain the potential harm and its severity. Describe context and assumption as applicable	Argue that hazardous situations are identified and mitigated. Confidence argument on why hazardous situations are identified completely	Evidence to support strategy or argument as applicable
Sub-Claims	Risk of **Hazardous Situations** is Mitigated	Explain the hazardous situations. Describe context and assumption as applicable	Argue that causes are identified and mitigated. Confidence argument on why causes are identified completely	Evidence to support strategy or argument as applicable
Sub-Claims	Risks of **Causes** are Mitigated	Causes include faults, conditions, interactions and contributing factors. Describe context and assumption if any	Argue that sub-causes are identified and mitigated. Confidence argument on why sub-causes are identified completely	Evidence to support strategy or argument as applicable
Sub-Claims	Risks of **Sub-Causes** are Mitigated	Describe context and assumption information as applicable	Argue that controls are established. Confidence argument on why control (s) are collectively sufficient to reduce the risk to be at acceptable level	Evidence to support strategy or argument as applicable
Sub-Claims	**Risk Control** is established	Describe context and assumption as applicable	Argument on why control implementation is correct, complete and appropriate	Requirements, Design, V&V, Labeling, SOPs etc.

The architecture of a safety assurance case exercises a top down analysis to support the top claim

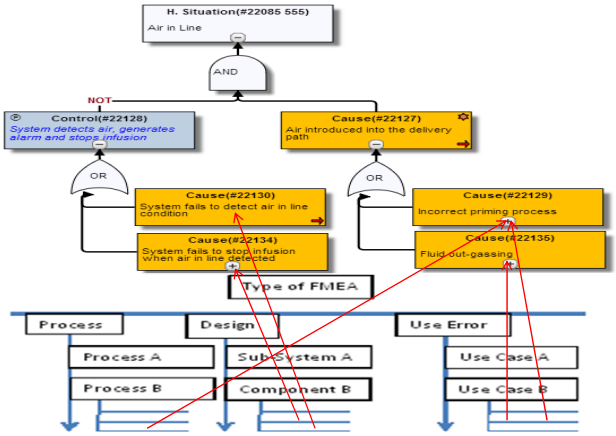
- A safety assurance case for a medical device is argued in a hierarchical fashion with a top level claim (e.g., “this infusion pump is reasonably safe”) and multiple layers of sub-claims (e.g. “risk of over dose hazard is mitigated to be acceptable”)
- The architecture of the safety assurance case is to lay out a logical structure of sub-claims that support the top claim that the device is safe for its intended use
- Without systematically understanding what the top level hazardous situations and associated causal chains are, it will be impossible to identify the sub-claims that are cohesive to formalize a convincing safety assurance case architecture.
- This ensures the limitations of the bottom up analysis methods are addressed.

Developing Assurance Case Confidence Argument requires critical thinking

- Developing an argument for the parent claim requires critical thinking of why its decomposition into sub-claims is complete and correct
- This critical thinking stimulates the identification of hazardous situations, causes, or sub-causes including low level causes that can be more efficiently identified using a bottom up analysis



Developing Assurance Case Confidence Argument requires end to end system thinking



- This assures not only that bottom up analysis needs to be adequately performed, but also the bottom up analysis needs to be connected logically to the top down analysis.
- As such, the limitations with top down analysis methods and the limitations with independent top down analysis and bottom up analysis are both addressed.

Assurance Case Argument requires objective evidence for risk acceptability

- Each claim of “risk is mitigated” that has “risk control is established” as sub-claims should have argument to explain why the risk controls collectively reduce the risk to be acceptable.
- 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 (e.g. RPN) that the objective evidence is not always documented

Assurance Case Argument connects the quality evidence and safety claims

- Each claim of “risk control is established” is not only supported by implementation evidence, such as requirements, procedures, and verification, but also has an argument on 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

Assurance Cases Explicitly Requires Context & Assumption Information Documented & Communicated

