Certainty, Risk and Gambling in the Development of Complex Systems

Andrew C Pickard,
Chief of Process, Controls Engineering

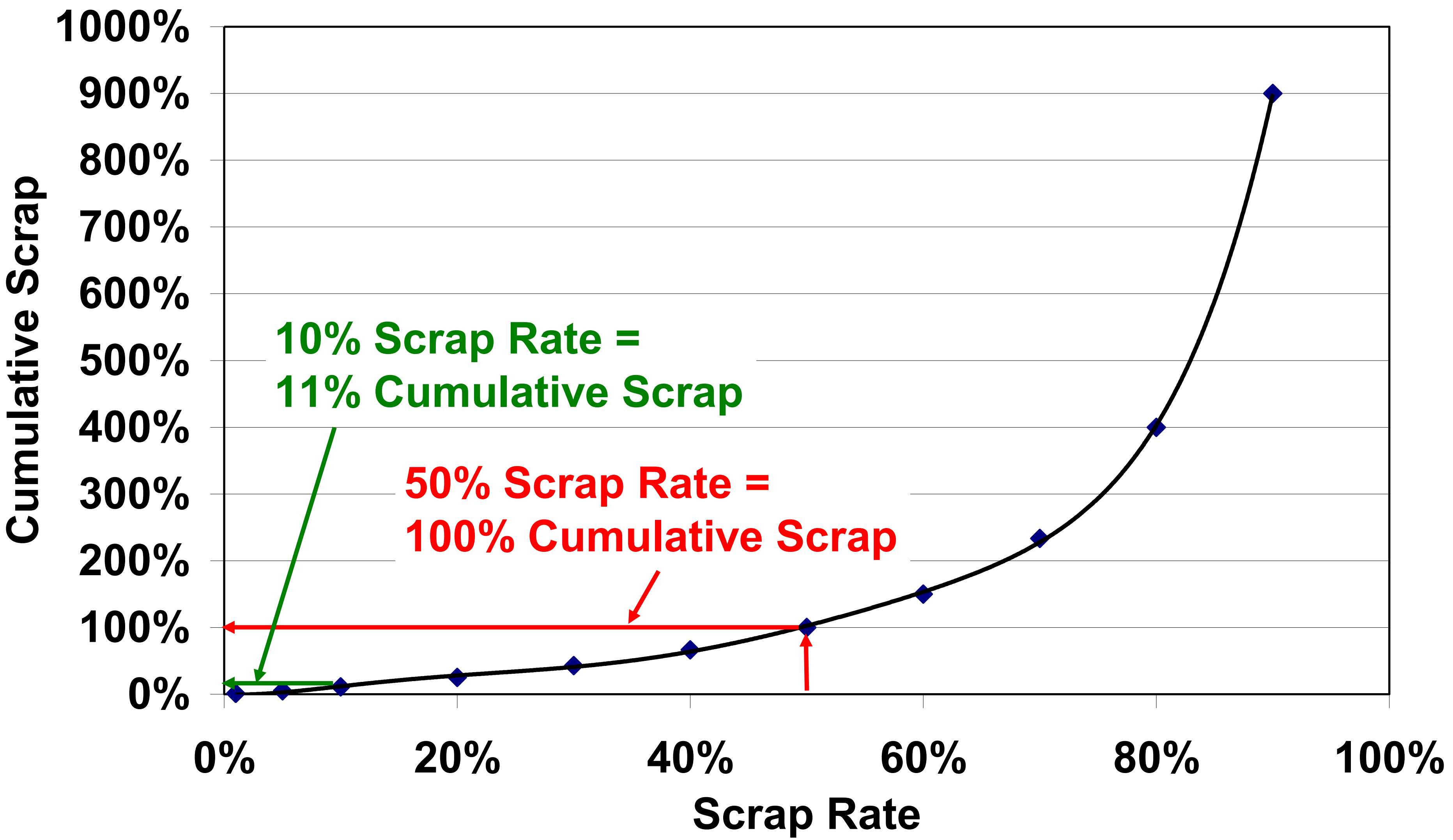
Andrew J Nolan,
Chief of Software Improvements - Software Centre of Excellence

Richard Beasley,
Systems Engineering Specialist and Corporate Skill Owner
Rolls-Royce plc

