Do’s and Don’ts with Product Risk Management

Thomas M. Heckmann, P.E

October 25, 2023
Agenda

• Introduction

• Risk Management

• Some Dos and Do Nots with

• Tales of Weal and Woe

• Discussion / Questions

Disclaimer:

• *Statements and opinions given here are my own, and may not represent the position of Baxter or any other organization*

• *Topics presented are anonymized or available in the public record*

• *Images are used with attribution or are not copyrighted in the public domain*

• *Presentation content not to be reproduced except in entirety*

• *Any case-studies are “Monday-morning-quarterbacking” and based upon incomplete information – not to second-guess behaviors at time or trying to identify culpability, fault, etc. – rather, my intent is to learn from past to help improve safety for everyone in the future*
Introduction
About me

- **Thomas M. Heckmann, P.E.**
- Sr. Principal Engineer, Quality Operations / Element Steward GQR-10, Product Risk Management
- Located in Buffalo-Niagara region of New York
- Serving Baxter since November 2015
- Licensed Professional Engineer (P.E.) since 2003
- Senior Member IEEE
- BS Engineering Physics (Electrical Engineering and Physics) from SUNY at Buffalo
- Prior experience in Research, Product Development, Manufacturing, Forensic Analysis, Laboratory Operations, Global Regulatory Compliance, Quality Management, and 3rd party Quality/Health/Safety/Environmental Certification

Statements and opinions given here are my own, and may not represent the position of Baxter.
My Day Job

- My Function is Element Owner/Steward for QMS Element 10 – Product Risk Management
- Primary responsibilities

  An element steward is assigned to each QS element as the lead Subject Matter Expert. Element Stewards are responsible for the following:
  - Develop and maintain quality processes and systems that meet customer and regulatory requirements
  - Drive consistent deployment of their QS element
  - Provide guidance around their QS element
  - Ensure alignment throughout the organization through global input/interaction
  - Drive continuous improvement and implement best practices
  - Ensure process implementation applies a risk-based approach, as appropriate

The Quality System Element develops/revises content with input from global subject matter experts
Steward:

- We cannot have wide open processes leading to wild behavior

- We cannot smother the business with strict administration

- We must curate a middle way with balanced and interconnected processes to allow adaptation and efficiency operation to enable a broad portfolio of safe and approved products
Sterility Assurance & Quality Risk Management Conference

Risk Management
A ship in harbour is safe, but that is not what ships are built for.

- John A. Shedd, 1928
What kind of Risk are we talking about?

The **product** must be of **benefit** when **weighed** against the **risks**.

- **Medical Products**
- **Medical Benefit**
- Judged by Persons qualified by education and experience
- Considering the residual risks (acceptable only after mitigations reduce risks as far as possible)

Or else the product cannot be put on the market!
Evolution of Safety Standards

- BASIC SAFETY – Straightforward – Follow Code
  - Fire
  - Electric Shock
  - Mechanical Injuries (sharp points/edges)
  - Toxins
  - High Temperatures, High Pressures
  - Other Energy (Lasers, Audio levels)
- ESSENTIAL PERFORMANCE – Tricky
  - Need to cause ‘harm’ to cure
  - Innovation needed
  - “Compliance is checked by inspection of the Risk Management File”
Risk Management in Standards

- Example: IEC 60601-1 Medical Electrical Equipment – Part 1: General requirements for basic safety and essential performance

- Risk Management is used throughout the standard
  - “the Risk Management File” is used 226 times in consolidated version; discounting redline (duplicates), and information, around 100 uses
  - “Compliance is checked by inspection of the Risk Management File”, 30 times in the Blackline version
  - Typical entries:

```plaintext
12.1 Accuracy of controls and instruments
When applicable, the MANUFACTURER shall address in the RISK MANAGEMENT PROCESS the RISKS associated with accuracy of controls and instruments.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

11.6.8 Compatibility with substances used with the ME EQUIPMENT
When applicable, the MANUFACTURER shall address in the RISK MANAGEMENT PROCESS the RISKS associated with compatibility with substances used with the ME EQUIPMENT. Such RISKS may be addressed through the application of appropriate ISO or IEC standards (giving the presumption of acceptable RISK according to 4.2) such as ISO 15001 [70] for components that contain oxygen at pressures greater than 50 kPa or through the MANUFACTURER’s own testing and RISK CONTROL measures.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.
```
Common Sense?