- 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

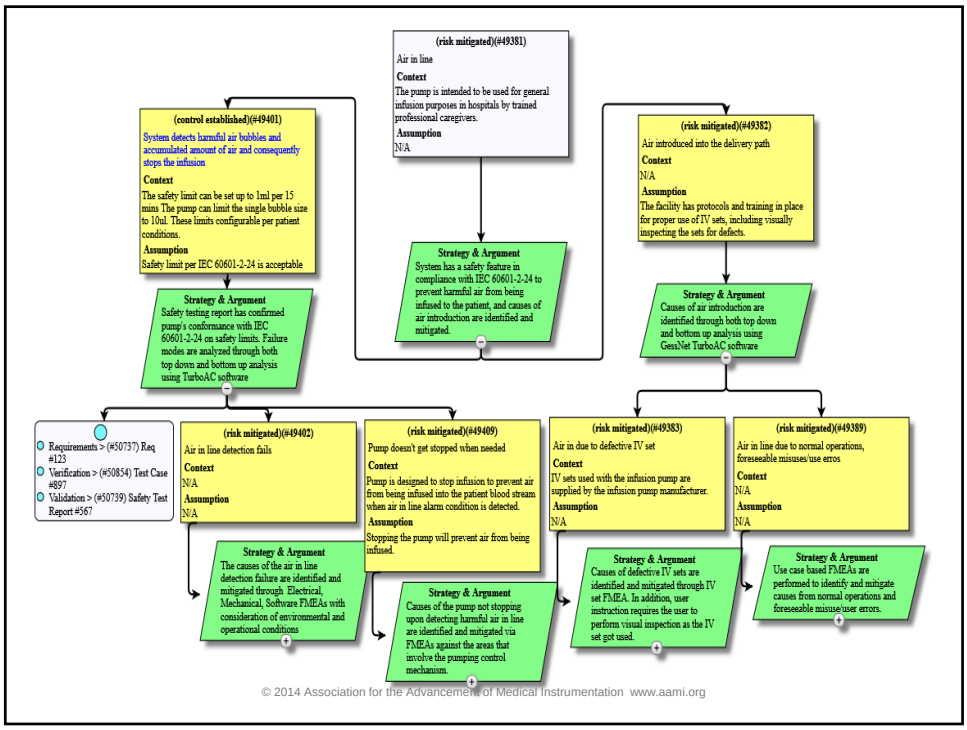
Safety Assurance Cases - Summary

1. Provide a framework and a vehicle to stimulate critical thinking,
2. Assure the completeness of risk identification and risk controls,
3. Provide rationale for the validity of risk acceptance,
4. Logically document and connect safety critical information in an easily understandable manner, and
5. Communicate safety critical information effectively to internal and external stakeholders
6. Offer a comprehensive information format to continuously build the body of knowledge on product safety

Final Thoughts

- More safety recalls are occurring in increasingly complex devices and environments
- There are limitations with existing risk management methods and practices in today's complex medical technology and environment
- By requiring a holistic body of argument that is logically structured with supporting objective evidence, safety assurance cases "connect" the dots and "ask" the right questions to assure safety in these complex situations.
- They intuitively guide critical thinking on product safety and drive risk management's completeness and effectiveness.
- Exercising this critical thinking will result in more complete identification of scenarios leading to hazardous situations and more adequate and effective risk controls, and ultimately reduce product recalls by addressing the common causes of the recalls.


AAMI
Advancing Safety in Medical Technology
Questions?
Type your question in the Q&A box on the left side of your screen and press Enter
© 2014 Association for the Advancement of Medical Instrumentation www.aami.org
47


(risk mitigated)(#49381)
Air in line
Context
The pump is intended to be used for general infusion purposes in hospitals by trained professional caregivers.
Assumption
N/A
(control established)(#49401)
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 configurable per patient conditions.
Assumption
Safety limit per IEC 60601-2-24 is acceptable
Strategy & Argument
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.
(risk mitigated)(#49382)
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.
Strategy & Argument
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
Strategy & Argument
Causes of air introduction are identified through both top down and bottom up analysis using GessNet TurboAC software
Requirements > (#50737) Req #123
Verification > (#50854) Test Case #897
Validation > (#50739) Safety Test Report #567
(risk mitigated)(#49402)
Air in line detection fails
Context
N/A
Assumption
N/A
(risk mitigated)(#49409)
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.
(risk mitigated)(#49383)
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
(risk mitigated)(#49389)
Air in line due to normal operations, foreseeable misuses/use erros
Context
N/A
Assumption
N/A
Strategy & Argument
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
Strategy & Argument
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.
Strategy & Argument
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.
Strategy & Argument
Use case based FMEAs are performed to identify and mitigate causes from normal operations and foreseeable misuse/user errors.
© 2014 Association for the Advancement of Medical Instrumentation www.aami.org

Closing Reminders

- Be sure to fill out the evaluation form at: http://aami.confedge.com/ap/survey/s.cfm?s=GoodDesign
- AAMI is planning the following webinars that may be of interest to you:
  - November 20 – Beyond Printed Instructions

Closing Reminders

- Be sure to fill out the evaluation form at: http://aami.confedge.com/ap/survey/s.cfm?s=SafeAssur
- AAMI is planning the following webinars that may be of interest to you:
  - Sept. 30 – Reliability Practices in Implantable Devices
  - Oct. 21 – Optimization of Validation Activities

Closing Reminders

- Announcing AAMI University - a better way to manage your professional development
  - Online and live comprehensive education resources for medical technology professionals
  - Access to AAMI's industry-leading curriculum and instructors
  - Please visit AAMI U at http://university.aami.org/

Learn. Think. Implement.