Adapting Classic Assurance Case Theory to Medical Device Development: A Manufacturer's Perspective

62nd Meeting of IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance

Rockport, MA

Baxter Healthcare Corporation
pat_baird@baxter.com

June 30, 2012

Problem Statement

- Risk Management processes and submissions to regulatory authorities are like puzzles that the reviewer must be put together to be understood.

- Medical Device designs are getting sufficiently complex that the designers and regulators have challenges seeing potential defects. We cannot spot if there are missing pieces

Agenda

- **Background**
- Creating a Medical Device Assurance Case
- Reviewing a Medical Device Assurance Case
- “Challenge Cases”
- Wrap-up
- Open Discussion

We could keep the tools and techniques we currently have

Or we could look to see what others are doing and how that might be adapted to our problem

Assurance Cases in Other Industries

Banks have used “Security Cases” to uncover potential cyber-security issues.

DoD used “Supply Chain Assurance Cases” to ensure repair parts are available for UAVs – lack of parts availability was seen as a risk to soldiers on the ground.

A Safety Case was developed for a dry-dock crane that lifts nuclear submarines out of the water for repairs.

FDA's Interest…

Medical Device Pre-Market Programs: An Overview of FDA Actions

Executive Summary {emphasis added}

- **Implement an Assurance Case Pilot Program** - Assurance cases have been used successfully by other industries, such as avionics, to efficiently minimize product risks and expedite government reviews. … The assurance case gives the reviewer a roadmap through the 510(k) submission and allows the reviewer to see the big picture of how the sponsor has mitigated risks and reduced the likelihood of device error. On March 31, 2011, we started a pilot on the use of assurance cases for infusion pumps… Preliminary results suggest the use of an assurance case can reduce review times, at least for some infusion pump submissions…. We intend to make the results of the pilot available to the public and will seek public input first if we think there would be value to expanding the use of assurance cases**.**

Source: http://www.fda.gov/AboutFDA/CentersOffices/CDRH/CDRHReports/ucm276272.htm , Oct 25, 2011

Definitions of a Safety Case

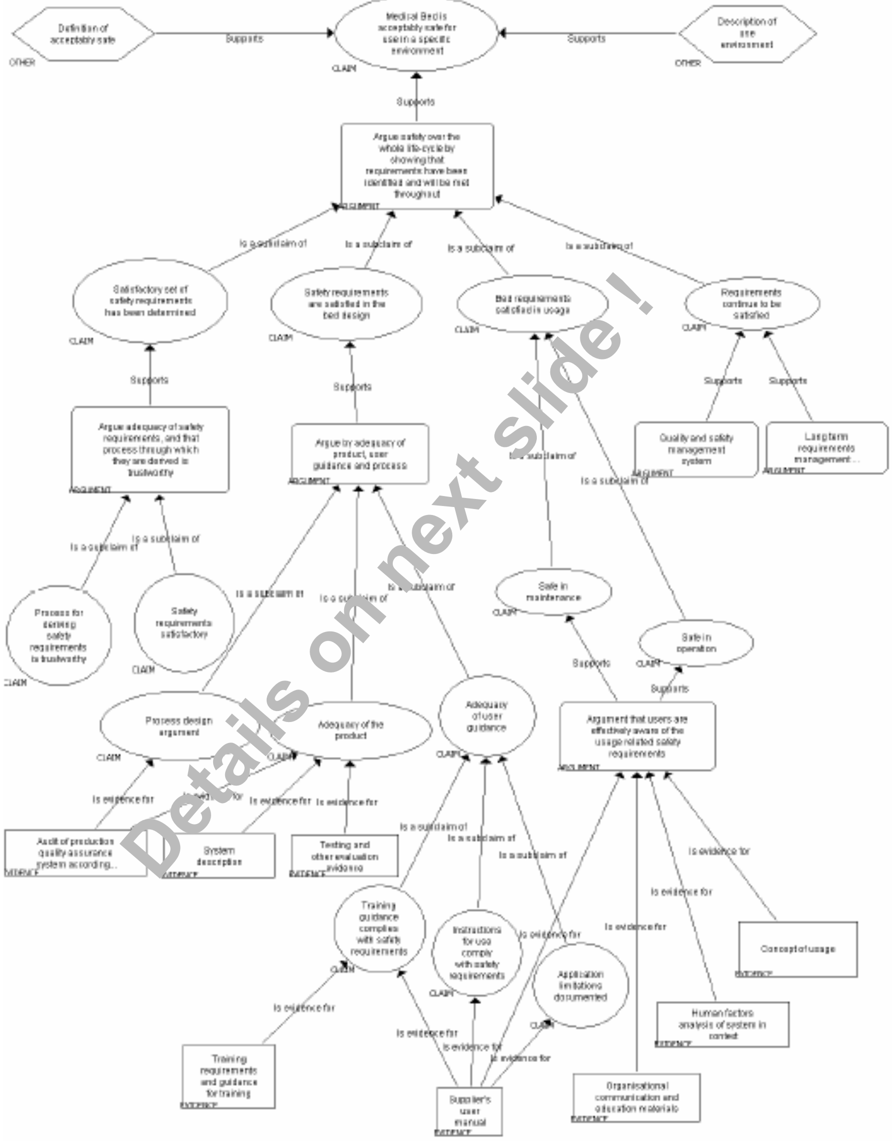
"A formal method for demonstrating the validity of a claim by providing a convincing argument together with supporting evidence" [Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions]

"A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment" [Adelard Safety Case Development Manual]

"A safety case presents the argument that a system will be acceptably safe in a given context" [Kelly]

"A safety case should communicate a clear, comprehensive and defensible argument that the system is acceptably safe to operate in a particular context." [Kelly]