• “Isn’t Risk Just Common Sense?”
Do Remember that Risk Management Files Must Communicate Risks to Stakeholders

Risk Files must ‘Tell the Story’ of Safety
“Can I go to my friend’s house?”

- You’re the Mom.
- Yes or No, is it safe for her to go to her friend’s house?

What are the Risks? Are they acceptable?
Hazards?

• Could injure feet walking. Severity 3
• Could get lost walking journey. Severity 4
• Could get wet in Rain/Snow Storm. Severity 2
• Could get mugged/assaulted. Severity 5
• Could get hit by traffic. Severity 5
• Could arrive destination late. Severity 1

ACCEPTIBILITY CRITERIA – BECAUSE MOM SAYS SO!
MONITORING – Chris’s parents will call Mom.
“Can I go to my friend’s house?” Analysis?

Failure Modes & Causes And Effects:
Daughter takes wrong way
Daughter slips/trips/has problems walking
Daughter not able to cross the street properly
Acts of God (Weather)
Stranger Danger / Criminals
Construction sites
Leave too late (dark)
Risk Controls?

“I know the way, Ma!”

“No crossing busy streets!” or “Wear a coat!”

“Call or get a ride home if after dark”
Unacceptable/Unneeded Risk Controls?

Risk of overheating, loss of peripheral vision, loss of mobility

Stranger Danger / Criminals

- A Christmas Story (1983) MGM
BENEFIT?

Clinical Risk Benefit Analysis

“Why should you be allowed to go to your friend’s house?”

- Good for child’s happiness, socialization and development
- Get some peace and quiet for Mom
- Mom doesn’t have to drive

“Fine you can go! Be back before dark.”
Follow On

Do Not Ignore Risk Management File when Writing Plans and Reports

Communicate! Work together...
Clinical design goals align with Risk
Do Standardize Hazardous Situations and their Harms

The Clinical focus on these
Severity of Harm modeling systems

ISO 14971:2019 Clause 5.5:
“The system used for...categorization of...severity of harm...shall be recorded in the risk management file."

- Manufacturers are responsible for identification of any system of their choice* (*that works best for them)
  - Needs to function within their company
  - Needs to allow manufacturers to make wise decisions
  - Needs to allow manufacturers to innovate and adapt
  - Needs to help manufacturers to make safe products
- The system chosen shall categorize the harms
  - Categories by ‘level’ or ‘range’ enable consistent analysis
- The system shall be recorded
  - This enables communication to internal company functions that all use the risk model
  - The system is communicated to regulatory authorities in documents

Baxter – Public Release
Plotting Severity of Harm on Y axis implies a continuous value, but placement of risk points implies discrete values. “Severity is, in reality, a continuum; however, in practice, the use of a discrete number of severity levels simplifies the analysis.”
Definition and levels are common, simple numbers can be used for levels.
Limits with Simple numbers in Risk model

Linear?

No! Clearly five harms of level 1 severity are not the same as one 5+

Exponential?

Level 1 and Level 2 harms irrelevant, 3 pales in comparison to 4, 5

Mathematical operations on these categories are model abstractions that may not be meaningful or appropriate.
Problems with Simple numbers in Risk model

Can one number represent the result for a Hazardous Situation appropriately?

Example:
10 million units in field. 1000 complaints of event of Hazardous Situation ‘Sharp Point at X’ occurring to patient in the field.

Careful Study of the events of the same exposure of Hazardous Situation find:
- 887 patients had no injury observable, but reported the exposure to the H.S.
- 100 lacerations occurred to patients’ limbs, needing only adhesive bandage
- 10 lacerations occurred to patients’ limbs, needed reapproximation (surgical closure of wound) and sutures to prevent scarring
- 1 patient had arterial bleeding and needed blood transfusion and surgery
- 1 patient died, possibly of heart attack

What Number / Level represents the proper Severity of Harm to use in a Risk Model for Hazardous Situation ‘Sharp Point at X’ in this Case?

