A therapy based approach to risk in medical devices
Key Takeaways

A Framework for linking intended uses, patient risks and product design

✓ A mission based therapy approach

A guide to understanding the complete risk profile of the product

✓ Residual Risk rolls up all therapy related risks

A template for post-production risk analysis

✓ Complaints map directly to the risk analysis
Risk management principles should be applied throughout the life cycle of medical devices...

• …The first phase can be the determination of levels of risk that would be acceptable in the device …

• The second phase … Identifying hazards that may occur due to characteristics or properties of the device during normal use or foreseeable misuse.

• In the third phase, the estimated risks are compared to the risk acceptability criteria .. This is called risk evaluation.

• The fourth phase can be composed of risk control and monitoring activities. …

“Implementation of risk management principles and activities within a Quality Management System”
GHTF Study Group 3, May 20, 2005
Most People Address Risk through ISO 14971

ISO 14971 Outlines Risk within the following framework:\(^1\)

- **Risk** - *probability of occurrence of harm and consequences of that harm*
- **Residual Risk** - *the risk remaining after risk control measures*
- **Risk Evaluation** – *is the overall residual risk acceptable?*

There are issues associated with the ISO 14971 framework

- **There is no preferred method for evaluating residual risks**
- **The device based approach can yield incomplete results**
- **Most approaches don’t easily supports the gathering of post-production information**

\(^1\)Reference ISO 14971:2007
To determine the Residual Risk

- **Determine all P1 exposures creating a hazardous situation**
- **For each hazardous situation determine the severity and probability of harm**
- “probability of occurrence of harms” aggregated as occurrences per therapy

Note: P1 is the probability of a hazardous situation occurring
P2 is the probability of a hazardous situation leading to harm

Reference ISO 14971:2007
Fortunately the DOD has solved the problem

The FMECA (FMEA and Criticality Analysis) was developed by the National Aeronautics and Space Administration (NASA) to improve and verify the reliability of space program hardware.

A FMECA, to evaluate and document, by failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, maintainability and system performance.

Each potential failure is ranked by the severity of its effect so that corrective actions may be taken …. High risk items are those items whose failure would jeopardize the mission or endanger personnel.

"Department of the Army, TM 5-698-4, Failure Modes, Effects and Criticality Analyses (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 29 September 2006."
The Benefits of a Therapy/Mission Approach

Each Therapy is made up of phases and functions comprising a “mission”

✓ *Sequence of events from ISO 14971*

Hazards or failure modes have different criticality based upon where in the “mission” they occur

✓ *P1 exposure from ISO 14971*

The overall criticality maps failures to the “mission” impact and thus to the severity of harm

✓ *Residual Risk of ISO 14971*
Determining Mission Phases and Functions

The Mission Phases
(through the entire lifecycle)

Device Acquisition
Training
Deployment
Setup (Clinical Environment)
Programming Pump
Infusion Running
Handoff Between Users
Tear Down/Decontamination
Service the Pump

The Functions for a phase
(based upon clinical actions)

Programming Pump
- Allow Clear / Resume of Previous Infusion
- Allow General Infusion Settings to be Selected by Clinician
- Accept Infusion Data
- Accept Patient Data
- Accept Clinician Data
- Display Programming Information (Unique name specific to information displayed while programming)
- Allow General Pump Settings to be Changed (contrast, alert / alarm volume, audible feedback, etc.)
- Allow stand-by activation / deactivation
- Prevent Device Tampering
- Allow User to Start Infusion

“Failure Mode Effect Analysis Applied to the Use of Infusion Pumps”
From UCSF Study, 2005
P1 Exposure Event - a hazard (failure), sequence of events and resulting hazardous situation.

- Systematically identify events through Mission phases and functions
- Map hazards and hazardous situations for event
- Calculate probability per opportunity (infusion, session, etc.)

Note: P1 is the probability of a hazardous situation occurring
P2 is the probability of a hazardous situation leading to harm
Breaking Down the Elements of a Risk Event

\[ \lambda \times \alpha \times \beta \]

- Probability of failure leading to specific hazardous situation\(^1\)

- Event occurrence rate in each mission phase\(^1\)

- Probability of an initiating failure mode\(^1\)

\( \lambda \) – probability of a keyboard failure (device specific) \( .0000001 \)

\( \alpha \) - probability of it happening during therapy programming (therapy specific) \( .99 \)

\( \beta \) - probability of getting incorrect therapy program given the data entered is wrong (therapy specific) \( .0001 \)

Overall Probability of Hazardous Situation \( 1 \times 10^{-10} \)

\(^1\)IEC 60812, Edition 2.0, 2006-01, 5.3.4
FMECA Addresses Therapy, the FMEA Design

FMECA – Design independent therapy Level

- Therapy based identification of hazards, situations and hazardous situations
- Risk event occurrence rates consider mission/phase (α) and probability of a specific hazardous situation (β)
- Rolls up the overall residual risk

FMEA – Design dependent level

- Hazards (failures) flow down from the FMECA
- Component analysis yields predicted failure rate (λ)
- Rolls up the failure rate
P2 – Given a hazardous situation has occurred, what is the probability of harm

- **Five categories for harm** – from catastrophic (death) to negligible
- **Each hazardous situation can create every severity of harm**
- **Residual risk is calculated for each severity level**

Note: P1 is the probability of a hazardous situation occurring
P 2 is the probability of a hazardous situation leading to harm
Clinical Analysis Drives Probability of Harm

- Identify hazardous situations and harms based on MAUDE database, complaint data, literature and industry reporting
- Probability of harm estimated using these inputs, applying clinical judgment, considering current therapies, the treatment situation and patient demographics