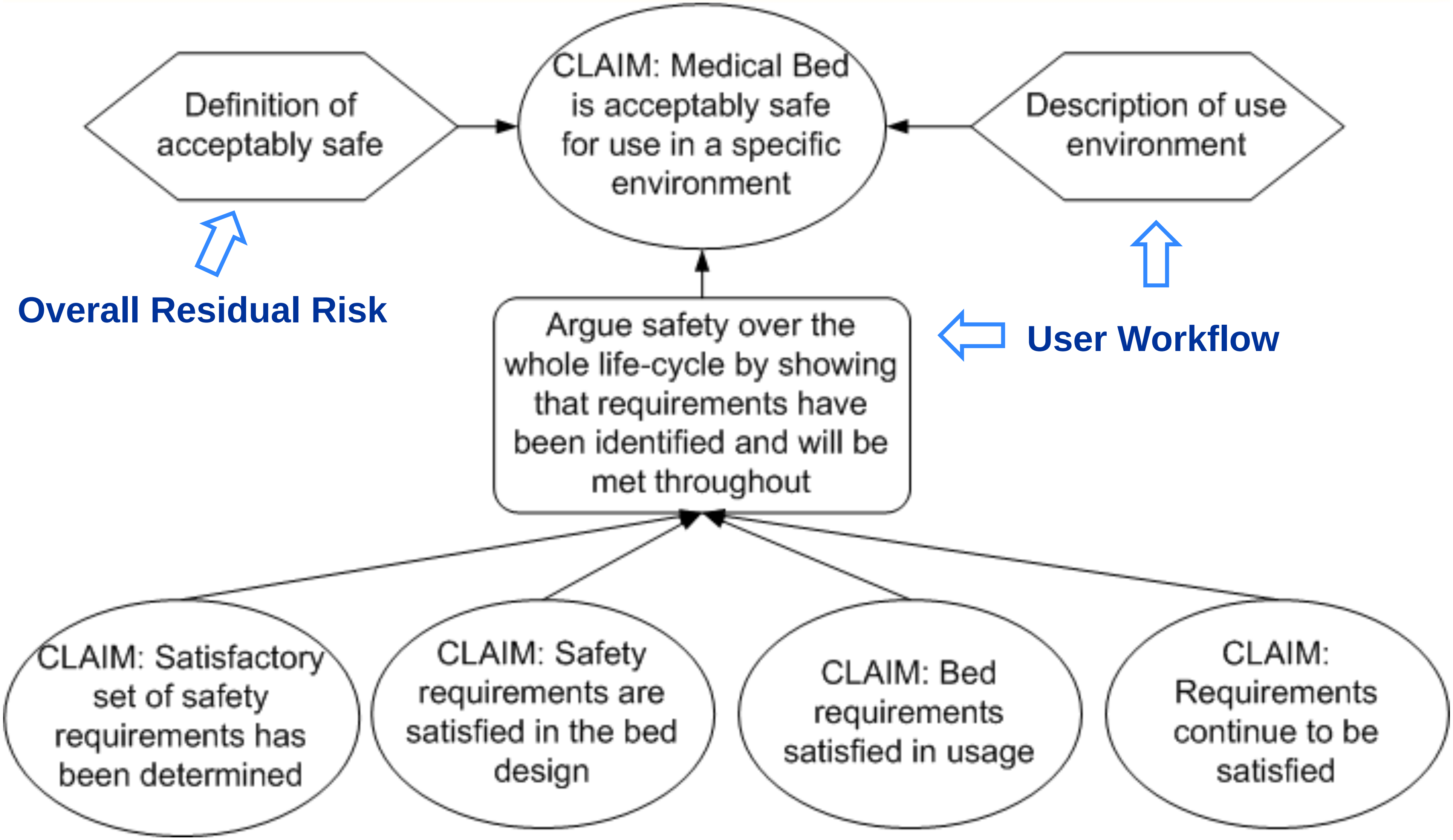
Example Assurance Case / Safety Case


Definition of acceptably safe
OTHER
Supports
Medical Bed is acceptably safe for use in a specific environment
CLAIM
Supports
Description of use environment
OTHER
Supports
Argue safety over the whole life-cycle by showing that requirements have been identified and will be met throughout
ARGUMENT
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is a subclaim of
Satisfactory set of safety requirements has been determined
CLAIM
Safety requirements are satisfied in the bed design
CLAIM
Bed requirements satisfied in usage
CLAIM
Requirements continue to be satisfied
CLAIM
Supports
Supports
Supports
Supports
Argue adequacy of safety requirements, and that process through which they are derived is trustworthy
ARGUMENT
Argue by adequacy of product, user guidance and process
ARGUMENT
Quality and safety management system
ARGUMENT
Long term requirements management...
ARGUMENT
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is a subclaim of
Process for deriving safety requirements is trustworthy
CLAIM
Safety requirements satisfactory
CLAIM
Safe in maintenance
CLAIM
Safe in operation
CLAIM
Supports
Supports
Process design argument
CLAIM
Adequacy of the product
CLAIM
Adequacy of user guidance
CLAIM
Argument that users are effectively aware of the usage related safety requirements
ARGUMENT
Is evidence for
Is evidence for
Is evidence for
Is evidence for
Audit of production quality assurance system according...
EVIDENCE
System description
EVIDENCE
Testing and other evaluation evidence
EVIDENCE
Is a subclaim of
Is a subclaim of
Is a subclaim of
Is evidence for
Is evidence for
Is evidence for
Is evidence for
Training guidance complies with safety requirements
CLAIM
Instructions for use comply with safety requirements
CLAIM
Application limitations documented
CLAIM
Concept of usage
EVIDENCE
Human factors analysis of system in context
EVIDENCE
Is evidence for
Is evidence for
Is evidence for
Is evidence for
Training requirements and guidance for training
EVIDENCE
Supplier's user manual
EVIDENCE
Organisational communication and education materials
EVIDENCE

Details on next slide !

Source: "Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges" Mark-Alexander Sujan, Floor Koornneef, and Udo Voges (2007)

Zoom In to Top Level…



Definition of acceptably safe

CLAIM: Medical Bed is acceptably safe for use in a specific environment

Description of use environment

Overall Residual Risk

Argue safety over the whole life-cycle by showing that requirements have been identified and will be met throughout

User Workflow

CLAIM: Satisfactory set of safety requirements has been determined

CLAIM: Safety requirements are satisfied in the bed design

CLAIM: Bed requirements satisfied in usage

CLAIM: Requirements continue to be satisfied

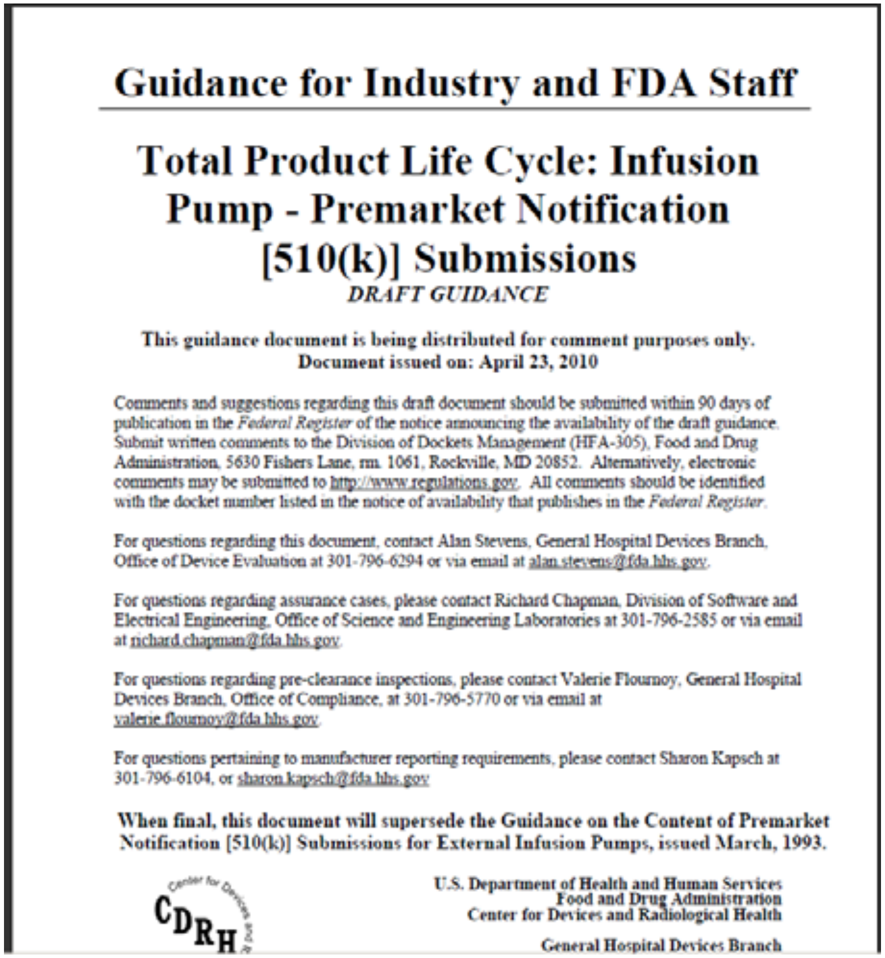
My Background

Systems Engineer at Baxter, one of the companies undergoing the FDA pilot program.