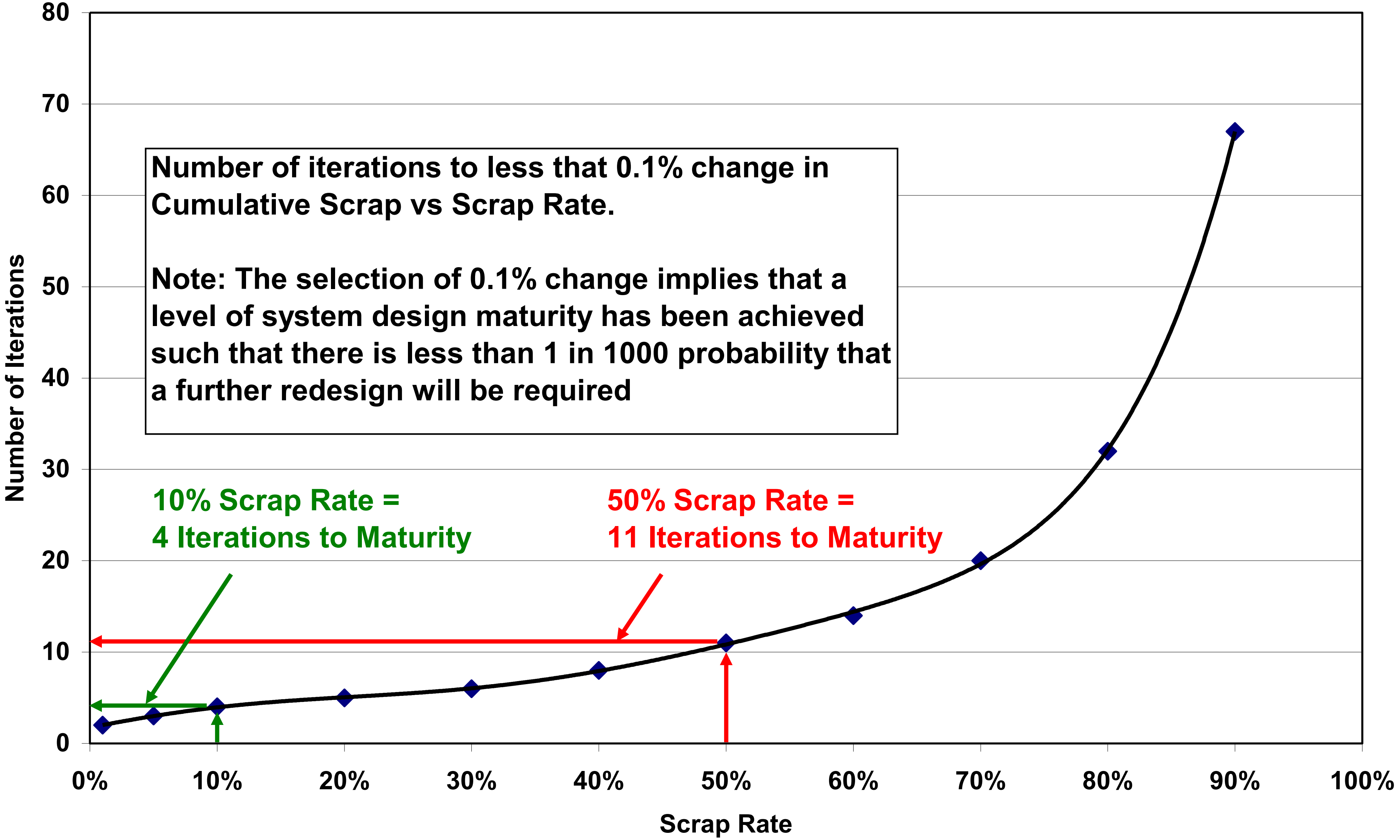
Presentation Structure

- Impact of Scrap and Rework in the Engineering Process
- Requirements Uncertainty
- Cost Impact of Late Change and Escapes
- Risk and Technical Risk Management
- Root Causes for not performing Technical Risk Management
- Technical Risk Maturity Assessment
- Risk Checklists
- Technical Risk Management Metrics
- Benefits of Technical Risk Management
- Conclusions

