Risk Management Policy


Life Cycle Activities


Top Down Analysis


Bottom Up Analysis

Top Down & Bottom UP

Trace to Requirements/V&V

Assurance Case Integration

Reports for Submission

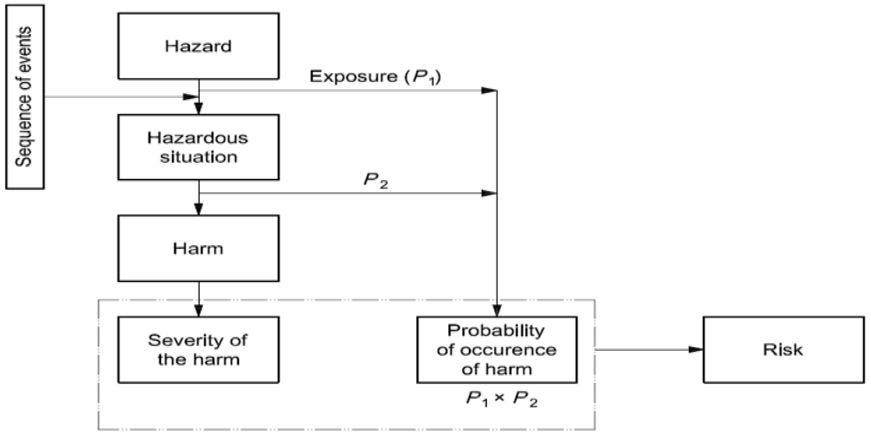

Regulatory Review

Risk management is a systematic life cycle process to identify, control and evaluate risks. Safety assurance case is a methodology that has a set of disciplines to structurally demonstrate that a safety goal/claim is achieved or fulfilled. If applied properly, safety assurance case can become an effective method to proactively challenge the logic, results and process of the risk management and yield more streamlined, thorough, data & facts based risk management practices, and then ultimately help to assure and demonstrate the safety of the medical devices. GessNet TurboAC™ software provides a powerful all-in-one environment to develop and maintain risk management files through the product life cycle, and integrate safety assurance case into the risk management process as needed.

Define and Manage Risk Management Policy

Per ISO 14971, risk is defined as the combination of the severity of the potential harm and probability of the potential harm occurrence, and safety is freedom from unacceptable risk. Individual company or organization typically has its own policy in terms of how to measure (i.e. scales) severity and probability, as well as how to evaluate whether the risk is acceptable or not (i.e. acceptability matrix).

GessNet TurboAC™ software provides the capability for users to define and manage their risk management policy, i.e. risk severity and probability scales, and risk acceptability matrix. GessNet TurboAC™ software provides the functionality to automatically apply the risk management policy to the company-wide products



NOTE P_1 is the probability of a hazardous situation occurring.
P_2 is the probability of a hazardous situation leading to harm.

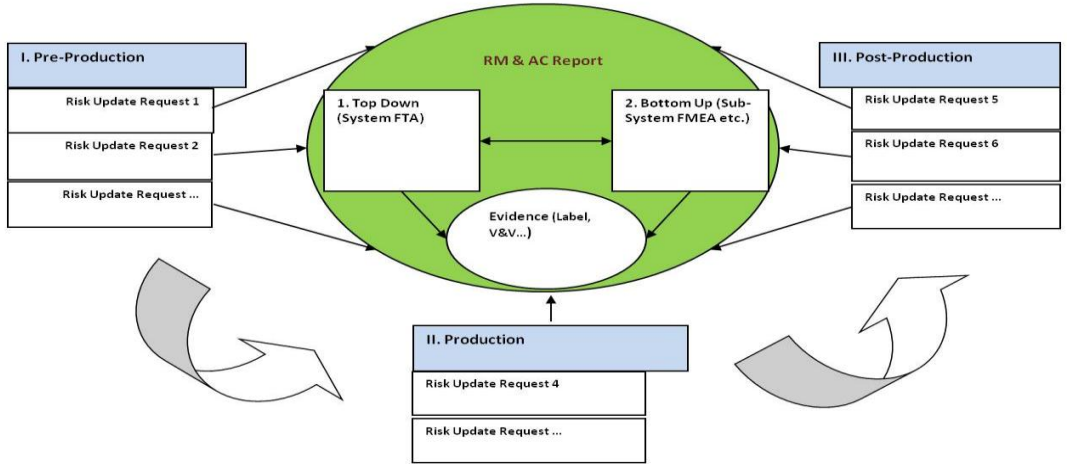
Figure E.1 — Pictorial representation of the relationship of hazard, sequence of events, hazardous situation and harm