More Detailed Models of Severity of Harm may be More Useful in this case.
Not Every Exposure to a Hazardous Situation has the same result

Many people may be ‘exposed to’ a toy on the steps, few people will suffer the harm of fall and injury of broken bones.
An Implementation: Three Ranks of Harms

<table>
<thead>
<tr>
<th>Severity Rating</th>
<th>Harm Severity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Death, permanent impairment of function... etc.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Temporary or non-life-threatening impairment... etc.</td>
</tr>
<tr>
<td>Minor</td>
<td>Results in no harm, or a temporary impairment that does not require additional medical interventions ... etc</td>
</tr>
</tbody>
</table>
An Implementation of Seven Ranks of P2

Each Level of Harm has a P2 Probability Rating Term established, which also represents a mathematical range

<table>
<thead>
<tr>
<th>Probability Rating Term</th>
<th>Qualitative Definition</th>
<th>Percentage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected</td>
<td>This is the outcome that will occur the majority of time</td>
<td>&gt; 50% - 100%</td>
</tr>
<tr>
<td>Likely</td>
<td>This a frequent outcome</td>
<td>&gt; 24% to &lt;= 50%</td>
</tr>
<tr>
<td>Often</td>
<td>This outcome is expected to occur regularly</td>
<td>&gt; 10% to &lt;= 24%</td>
</tr>
<tr>
<td>Periodic</td>
<td>This outcome it expected to occur intermittently</td>
<td>&gt; 1% to &lt;= 10%</td>
</tr>
<tr>
<td>Occasional</td>
<td>This outcome may occur</td>
<td>&gt; 0.01% to &lt;= 1%</td>
</tr>
<tr>
<td>Rare</td>
<td>This outcome is unlikely</td>
<td>&gt; 0.0001% to &lt;= 0.01%</td>
</tr>
<tr>
<td>Exceptional</td>
<td>This outcome is extraordinary</td>
<td>&gt; 0 to &lt;= 0.0001%</td>
</tr>
</tbody>
</table>
Result

Table for each medical therapy, identifying the hazards, list of hazardous situations and classification of severity of harms to be considered for risk evaluation

Example Hazard, Hazardous Situation list with scored Harms:

<table>
<thead>
<tr>
<th>Risk Identification (Therapy Level)</th>
<th>Risk Analysis (Therapy Level) (P2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard</td>
<td>Hazardous Situation</td>
</tr>
<tr>
<td>A</td>
<td>A1</td>
</tr>
<tr>
<td>A</td>
<td>A2</td>
</tr>
<tr>
<td>A</td>
<td>A3</td>
</tr>
<tr>
<td>B</td>
<td>B1</td>
</tr>
<tr>
<td>B</td>
<td>B2</td>
</tr>
<tr>
<td>C</td>
<td>C1</td>
</tr>
<tr>
<td>D</td>
<td>D1</td>
</tr>
<tr>
<td>D</td>
<td>D2</td>
</tr>
</tbody>
</table>
Follow On

Do Not Overclassify the Severity of Harms for Hazardous Situations

Overly conservative scoring does not lead to a safer product
**Follow On**

Do not define your Hazardous Situation Ranges down to Zero

At some level (band) there is no hazard
Tales of Weal and Woe
Do use the FDA Recall database to look at similar / competitive products

Learn from other’s mistakes
The Tale of Heal Thyself Eye Doctor

- New Product Planned
- Performed Risk Analysis
- Identified Competitor Recall for issue
- Added foreseen risk in Risk Analysis
- Two mitigations
  - Fortify the mechanism
  - Improve the tip
- Successful product launch with no delays

Do learn from others
Do capture as foreseen risk
Do mitigate
Do Not Over Mitigate

Excessive Risk Controls can introduce risks
The Tale of Mitigating the Mitigating

- Legacy fluid pumping device
- Had complaints related to an alarm code
- Alarm code to detect (mitigate) if two temperature sensors disagreed

Complaints of Alarm Stopping Fluid Flow
Tale of Mitigating the Mitigating

- First Temperature Sensor Compensated (Mitigation) for Temperature Error
  - Data showed that ambient temperature can cause error in accuracy
- Second Temperature sensor monitored the first, as a Risk Mitigation to the failure of the first Mitigation
  - If the temperature monitor disagreed during monitoring, Alarm and Stop
• **Basic Safety & Essential Performance**
  - Life saving / Life Sustaining
  - Risk if doing something; risk if doing nothing.