The Cumulative Effect of Scrap

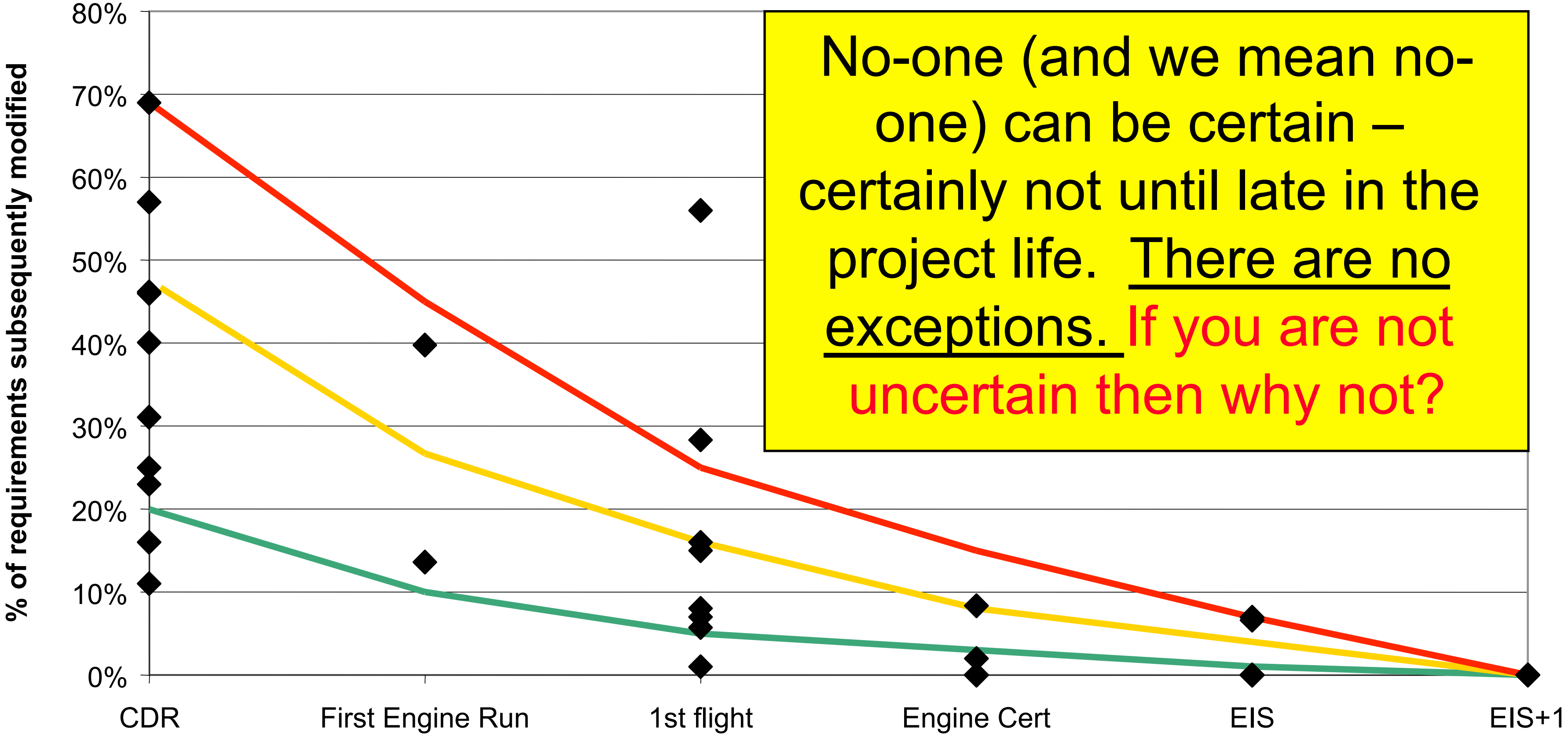


Scrap Rate and Iterations to Maturity



Historic Volatility

Requirements Uncertainty At Key Project Phases



No-one (and we mean no-one) can be certain – certainly not until late in the project life. <u>There are no exceptions.</u> If you are not uncertain then why not?