Define and Manage Life Cycle Risk Management Process

The best practices of risk management typically start from top down system analysis (e.g. hazard analysis and fault tree analysis), followed by bottom up (e.g. FMEA), as illustrated in the following table:

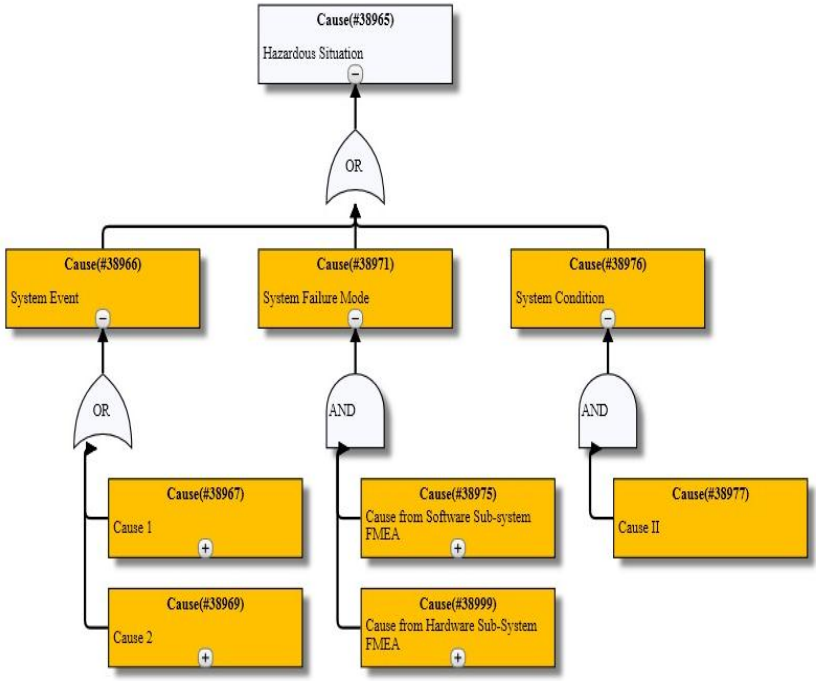
Life Cycle Process	Input	Output				
		Hazards	Hazardous Situations	Failure Modes	Causes	Risk Controls
System Hazard Analysis	Intended use, use conditions, historical data, guidance, standards	<=======Focus=========>				Safety Feature Identification
System Fault Tree Analysis	Safety Features, System Requirements and Design, Safety Features		<============Focus===========>			System Safety Requirements
Sub-System FMEAs	Sub-system Requirements & Design			<=======Focus==========>		Sub-system safety requirements
Component/Unit/Process FMEA				<=======Focus==========>		Component/Unit/Process safety requirements
Production	Production information, design/process change			<=======Focus==========>		Production safety requirements
Post Production	Field Performance/Industry Information	<=====================Focus=====================>				New/additional safety requirements

GessNet TurboAC™ software provides the capability for users to perform risk management activities in following the best industry practices. With TurboAC™ software, users are able to perform both top down and bottom up analysis at appropriate stages of the product life cycle. Users can define and configure the product life cycle risk management process, assign owners, track progress, capture results and manage reviews and approvals for each of the life cycle activities.



Conduct Top down Analysis e.g. System Hazard Analysis and System Fault Tree Analysis

The Top Down Analysis starts with the top system hazards that are applicable to the product, and then deductively breaks down into system hazardous situations, system faults /failure modes or contributing factors, and risk controls corresponding to each level if applicable.