You'll be "damned if you do, and damned if you don't."

— Eleanor Roosevelt —

"DO WHAT YOU FEEL IN YOUR HEART TO BE RIGHT — FOR YOU'LL BE CRITICIZED ANYWAY. YOU'LL BE DAMNED IF YOU DO, AND DAMNED IF YOU DON'T."

ELEANOR ROOSEVELT
The Tale of Mitigating the Mitigating

• Analysis showed LESS risk to NOT monitor the primary inaccuracy monitor with secondary monitor. Allow the primary monitor to function with other controls in place
• Primary monitor was reliable with self-tests; external monitor
• Result – Next gen product removed monitor of monitor from system
  • Lower Risk
  • Fewer complaints
  • Saved $

Do Not mitigate to excess, or incorrectly
Do assess mitigations for new risks
Fewer mitigations decreased risk in this case
Follow On

Do Understand how to mitigate As Far As Possible

What degree of controls is sufficient?
Risk Reduction Methods

Inherent safety by design and manufacture

Hazard is removed or cannot occur by design.

Applies when risk is no longer reasonably foreseeable by product’s inherent properties.

Example: Design with an alkaline battery power eliminates risk of electric shock from AC power.

Adding Risk Control (design mitigation)
Risk Reduction Methods

Control measures in product or process

Reduced

Adding Risk Control (design mitigation)

Most typically control measures are applied. Control measures can reduce the risk. Controls measures that apply to process can reduce risk of defects.

Example electrical insulation is a risk control to reduce the risk of electric shock.
Information for Safety (Labeling, Training) can instruct users on behaviors to be aware of residual risks.

Trained and educated users benefit from more complete information for safety.

Example: warnings, procedures, and training helps service personnel avoid the hazard of electric shock.
AFAP does not mean infinite risk mitigation, rather, the right amount of mitigation.

Adding too many mitigations can increase risk...

...from usability complexity, loss of reliability, more failure modes, deskilling, unexpected behavior.
Follow On

Do not associate All Alarms with Malfunctions if not appropriate

Some Alarms are related to normal function
Do use Risk Management to manage Alarm prioritization
Do not ‘Systems Engineer’ the Risk Management File overmuch

Overdoing a risk file makes it hard for others to comprehend
Did a Survey for speaking topics

<table>
<thead>
<tr>
<th>Topic</th>
<th>Votes:</th>
<th>1 (least)</th>
<th>2</th>
<th>3</th>
<th>45 (most)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>F</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>G</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>I</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>J</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>K</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>L</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>M</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>N</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Weighted the Results by Vote Preference

<table>
<thead>
<tr>
<th></th>
<th>1x(least)</th>
<th>2x</th>
<th>3x</th>
<th>4x</th>
<th>5x (most)</th>
<th>SUM</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>8</td>
<td>0</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>2</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>8</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>8</td>
<td>0</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>21</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>8</td>
<td>5</td>
<td>18</td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>1</td>
<td>0</td>
<td>9</td>
<td>4</td>
<td>5</td>
<td>19</td>
<td>4</td>
</tr>
<tr>
<td>G</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>4</td>
<td>5</td>
<td>21</td>
<td>2</td>
</tr>
<tr>
<td>I</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>14</td>
<td>9</td>
</tr>
<tr>
<td>J</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>4</td>
<td>0</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>K</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>8</td>
<td>10</td>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>L</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>10</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>M</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>15</td>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>N</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>8</td>
<td>5</td>
<td>20</td>
<td>3</td>
</tr>
</tbody>
</table>

Isn’t this Weighting just like risk?  
Are these 22’s and 16’s really important?
Physicist Approximations

We'll assume the curve of this rail is a circular arc with radius $R$. 

$d = 2\pi \left( \frac{R}{2} \right)$
**Physicist Approximations**

We'll assume the curve of this rail is a circular arc with radius $R$.