Chair of the AAMI group creating a Safety Assurance Case guidance for medical devices

One of the AAMI trainers for the Safety Assurance Case 3-day course

Active in the AdvaMed Infusion Pump Working Group that has developed an example assurance case for the FDA’s review



Guidance for Industry and FDA Staff

Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.
Document issued on: April 23, 2010

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Alternatively, electronic comments may be submitted to http://www.regulations.gov. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this document, contact Alan Stevens, General Hospital Devices Branch, Office of Device Evaluation at 301-796-6294 or via email at alan.stevens@fda.hhs.gov.

For questions regarding assurance cases, please contact Richard Chapman, Division of Software and Electrical Engineering, Office of Science and Engineering Laboratories at 301-796-2585 or via email at richard.chapman@fda.hhs.gov.

For questions regarding pre-clearance inspections, please contact Valerie Flournoy, General Hospital Devices Branch, Office of Compliance, at 301-796-5770 or via email at valerie.flournoy@fda.hhs.gov.

For questions pertaining to manufacturer reporting requirements, please contact Sharon Kapsch at 301-796-6104, or sharon.kapsch@fda.hhs.gov

When final, this document will supersede the Guidance on the Content of Premarket Notification [510(k)] Submissions for External Infusion Pumps, issued March, 1993.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health

General Hospital Devices Branch

Problem Statement

Medical devices have grown to be so complex that regulators may have a hard time assessing if a device is safe.

Additionally, have you ever faced a situation where:

1. The design team missed a detail ?
2. The design team forgot to write down the rationale for a decision ?
3. You can’t find where something is documented ?

What isn’t working?

The Risk Management process can be like the child’s game of telephone

Intended Use > Hazards

Hazards > Causes

Causes > Risk Controls

Risk Controls > Requirements

Requirements > Verification

With 5 levels of transition, are we really sure that the Verification step is still testing to the Intended Use? Is it a consistent story?

Challenges with the Risk Management Std 14971:2007

Offers results, but now how you got there.

Doesn’t explain the “Why?”

“Lite” version of the Risk Management Report

Game-of-telephone approach

What's Different About Medical Devices

Safety Cases have been used for years in other industries. Why should medical devices have any issues adapting?

- Shorter development cycles
- Diversity of product types
- Less control over users & environments
- Different Regulatory model

Challenges with Direct Adoption of Classic Assurance Case Methods

The FDA's Premarket Notification Requirements (regulatory submission) are at a different level of depth and breadth than other industries

Frustrating terminology – "Claim" has a special meaning

Duplicates effort with existing risk management activities

Classic Assurance Cases don't address all the frustrations with current risk management

Creating a Medical Device Assurance Case

Aha!

Aha Moment! Rather than start with Classic and subtract detail, why not start with 14971 and add? Why don't we adopt Assurance Case Theory and supplement 14971?

"Classic minus Something" vs. "14971 plus Why"

Rather than completely embracing a new methodology, lets use it to improve 14971!

Requirements for Adoption

The Safety Case must be:

- Easy to author
- Easy to maintain
- Easy to review

The final form must work for both the author and the reviewer.

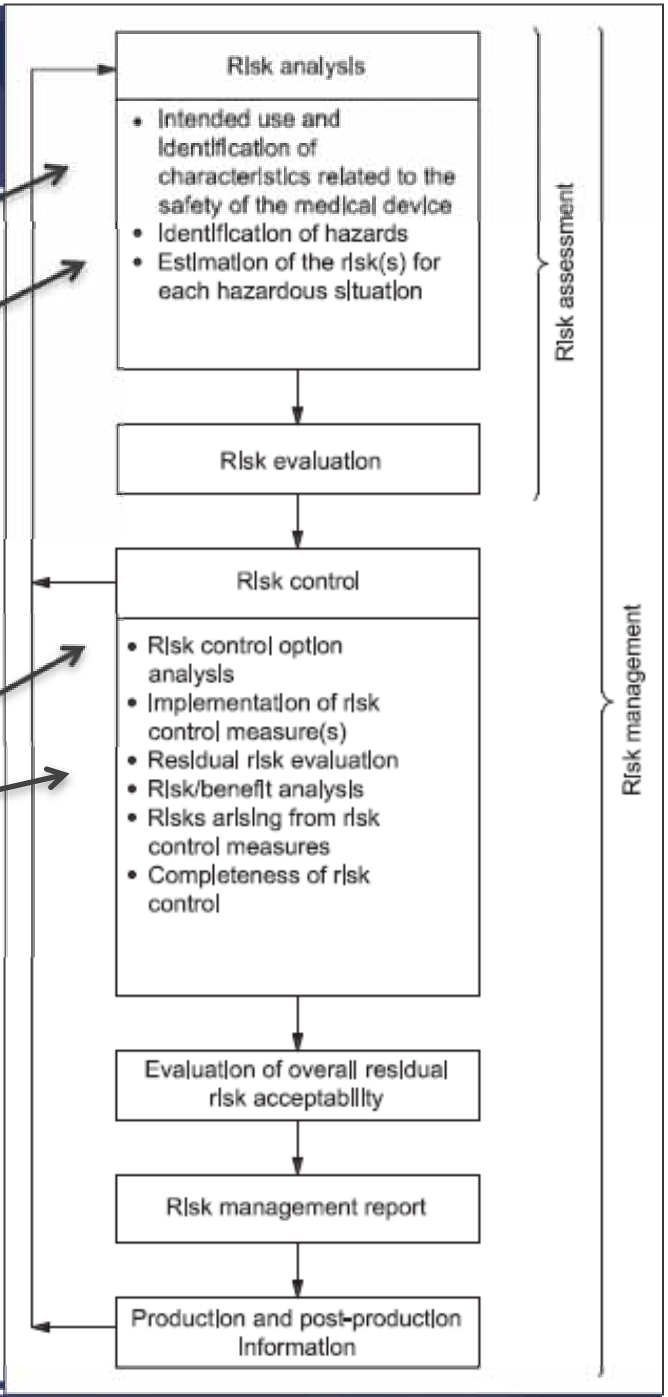
Risk Management, In a Nutshell

1. What are you trying to do?

2. What can go wrong?

3. What are you going to do about it?

4. Did it work?


Risk analysis
• Intended use and identification of characteristics related to the safety of the medical device
• Identification of hazards
• Estimation of the risk(s) for each hazardous situation
Risk evaluation
Risk assessment
Risk control
• Risk control option analysis
• Implementation of risk control measure(s)
• Residual risk evaluation
• Risk/benefit analysis
• Risks arising from risk control measures
• Completeness of risk control
Evaluation of overall residual risk acceptability
Risk management report
Production and post-production information
Risk management