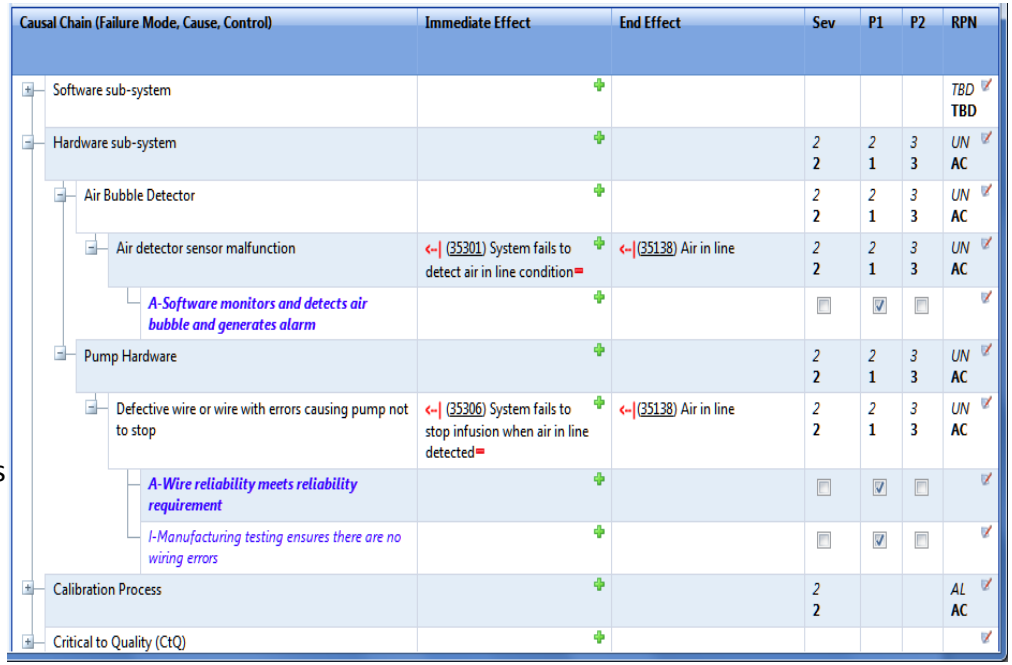
With GessNet TurboAC™ software, users can facilitate the group brainstorming, document and present the results in either graphic format or tabular format. This will include

- Identify potential harms/risks
- Identify applicable top hazards
- Identify applicable hazardous situations
- Identify system failure modes and causes
- Identify system level risk controls (safety requirements)
- Identify and track the essential requirements

Conduct Bottom up Analysis e.g. Sub-System/Component/Process FMEA

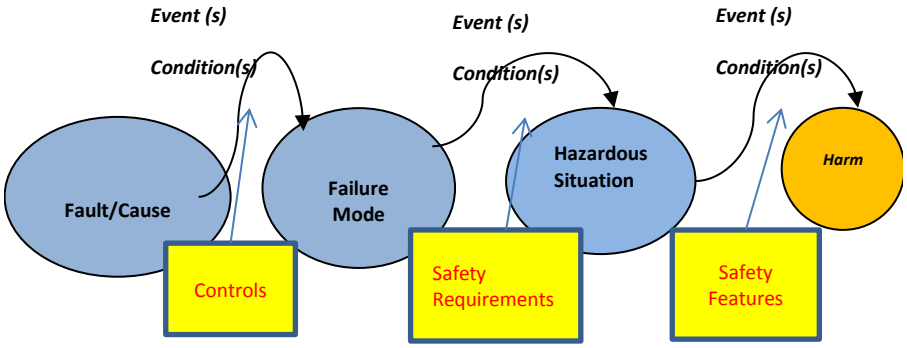
The Bottom Up Subsystem FMEA Tree (e.g. Design FMEAs, Process FMEAs, User Error Risk Analysis etc.) is to analyze and capture the design/user errors/process Failure Modes, Effects, Causes, Priority Assessment, and Mitigation Identification. With GessNet TurboAC™ software, users can go as deep as needed to decompose the system and drive the root cause analysis. Specifically, users can perform, document and present the results of following activities:

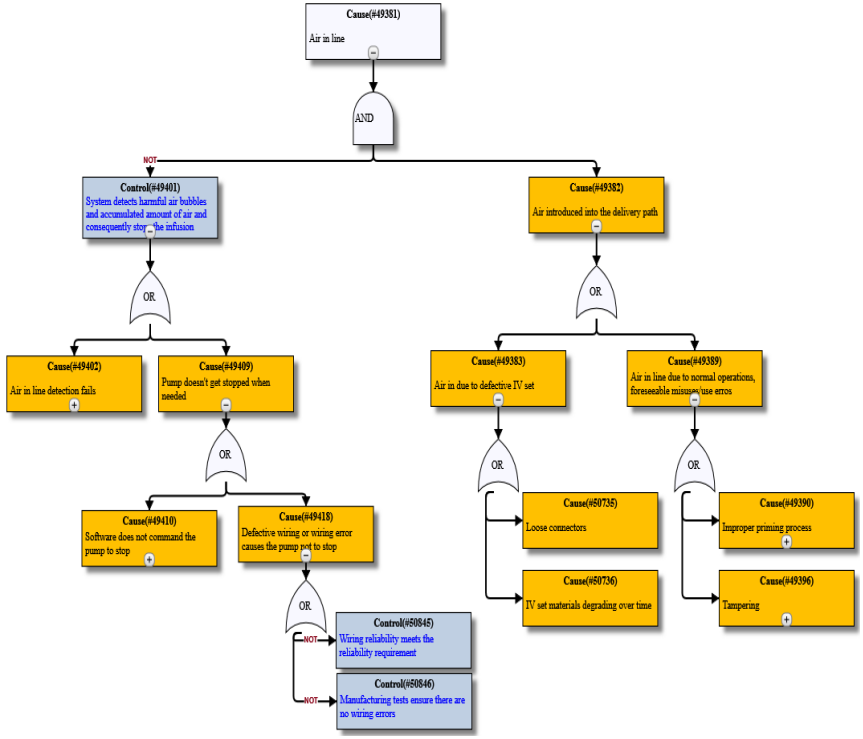
- Identify components/functions/areas in need of FMEA
- Identify potential failure modes and their causes
- Identify local and system effects for each failure mode
- Conduct risk assessment for each failure mode
- Identify risk mitigation as applicable



