



Improving Risk Management Processes

Experience Report

Pat Baird

December 2009



Background

- My team is involved in the investigation and remediation of product issues found in fielded devices.
- This Experience Report is about how this team has used Risk Management to improve safety faster & with less cost.



Problem Statement

My team would come to me with questions such as

- “There are multiple root causes that can be addressed – how do I know when to stop?”
- “What fixes go into new production vs. what are mandatory field upgrades?”



Investigation Initiation

- Complaint handling is bucketed by error code reported by device
- Investigations are triggered when complaint rate exceeds a threshold
- Actions are taken to reduce the rate of a particular error code
- But, each error code can have multiple root causes
- And, each cause can have multiple fixes

Reduction in Complaints =

$$\begin{aligned} & \text{Root Cause}_1 * \% \text{Contribution}_1 * (\text{Fix}_{1,1} * \% \text{Effectivity}_{1,1} + \text{Fix}_{1,2} * \% \text{Effectivity}_{1,2} + \dots) + \\ & \text{Root Cause}_2 * \% \text{Contribution}_2 * (\text{Fix}_{2,1} * \% \text{Effectivity}_{2,1} + \text{Fix}_{2,2} * \% \text{Effectivity}_{2,2} + \dots) + \\ & \dots \end{aligned}$$

Hypothetical Example -- Communication Error

Root Cause	RC #	% Contrib	Fix	F#	% Effective	Total
Software Bug	RC1	30%	Bug fix	F1	100%	30%
Cable disconnect	RC2	60%	Locking connector	F2.1	70%	42%
			Unknown	F2.2	30%	18%
Unknown	RC3..nn	10%	Unknown	F3..nn	100%	10%
					Total	72%

So far, projected 70+% reduction – isn't that good enough?



Today's Situation

- Existing standards & SOPs tell us that Risk Management must be done in a planful way, and defines a minimum set of deliverables.
- They do not give specific direction on when to stop – no specific criteria defined.
- A traditional tool in this situation is a Risk Table

Risk Tables from SOPs

	Severity of Harm				
Probability of Harm	Negligible I	Minor II	Serious III	Critical IV	Catastrophic V
Frequent E	Investigate I-E	Investigate II-E	Unacceptable III-E	Unacceptable IV-E	Unacceptable V-E
Probable D	Acceptable I-D	Investigate II-D	Unacceptable III-D	Unacceptable IV-D	Unacceptable V-D
Occasional C	Acceptable I-C	Investigate II-C	Investigate III-C	Unacceptable IV-C	Unacceptable V-C
Remote B	Acceptable I-B	Acceptable II-B	Investigate III-B	Unacceptable IV-B	Unacceptable V-B
Improbable A	Acceptable I-A	Acceptable II-A	Acceptable III-A	Investigate IV-A	Investigate V-A

- Note that there is no Acceptable level for Catastrophic.
- We had no “Unacceptable” issues in the field, but the rate of “Investigate V-A” spanned 5 orders of magnitude – what is a reasonable threshold to stop analysis? We have over 100 error codes that predict I Catastrophic outcome in 25,000+ years



Solution: Generation Threshold

- We noted that the generational lifecycle of similar products is ~ 20 years in the marketplace.
- We proposed a portfolio of fixes to reduce each error code to have a risk < 1 Catastrophic occurrence in a Generation.
- For additional margin and to keep the calculations simpler, we estimated 20 years @ peak usage, rather than trying to project marketshare gain / loss over time.



Stakeholder Management

Initially, it looked to be a tough sell. But..

- A Pareto showed that the top 10 errors made up 80% of the product risk.
- Of 300 unique error codes, the top 25 exceeded the Generational Threshold. This constituted 95% of the product risk.
- We had people working on 35 issues, risk analysis showed one with a likelihood of 1 catastrophic outcome in 700 years.



Outcomes

- We had originally identified 80 potential fixes, risk showed only 40 were needed.
- We stopped investigations on the 10 low-risk issues.
- We shifted resources to 2 issues that whose risk was not sufficiently reduced.
- We switched from complaint rate to risk as an action trigger



Residual Risk

- It shouldn't be a surprise that some failures could not reasonably be reduced below the Generational Threshold.
- However, it is easier to demonstrate an ALARP condition when you only have to focus on the few that exceed the threshold, instead of having to justify every issue.



Scale Activities to Risk Profile

We are using risk to scale the level of design & verification effort

- “How much design margin do I need?”
- “Is analysis sufficient for verification, or do I need a test too?”
- “What sample size do I use?”



Interaction with Business

- This was focused solely on risk-based activities to identify minimums.
- The business chose to implement some changes that were already well defined, proven to work, and low cost. While these changes would not reduce risk, they will reduce complaint rates & warranty costs.



Tips on the Sell..

- While failures / million opportunities is fine for calculations & comparative purposes, translating it to a number that people can relate to gets decisions made.
- I used “5 yr DSI” as the common unit for discussion



Questions?

- Contact: pat_baird@hotmail.com
-