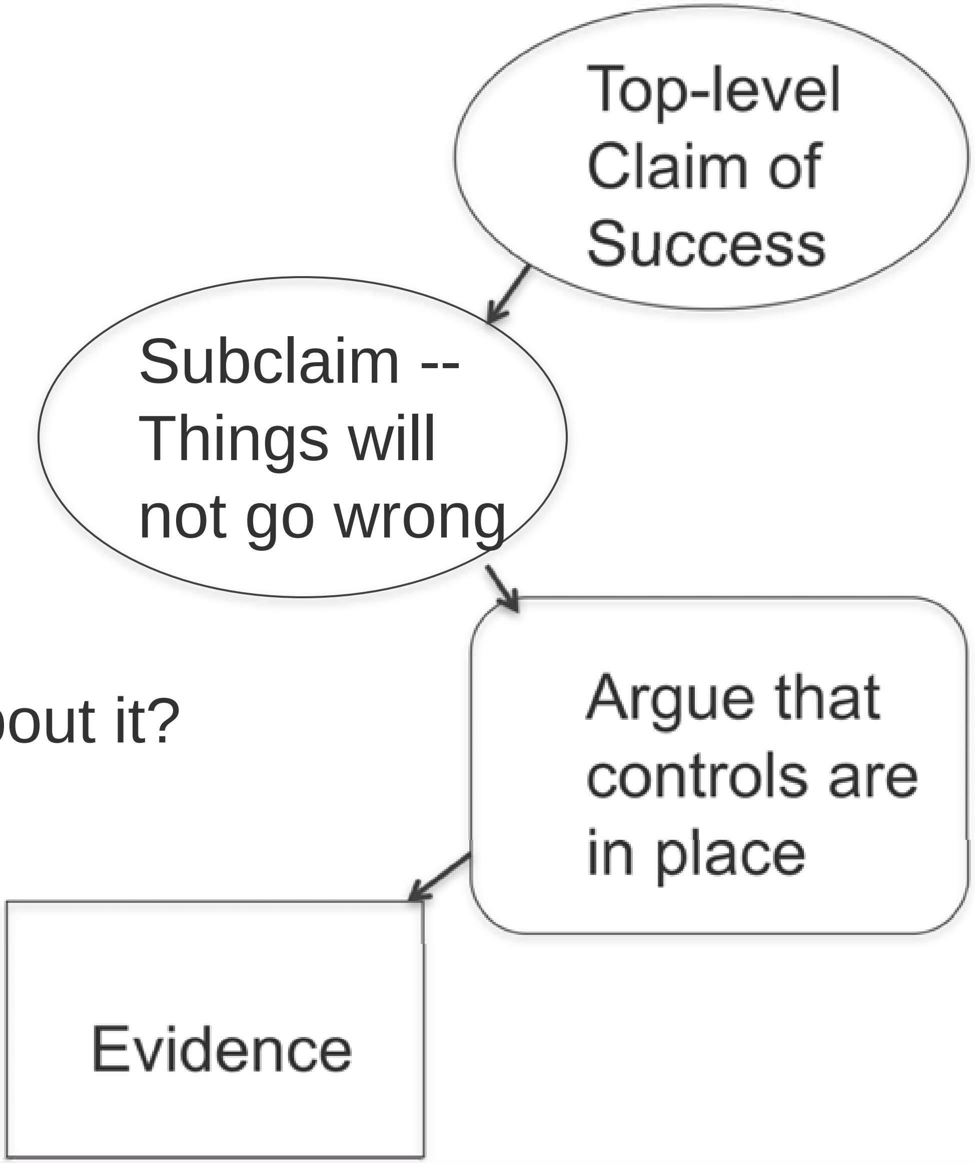
Risk Management & CAE

1. What are you trying to do?

2. What can go wrong?

3. What are you going to do about it?

4. Did it work?



Top-level Claim of Success

Subclaim -- Things will not go wrong

Argue that controls are in place

Evidence

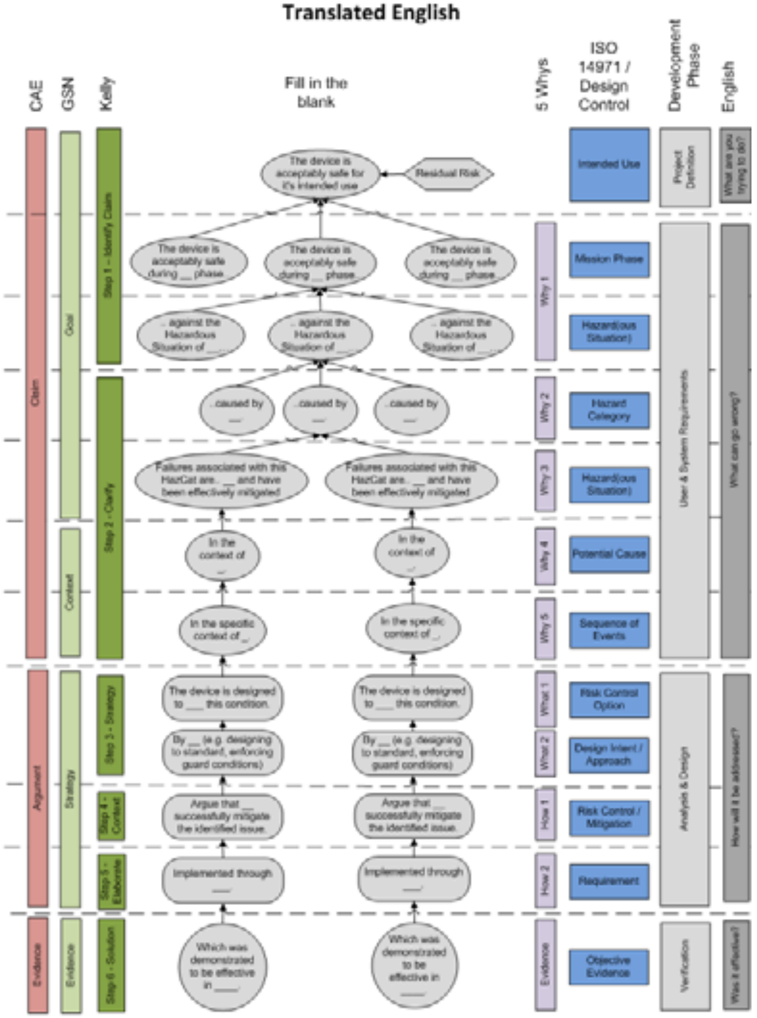
Frame of Reference?

GSN Terms	Goal					Context		Strategy			Evidence
CAE Terms	Top Claim	Sub-Claim						Argument			Evidence
ISO 14971 Terms / Design Control	Intended Use with Residual Risk	Mission Phase	Hazardous Situation	Hazard Category	Hazard	Potential Cause	Sequence of Events	Risk Control Option: Prevent / Detect / Label	Risk Control / Mitigation / Design Intent	Requirement	Objective Evidence
Development Phase	Project Definition	User & System Requirements						Analysis & Design			Testing
5 Whys			Why 1	Why 2	Why 3	Why 4	Why 5	What 1	What 2	How 1	How 2
English	What are you trying to do?	What can go wrong ?						How does the design address the issue?			Did the mitigation work?
Safety Story	"The device is reasonably safe for it's intended use"	"The device is acceptably safe during __ phase.."	".. against the Hazardous Situation of __..."	"caused by __."	"Failures associated with this HazCat are.. __ and have been effectively mitigated"	"In the context of _ [basic cause]."	"in the specific context of __ [root cause]." or "Because ___."	"The device is designed to ___ this condition." (P: "prevent", D: "detect and inform the user", L: "provide instructions regarding..")	"Argue that __ sucessfully mitigate the identified issue."	"Which is met through requirement ___."	"Which was demonstrated to be effective by _____ in ___."

TRANSLATE was born..

TRANSLATE Approach:

- **T**eam
- **R**eadable
- **A**ssurance
- **N**otation,
- **S**tructured
- **L**ogic
- **A**nd
- **T**ranslated
- **E**nglish



TRANSLATE: Team Readable Assurance Notation - Structured Logic And Translated English

Baxter Healthcare, Inc.