**Engineer Approximations**

Let's assume this curve deviates from a circle by no more than 1 part in 1,000.
**PHYSICIST APPROXIMATIONS**

We'll assume the curve of this rail is a circular arc with radius R.

**ENGINEER APPROXIMATIONS**

Let's assume this curve deviates from a circle by no more than 1 part in 1,000.

**RISK APPROXIMATIONS**

Assume pi is one.

Pretty sure it's bigger than that.

Ok, we can make it ten. Whatever.

\[ d = 2\pi \left( r + \frac{r^2}{2} \right) \]
The Tale of Missing the Point

• Submission to Regulatory Body for approval
• Did not submit the list of hazards
• Did not submit the procedure for risk management
• Some parts of the risk management file absent
• Complex analysis submitted
• Receive Finding / non-acceptance
• Needed corrective action
• New procedure and training

Do Not forget that Risk Management communicates safety to the Regulator
Failure to be clear and to submit a complete risk file necessary for context can result in non-acceptance
Follow On

Do not use Numerical Probability of Occurrence Estimates in Human Factors or Software Risk Analysis

Do use Severity of Harm in such analyses;
Regulators do not accept veracity of estimates of occurrence
Do Focus on the New and Novel

Do Not assume what was good enough before will be enough to prevent disaster
The Tale of Change for the Worse

- Battery company that made alkaline 1.5 V button-cells released a new lithium metal 3 V coin cell
- Did foresee ingestion from past alkaline knowledge
- Did have warnings against ingestion
- Did meet all standards at the time
- Yet incidents in home with battery like loose change
- 2-year-old children ingest a battery
- Suffered esophageal burns and severe harms
- Lawsuit
- Company could not show risk management had considered the new risk - of tissue necrosis from electrolysis
- New Regs, new warnings

---

Do look at what’s new and novel in context of what’s known
Do not limit thinking and fail to capture alternatives
Higher Voltage -> electrolytic current that hydrolyzed tissue fluids -> caustic hydroxide was unappreciated at time
Do Consider complex systems, and man-machine interface

Human Responses are based on their Mental Model of System Operation
Mental Model

Designer’s Model (intent)

Original Design Specifications

Instructions

Training

Actual Device/System

Manufacturing Variance, Environmental

Aging, Changes over Time

Operational Experience

Design Intent Ideal, Mean “Happy Path”

User’s Mental Model

Adapted from Fig 2.9 Engineering a Safer World, Systems Thinking Applied to Safety
Tale of the Boeing 737 MAX 800

- New engines applied to old airframe body
- New engines more efficient – larger diameter
- Moved engines forward on wing to allow landing without ground-strike
- Airframe tendency to nose up at cruise with engines forward
- Software fix – “MCAS” maneuvering characteristics augmentation system to control pitch at cruise, to prevent nose up stall
- Software fix was assessed, accepted, documented as minor adjustment, low risk, based upon severity of control, and single actuation
- Second change adjusted MCAS severity, and made cumulative
- Boeing didn’t want simulator training of users, not documented in detail in user facing documents
- 2 crashes
  - Oct 29, 2018: Lion Air 610 prior day’s crew had problem, extra pilot identified, and turned off trim power; incomplete logs, incomplete fix overnight, miscalibrated Angle of Attack sensor; airline didn’t notify next aircrew of that solution or ground the plane
  - Boeing issued operational manual guidance
  - Mar 10, 2019: Ethiopia Air 302, crew may have turned off, then turned on; tried to debug… Man-machine interface issues
- Angle of Attack sensor issues
- Culture that employees felt not empowered or comfortable to raise issues up
- Blamed schedule pressures, outsourcing, and distant HQ office from design activities
- Boeing initially thought FAA would give quick clearance of the fix
- Reorganized engineering oversight, to report to chief engineers rather business
- Added safety group, assuring work independent, reporting to the board
- New CEO
- $20B+ cost, years until cleared to fly; no 2019 bonuses to employees
Conclusion
Manage Risk well and a Ship can go Anywhere

Perseverance Rover & Ingenuity Helicopter

“This Ingenuity Mars Helicopter project is a high-risk, high-reward technology demonstration” – NASA 2021
Discussion / Questions
Thank You