### Estimated probability of Harm by Hazardous Situation (P2)

<table>
<thead>
<tr>
<th>Hazardous Situation</th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Serious</th>
<th>Minor</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazardous Situation #1</td>
<td>0.00000001</td>
<td>0.0000001</td>
<td>0.00000010</td>
<td>0.0010000</td>
<td>0.9989988</td>
</tr>
<tr>
<td>Hazardous Situation #2</td>
<td>0.0010000</td>
<td>0.0010000</td>
<td>0.0010000</td>
<td>0.0100000</td>
<td>0.9870000</td>
</tr>
<tr>
<td>Hazardous Situation #N</td>
<td>0.0010000</td>
<td>0.0010000</td>
<td>0.0010000</td>
<td>0.0100000</td>
<td>0.9870000</td>
</tr>
</tbody>
</table>
Putting it All Together to Calculate Risk

Scenario: Device powers on, detects a subsystem failure, delaying start of therapy

Failure causing delay of therapy (P1)
- 516 events per million therapies

Delay to catastrophic harm (P2)
- 0.1 per million events results in catastrophic harm level

Catastrophic risk for event (P1 x P2)
- $5 \times 10^{-13}$ catastrophic harms per therapy

Note: P1 is the probability of a hazardous situation occurring
P2 is the probability of a hazardous situation leading to harm
Using Total Residual Risk for Evaluation

- Residual Risk is the roll up of $P_1 \times P_2$ for all severities of harm

- Need to consider all sequences, hazard, and hazardous situation combinations

- Basis for consistent product/configuration comparisons
Consistent Linking of Development and Support

Product development

- Exposure events link sequences (intended use) to hazards (product design) and hazardous situations
- A clear mechanism for evaluating the risk implications of all design changes

Product support

- Quantitative monitoring of post market exposure events (complaints and MDR’s) linked directly to the design claims (requirements)
- More focused investigations into root cause and corrective, preventive actions
Device Complaints Map Well to the Therapy Model

What were you doing? – mission, phase and function

What went wrong? – the hazard

What issues did you have? – the hazardous situation

Was anyone hurt? – the harm and severity
Key Takeaways

A Framework for linking intended uses, patient risks and product design

✓ A mission based therapy approach

A guide to understanding the complete risk profile of the product

✓ Residual Risk rolls up all therapy related risks

A template for post-production risk analysis

✓ Complaints map directly to the risk analysis
Backup
The FMECA compiles the probability of exposure ($P_1$) with the probability of a Harm given a Hazardous Situation ($P_2$) to yield the risk. By combining all of the exposure events (component failures, Hazardous Situations and sequence of events) and probability of Harm, residual risk is established.

Within the FMECA the overall probability of a Hazardous Situation (exposure) $\lambda_i$ or $P_{1i}$, can be defined by the following equation

$$P_{1i} = \sum \lambda_j \cdot \alpha_i \cdot \beta_i$$

$\lambda_i$ – the probability of a given Hazardous Situation, $i$

$\lambda_j \cdot \alpha_i$ – the probability of a component failure. In cases where the component failure $\lambda_j$ can result in multiple Hazardous Situations, the term $\alpha_i$ is a ratio of the failure mode that results in this particular Hazardous Situation $P_{1i}$.

$\beta_i$ – the probability that this failure mode will result in the Hazardous Situation $P_{1i}$.

The summation above is across all of the component failures $j$. More information on this technique can be found within the IEC 60812:2006 specification on techniques for failure modes and effects analysis. These three terms or derivations of these terms will form the basis for the subsequent residual risk calculations.

Residual risk for the product is based upon the following formulation,

$$\text{Residual risk} = \sum P_{1i} \cdot P_{2i}$$

The summation is across all of the Hazardous Situations, $i$, for a selected Harm. That is, residual risk is the aggregation of the $P_1 \times P_2$ terms. The above calculation is conducted across all of the Harm levels for all of the distinct Hazardous Situations.
Residual Risk

The FMECA compiles the probability of exposure \( P_1 \) with the probability of a Harm given a Hazardous Situation \( P_2 \) to yield the risk. By combining all of the exposure events (component failures, Hazardous Situations and sequence of events) and probability of Harm, residual risk is established.

Within the FMECA the overall probability of a Hazardous Situation (exposure) \( \lambda_i \) or \( P_{1i} \), can be defined by the following equation

\[
P_{1i} = \sum \lambda_j \cdot \alpha_i \cdot \beta_i
\]

\( \lambda_i \) – the probability of a given Hazardous Situation, i

\( \lambda_j \cdot \alpha_i \) – the probability of a component failure. In cases where the component failure \( \lambda_j \) can result in multiple Hazardous Situations, the term \( \alpha_i \) is a ratio of the failure mode that results in this particular Hazardous Situation \( P_{1i} \).

\( \beta_i \) – the probability that this failure mode will result in the Hazardous Situation \( P_{1i} \).

The summation above is across all of the component failures \( j \). More information on this technique can be found within the IEC 60812:2006 specification on techniques for failure modes and effects analysis. These three terms or derivations of these terms will form the basis for the subsequent residual risk calculations.

Residual risk for the product is based upon the following formulation,

\[
\text{Residual risk} = \sum P_{1i} \cdot P_{2i}
\]

The summation is across all of the Hazardous Situations, i, for a selected Harm. That is, residual risk is the aggregation of the \( P_1 \times P_2 \) terms. The above calculation is conducted across all of the Harm levels for all of the distinct Hazardous Situations.