It’s a start…

TRANSLATE is a decoder ring to show developers how to supplement their FMEA with additional information – this Risk Based Table (RBT) provides the bulk of the Safety Case argument.

But additional information is needed:

- Intended Use
- Device Description
- High Level Hazards Analysis
- Development Process Summary
- Novel Technology or Post-Market activities

AdvaMed team came up with an example “IPAC”…

Baxter

AdvaMed IPWG Example

REPORT

Captures the argument and "tells the story" of the device. Acts as a pointer.

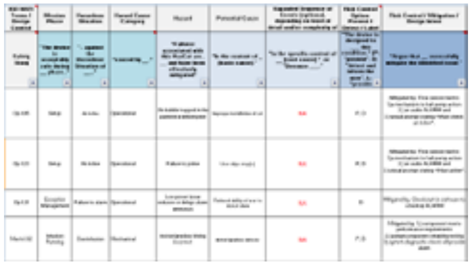
+

RISK-BASED TABLE

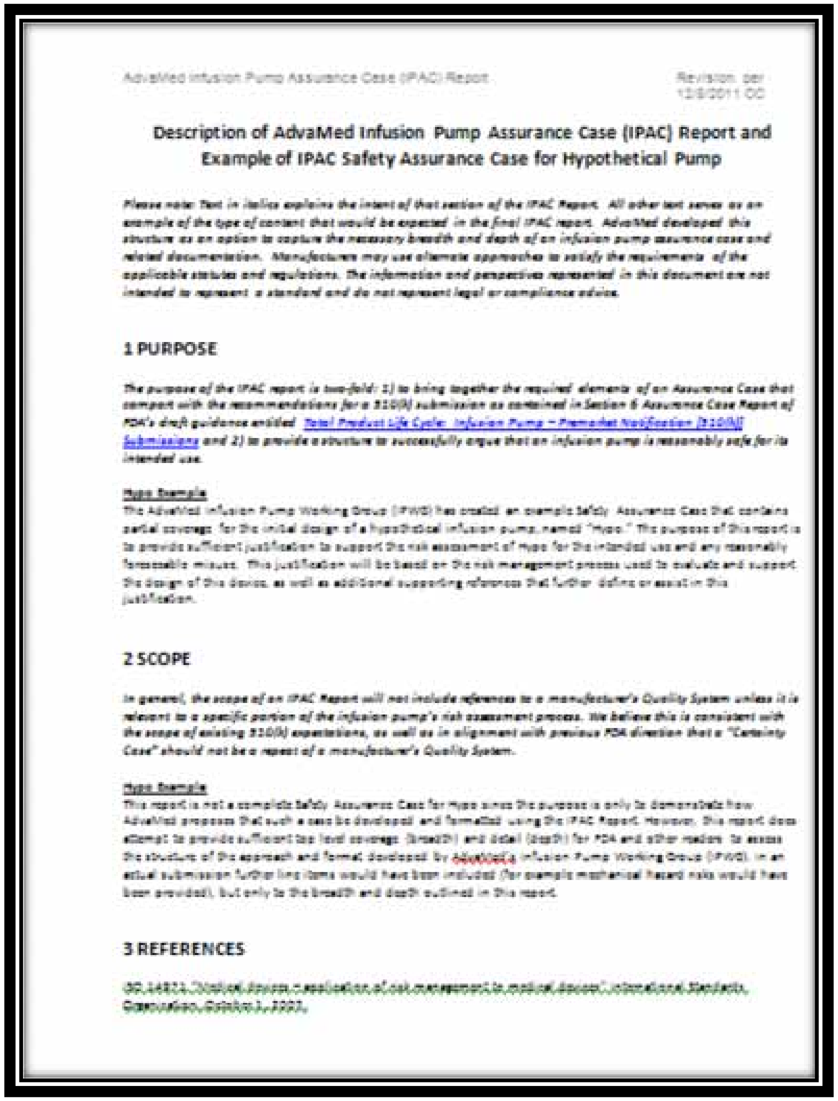
Top level, mitigated Risks are detailed and categorized

=

IPAC



AdvaMed Example Report



AdvaMed Infusion Pump Assurance Case (IPAC) Report

Revision: per
12/8/2011 CC

Description of AdvaMed Infusion Pump Assurance Case (IPAC) Report and Example of IPAC Safety Assurance Case for Hypothetical Pump

Please note: Text in italics explains the intent of that section of the IPAC Report. All other text serves as an example of the type of content that would be expected in the final IPAC report. AdvaMed developed this structure as an option to capture the necessary breadth and depth of an infusion pump assurance case and related documentation. Manufacturers may use alternate approaches to satisfy the requirements of the applicable statutes and regulations. The information and perspectives represented in this document are not intended to represent a standard and do not represent legal or compliance advice.

1 PURPOSE

The purpose of the IPAC report is two-fold: 1) to bring together the required elements of an Assurance Case that comport with the recommendations for a 510(k) submission as contained in Section 6 Assurance Case Report of FDA's draft guidance entitled Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions and 2) to provide a structure to successfully argue that an infusion pump is reasonably safe for its intended use.

Hypo Example

The AdvaMed Infusion Pump Working Group (IPWG) has created an example Safety Assurance Case that contains partial coverage for the initial design of a hypothetical infusion pump, named "Hypo." The purpose of this report is to provide sufficient justification to support the risk assessment of Hypo for the intended use and any reasonably foreseeable misuse. This justification will be based on the risk management process used to evaluate and support the design of this device, as well as additional supporting references that further define or assist in this justification.

2 SCOPE

In general, the scope of an IPAC Report will not include references to a manufacturer's Quality System unless it is relevant to a specific portion of the infusion pump's risk assessment process. We believe this is consistent with the scope of existing 510(k) expectations, as well as in alignment with previous FDA direction that a "Certainty Case" should not be a repeat of a manufacturer's Quality System.

Hypo Example

This report is not a complete Safety Assurance Case for Hypo since the purpose is only to demonstrate how AdvaMed proposes that such a case be developed and formatted using the IPAC Report. However, this report does attempt to provide sufficient top level coverage (breadth) and detail (depth) for FDA and other readers to assess the structure of the approach and format developed by AdvaMed's Infusion Pump Working Group (IPWG). In an actual submission further line items would have been included (for example mechanical hazard risks would have been provided), but only to the breadth and depth outlined in this report.

3 REFERENCES

ISO 14971, "Medical devices – application of risk management to medical devices", International Standards Organization, October 1, 2007.

Contents

- Purpose
- Scope
- Definitions
- Intended Use/Indications for Use
- Device Description
- Hazardous Situation Discussions
- Post Market Quality Actions
- Risk-Based Table
- High-Level Strategy

Emergent Behavior

By eliminating the game-of-telephone, and putting the safety story in a single top-to-bottom executive summary, we can see things that we didn’t see before.

This addresses two of the failure modes of risk management from an earlier slide:

1. The design team missed a detail
2. The design team forgot to write down the rationale for a decision

Replacement for the Risk Report

The Safety Case Report serves as an executive summary of the risk management activities and corresponding key results.

So why not make it the Risk Management Report required by 14971?

In fact, for demonstrating periodic reviews required by 14971, you could simply update the Safety Case Report. Clinical literature reviews, complaints, AEs, CAPAs, etc, all impact the risk file. What better way to reflect these updates than a refresh of the Safety Case Report?

Agenda

Reviewing a Medical Device Assurance Case

Properties of a good Assurance Case

Arguments must be compelling, valid, and sound; Evidence must be relevant, complete, etc.