Connect Top down and Bottom up --- Linking

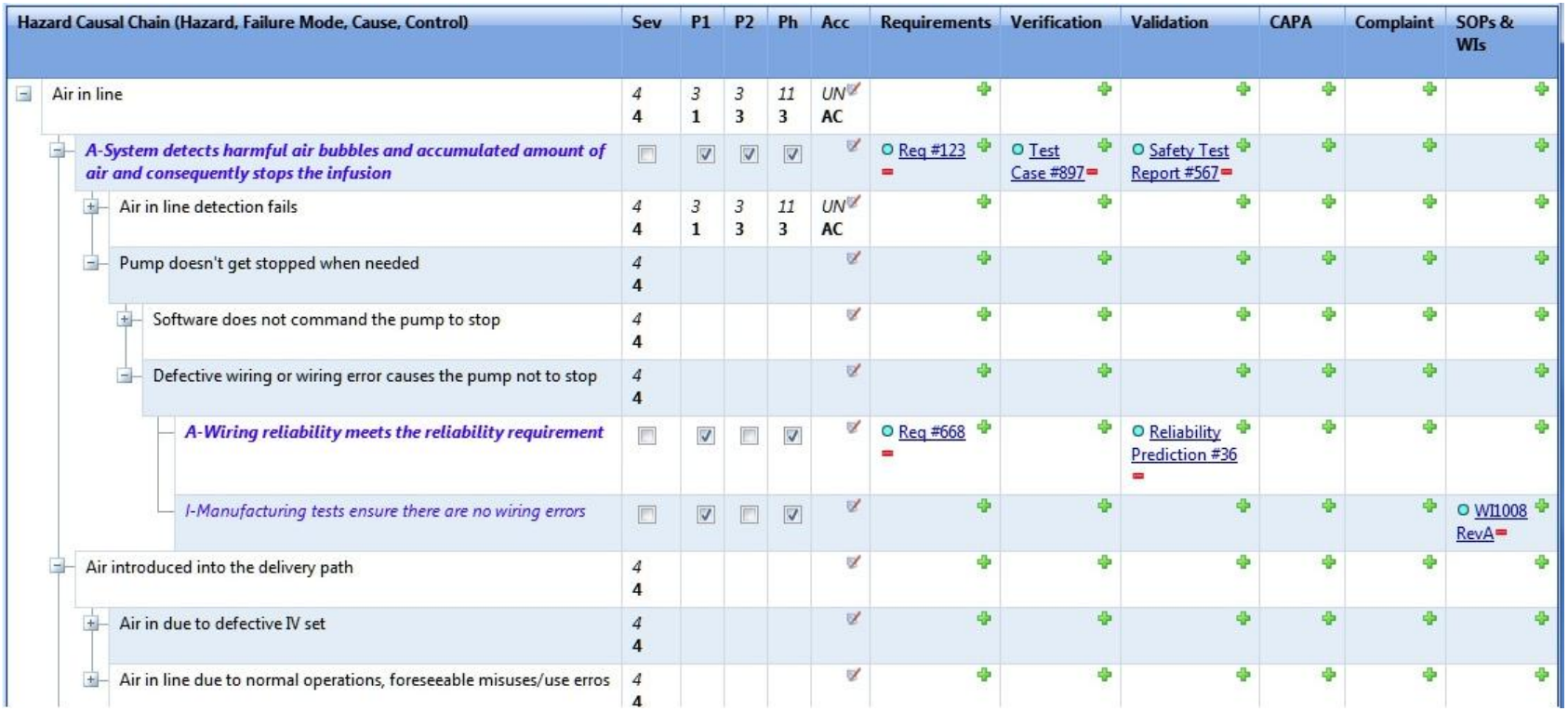
Being able to connect Top Down and Bottom Up analysis provides great benefits in identifying system level failure modes, sub-system/component level causes, as well as understanding the end to end cause effect big picture.
With GessNet TurboAC™ software, connectivity between the Top Down and Bottom Up analysis becomes one click away. Additionally GessNet software provides the capability to automatically passing down/up the severity and probability effect between Top Down and Bottom Up analysis results.





Establish Traceability to Requirements and/or V & V tests

It is commonly expected by regulators that the risk analysis report includes the traceability from the risk controls to artifacts such as requirements and/or V&V tests. Establishing and maintaining this traceability can be tedious. With GessNet TurboAC™ software, users can electronically organize and centralize the artifacts and maintain it through the product life cycle easily.