Developers do not normally have experience reviewing from these particular viewpoints.

Greenwell, Knight, Holloway, and Pease reviewed a series of Assurance Cases and documented their findings in “A Taxonomy of Fallacies in System Safety Arguments” – perhaps those fallacies could be the starting point for a developer’s review ?

Case Study – Project A, Initial Review

Project A was selected for an experimental review cycle. The team had completed ~ 50 arguments out of an estimated 300, and was looking for feedback.

The Taxonomy was used as a reference, I served as an independent reviewer.

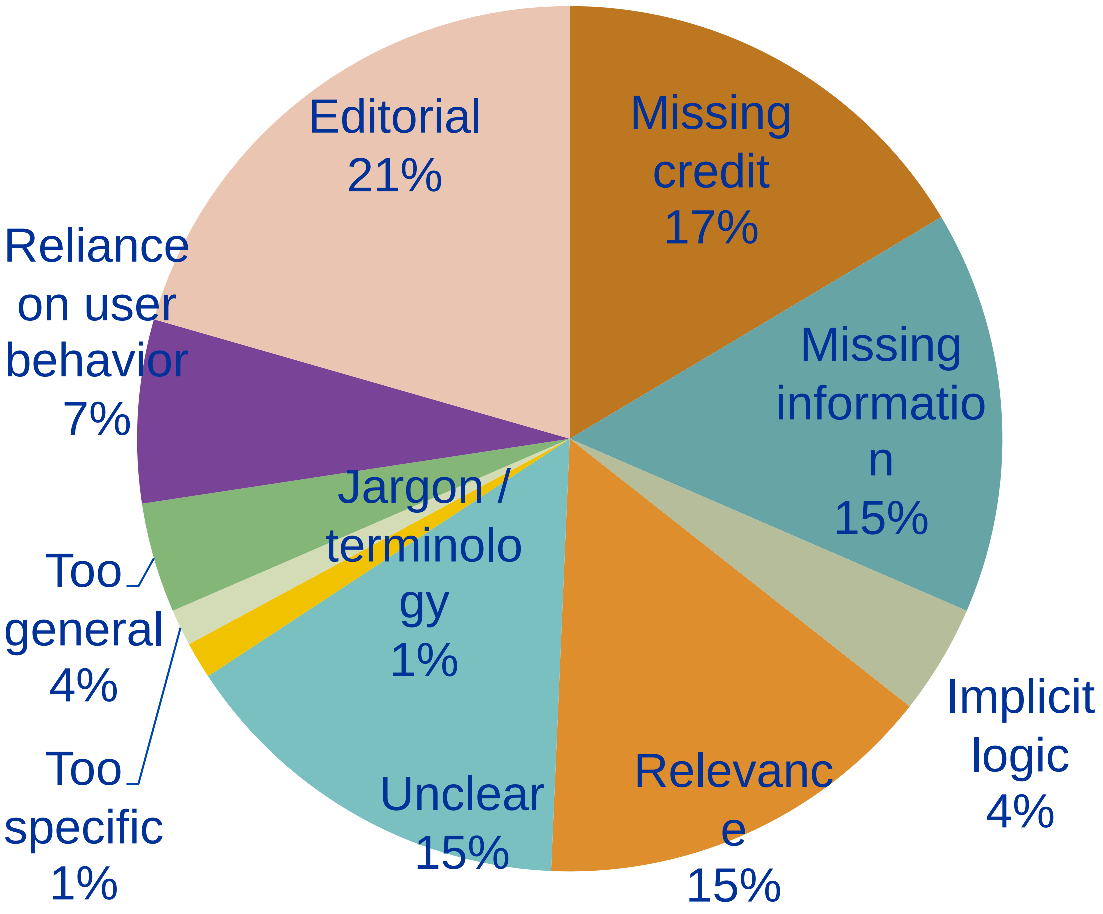
Results: While the Taxonomy provided feedback to the team, it did not give the team a good feel for areas of improvement. It’s useful to know what is wrong. It’s more useful to know what it takes to fix it.

Case Study – Project A, Secondary Review

Based on this feedback, a second review was performed to detect patterns of document errors – their own taxonomy of errors.

This new taxonomy was used for a re-review

Takeaway: Customized feedback is more valuable than Universal



Case Study – Project B, Initial Review

Project B is a legacy product where a Safety Case was being created from existing documents + new supplemental information.

Again, a sample set of Arguments and Evidence were selected to establish a taxonomy.

The team settled on just 4 categories:

- Incomplete
- Incorrect
- Unclear
- Weak

Reflection

Given this feedback, how should the team prioritize ?

How strong do Arguments and Evidence have to be?

It’s been said that

If everything is important, then nothing is important

Risk Control is about taking action commensurate with Risk.

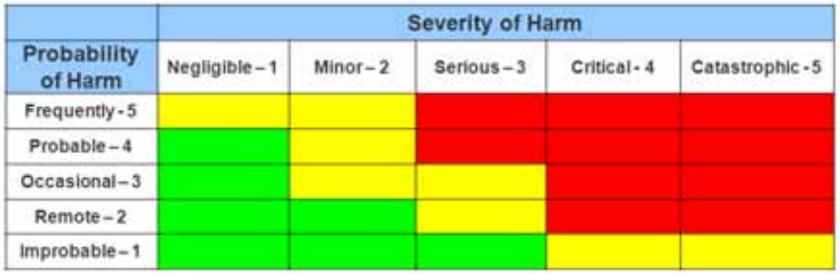
What if the Safety Case Review was commensurate with Risk?

Since we are in an FMEA anyway…

We normally calculate

Risk Priority Number (RPN) = Severity x Probability

and use a table to determine when to take action.



Probability of Harm	Severity of Harm				
	Negligible – 1	Minor – 2	Serious – 3	Critical - 4	Catastrophic - 5
Frequently - 5	🟨	🟨	🟥	🟥	🟥
Probable – 4	🟩	🟨	🟥	🟥	🟥
Occasional – 3	🟩	🟨	🟨	🟥	🟥
Remote – 2	🟩	🟩	🟨	🟥	🟥
Improbable – 1	🟩	🟩	🟩	🟨	🟨

We want high Risk items to have strong Arguments and Evidence… What if we assessed the Strength of the Argument & Evidence, and multiplied that by the RPN, and take action to strengthen the Arg & Evidence based on a similar table?

The Crossover Idea!

"Appropriateness Priority Number" is a supplemental calculation to the RPN.

Each Argument and Evidence is rated on a scale of High, Medium, and Low.

We created an Appropriateness table based on RPN and Strength. The goal is to have high Risk items mitigated by strong arguments and strong evidence.

This focuses the team on the most important things first.

Takeaway: Leverage the analytics of RPN with the strengths of Assurance Theory to come up with a system that is better than either alone!

Reviewing a Safety Case: Takeaway

Sometimes, you need to customize your review activities to work for a given situation..

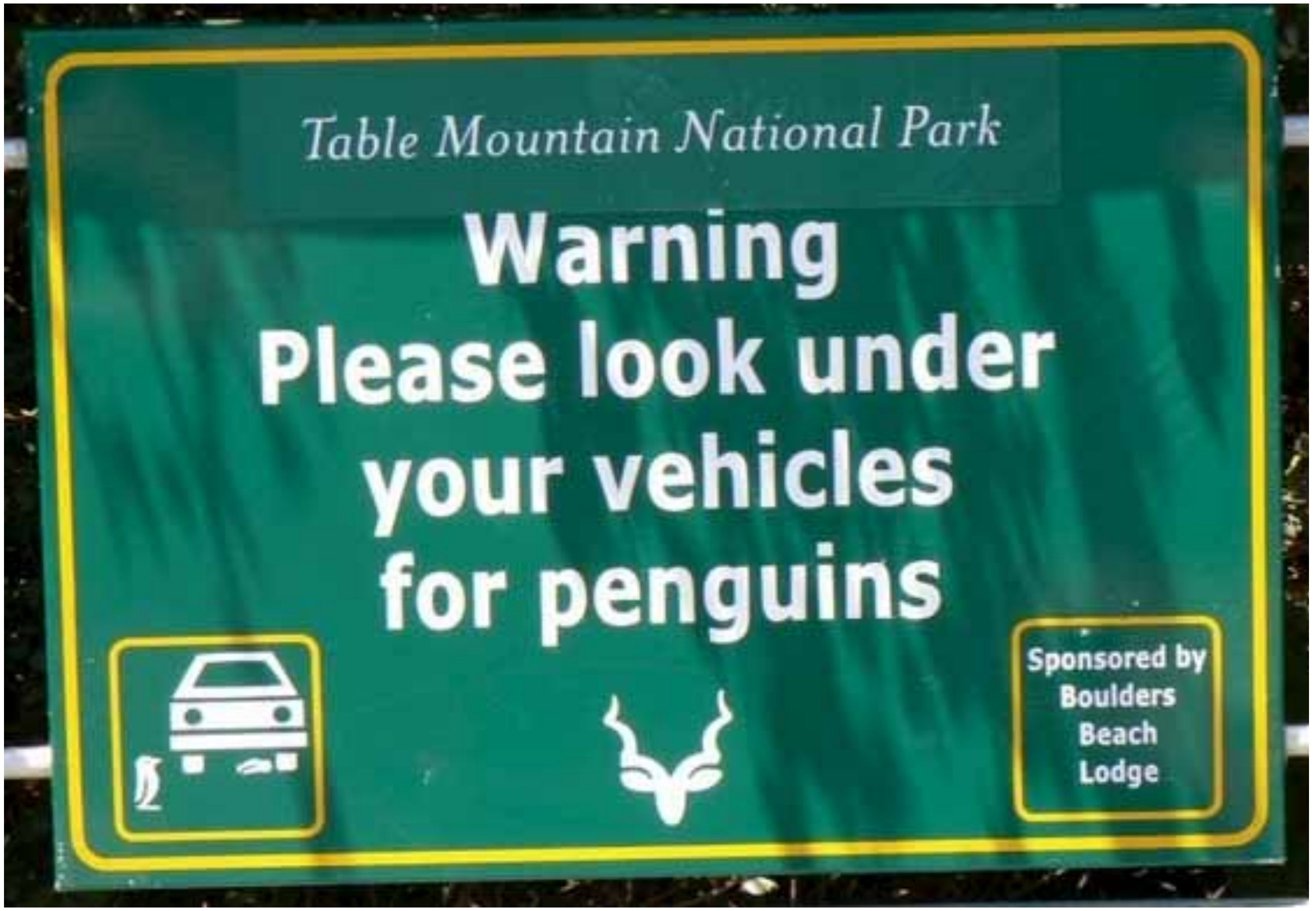


Table Mountain National Park
Warning
Please look under your vehicles for penguins
Sponsored by Boulders Beach Lodge

“Challenge Cases”

Extreme Assurance

When developing the Appropriateness measure, I came across “Success Arguments: Establishing Confidence in Software Development” [Graydon & Knight]

Success Arguments are a rigorous rationale for believing development efforts will succeed.

In statistics, it is common to “test for the null hypothesis.” To prove something is true, you attempt (and fail) to prove that it is not true.

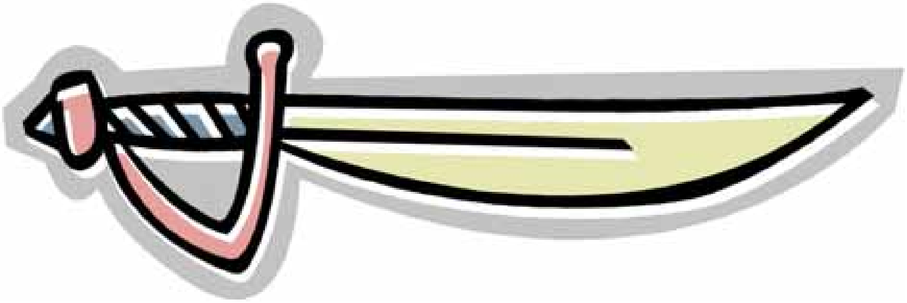
What if we did the same thing with Success Args..

The IDEA - “Challenge Claim”

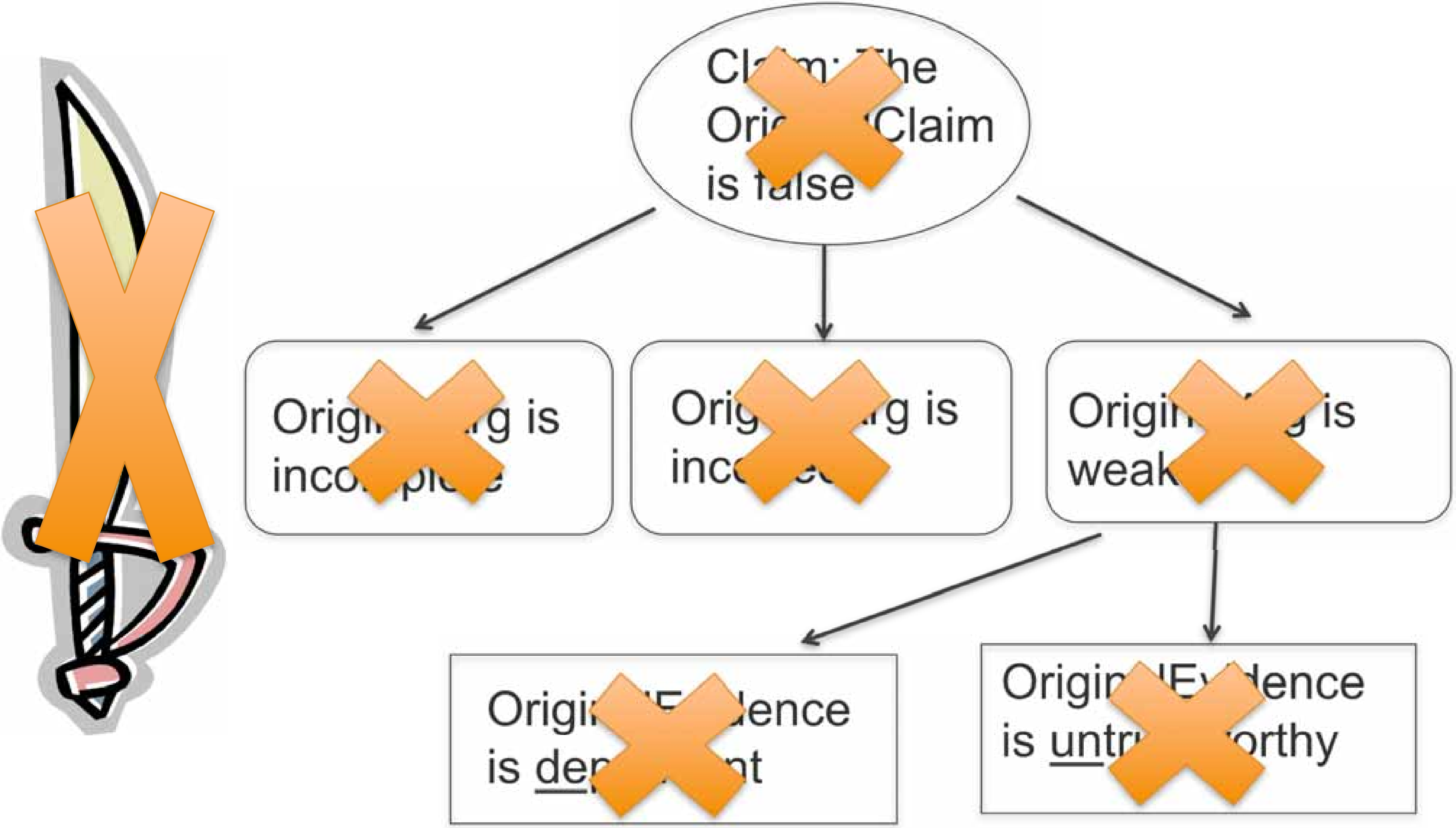
For vitally important Claims, what if we attempted make exactly the opposite Claim?