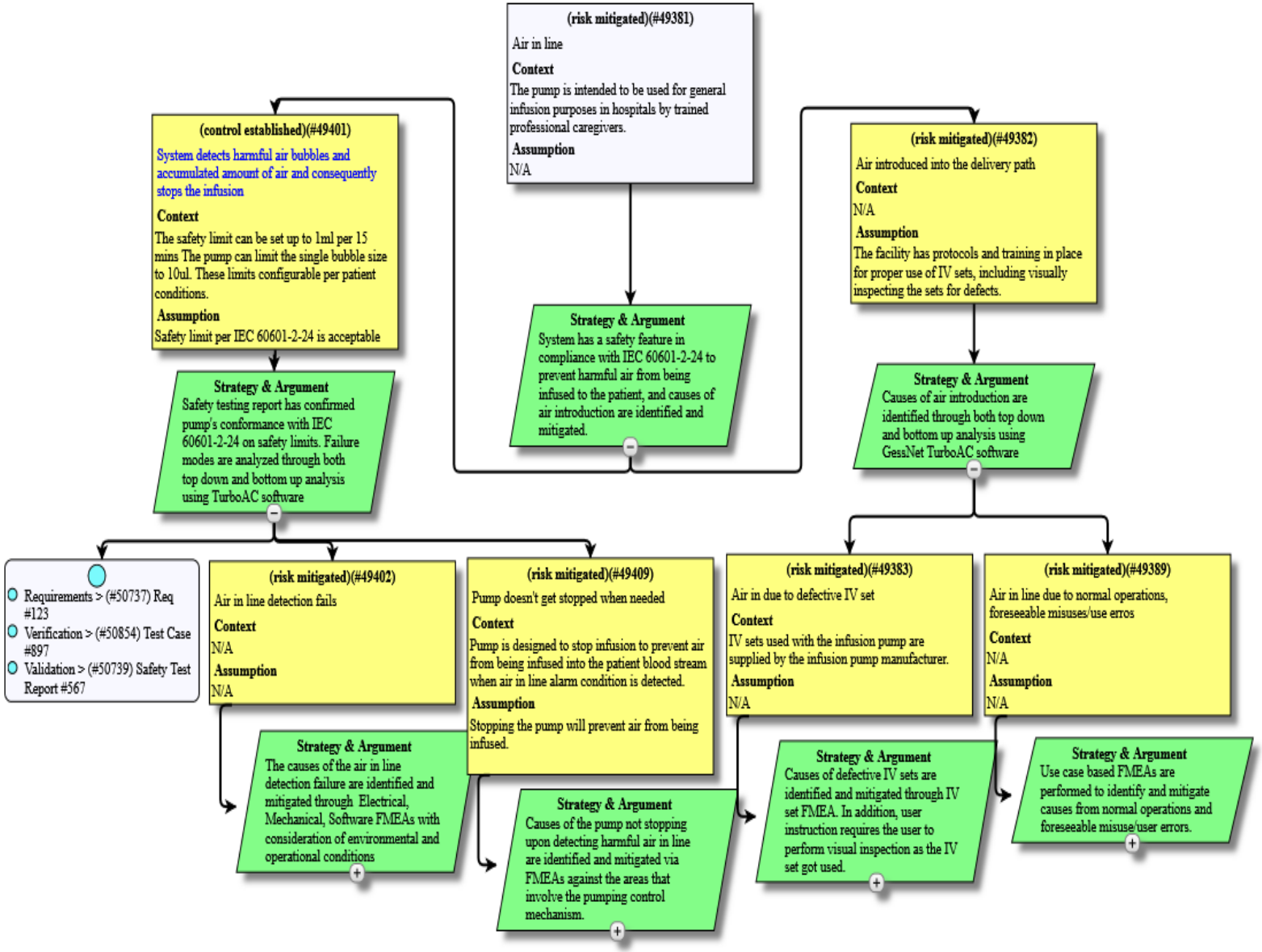
Hazard Causal Chain (Hazard, Failure Mode, Cause, Control)	Sev	P1	P2	Ph	Acc	Requirements	Verification	Validation	CAPA	Complaint	SOPs & WIs
Air in line	4 **4**	3 **1**	3 **3**	11 **3**	UN **AC**						
A-System detects harmful air bubbles and accumulated amount of air and consequently stops the infusion						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**										

Assurance Case Integration

Assurance Case is a structured method to demonstrate how a claim (goal) is fulfilled (achieved). It includes three fundamental elements: Claim (Goal), Argument (Strategy) and Evidence. In addition, as needed, the Context and Assumption information should also be included as applicable. A Safety Assurance Case is to demonstrate a safety claim is fulfilled. GessNet TurboAC™ software provides an integrated environment to generate assurance case in leveraging the risk management information. With GessNet TurboAC™, users could easily build safety assurance case, including:

- Define top claim and sub-claims;
- Describe arguments & strategy
- Centralize supporting evidence
- Link to evidence fully leveraging risk analysis traceability information

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



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.	

Reports for Regulatory Submission

1). User can save the reports into PDF files that can be printed onto regular paper.
2). User can export the graphic into a HTML file that is viewable through a web browser. The HTML file comes with the capability for the reviewer to navigate through the graphic conveniently (i.e. expand and collapse).
3). User can export the reports into an encrypted electronic file and submit it to FDA with read-only permission. Customers can export the reports in modes:

a. Export the data for review purpose such as FDA reviewers (when reviewer imported into their database, no editing allowed, but reviewer can add comments)
b. Export as a template for another similar product RMF (for further editing)

Regulatory review

FDA has the GessNet TurboAC™ application installed on its own IT environment, and has the capability to import and review the electronic file. The electronic copy of the assurance case report includes the information as illustrated in the AC Table. The AC report is readable only to FDA. FDA does have the permission to add/manage review comments within the agency. The electronic submission helps to expedite FDA's review and approval.