“ChallengeClaim: the OriginalClaim is false.”

The task for the reviewer then is to try to prove the ChallengeClaim is true. The task for the author is to disprove the ChallengeClaim.



Building the Challenge Argument


Claim: The Original Claim is false
Original Arg is incomplete
Original Arg is incorrect
Original Arg is weak
Original Evidence is dependent
Original Evidence is untrustworthy

Status

Currently developing a ChallengeArgument for software development processes.

Wrapup

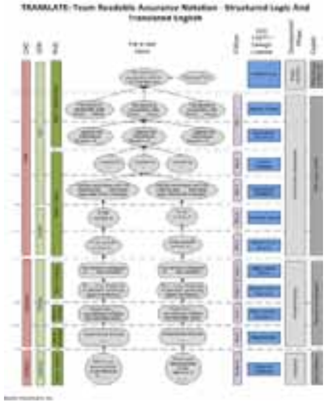
To Recap…

We examined our **Work Products**

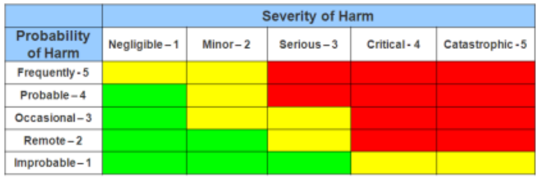
And our **Methods**

Others use **Assurance**

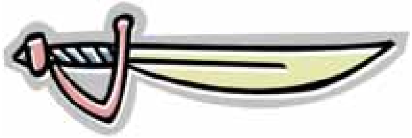
We can too.


TRANSLATE: Team Readable Assurance Notation - Structured Logic And Translated English

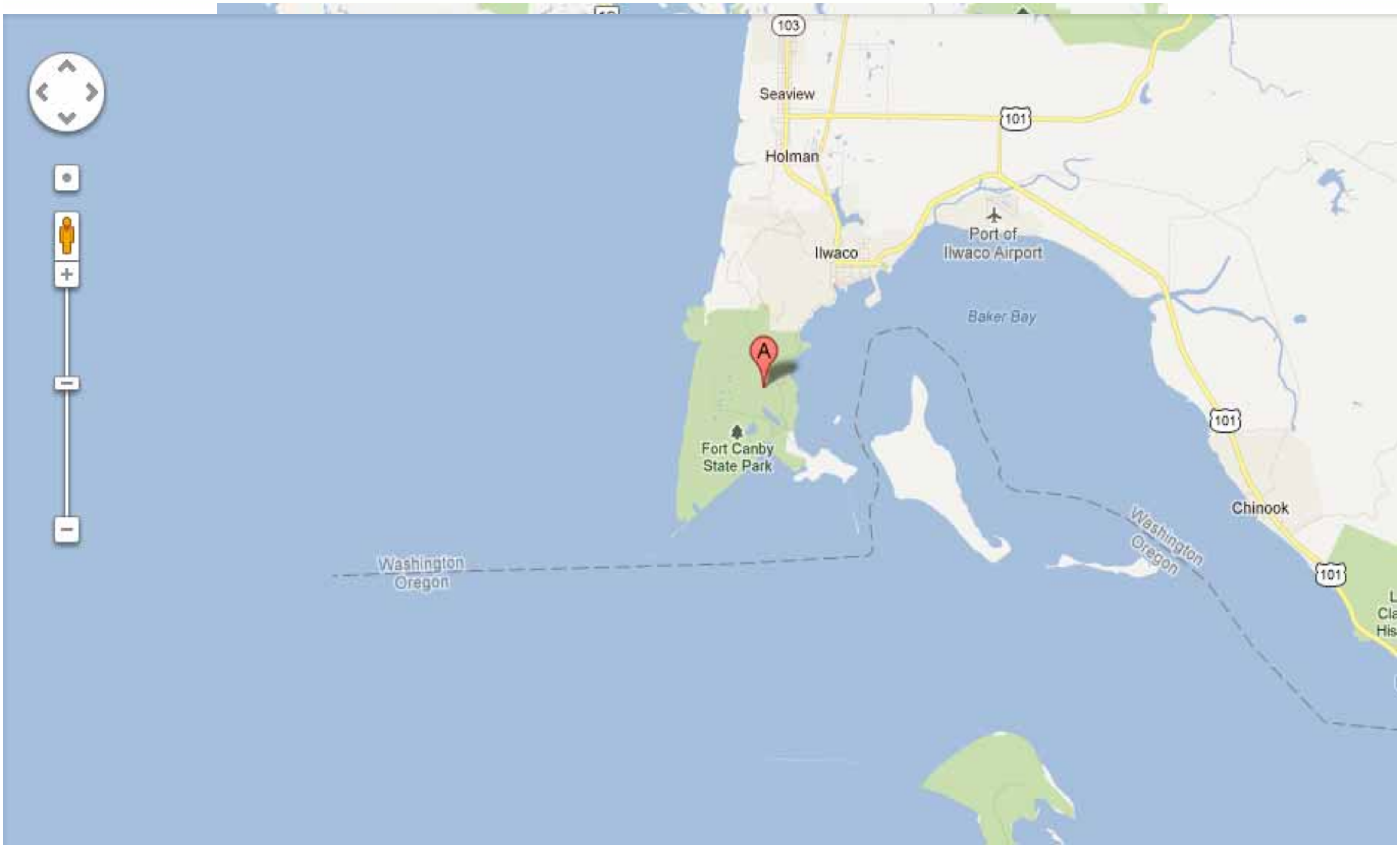
And maybe can even **Add to the Practice**



	Severity of Harm				
Probability of Harm	Negligible – 1	Minor – 2	Serious – 3	Critical - 4	Catastrophic - 5
Frequently - 5	🟨	🟨	🟥	🟥	🟥
Probable – 4	🟩	🟨	🟥	🟥	🟥
Occasional – 3	🟩	🟨	🟨	🟥	🟥
Remote – 2	🟩	🟩	🟨	🟥	🟥
Improbable – 1	🟩	🟩	🟩	🟨	🟨



Parting Thoughts – the Story of Cape Disappointment…



Wisdom from a well-published authority

“Unless someone like you

Cares a whole awful lot

Nothing is going to get better

It’s not.”

- Dr. Seuss

Open Discussion