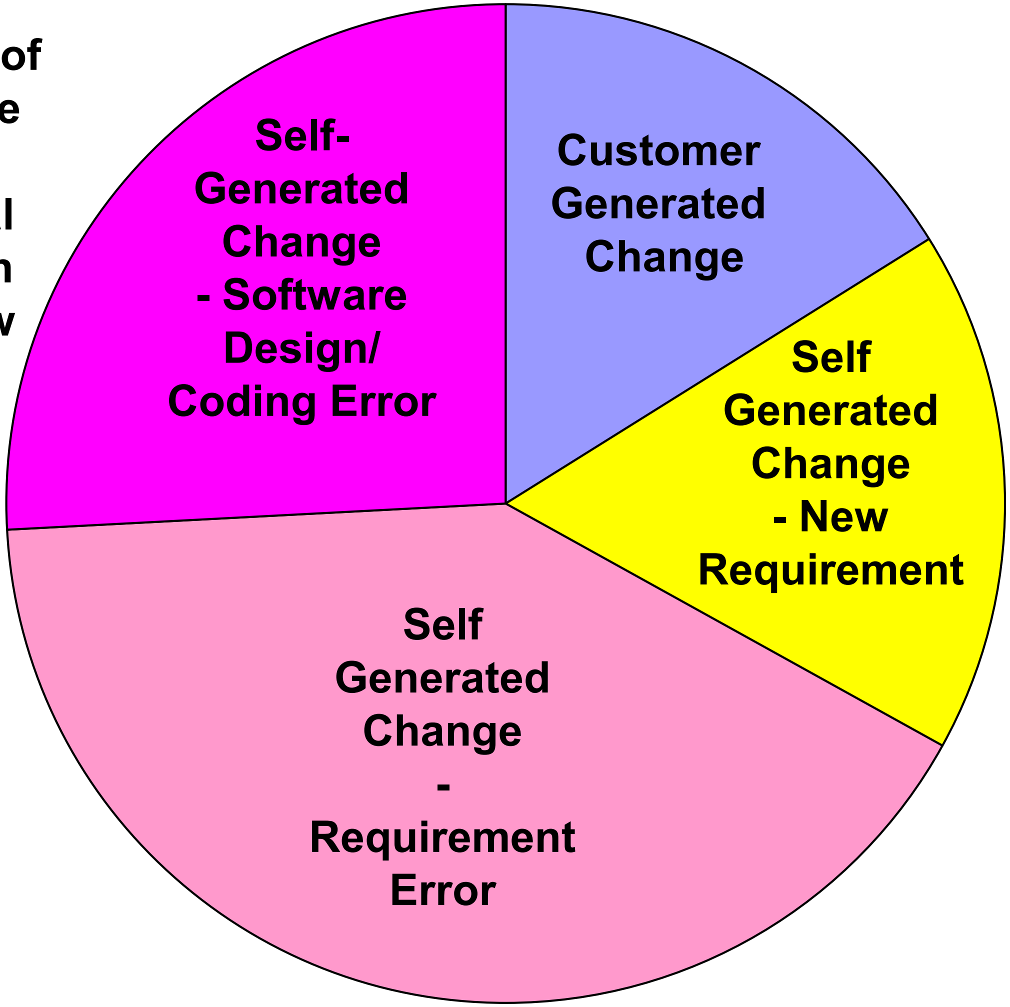
CDR = Critical Design Review

EIS = Entry into Service

EIS + 1 = Entry into Service + 1 Year

Most Uncertainty is self generated

Source of Change Post Critical Design Review



Where is the Uncertainty?

	Knowns	Unknowns
Known	Known-Knowns (28% of uncertainty arises here) *We failed on implementation*	Known-Unknowns … *risk*
Unknown	Unknown-Knowns … *We knew but forgot*	Unknown-Unknowns … ty … *Surprises*

Risk Management to move from Known-Unknowns to Known-Knowns

Risk Identification Techniques to move from Unknown – X to Known - X

Only a small % of uncertainty is a surprise

Cost of Late Detection - Example 1

Software Problem Report Analysis / Should have been found during: --> / Found during:	Matlab Animating	Reviewing	Application S/W Building	Low Level Testing	S/W Verification Testing	HSI Testing	System Verification Testing	Hardware Rig Testing	Engine Testing	Airframe Testing	Flight Testing	In Service	Key:	Cost Weight	Cost if found at right stage	Actual cost
Matlab Animating	0.5%												>= 8%	1	0.032	0.005
Reviewing	1.3%	55%											4% to 8%	1	0.798	0.566
Application S/W Building		0.7%	1.4%										2% to 4%	1	0.014	0.021
Low Level Testing	0.2%	2.6%		0.8%									1% to 2%	1	0.012	0.035
S/W Verification Testing		0.8%			0.4%								< 1%	5	0.031	0.060
H/W - S/W Integration Testing		1.0%				0.5%								5	0.080	0.077
System Verification Testing	0.9%	9.9%		0.4%	0.2%	0.8%	5.0%							25	1.592	4.301
Hardware Rig Testing	0.0%	1.3%					0.1%	0.4%						50	0.376	0.907
Engine Testing	0.1%	1.6%		0.0%		0.2%	0.4%	0.2%	1.6%					50	0.885	2.057
Airframe Testing	0.0%	3.8%				0.1%	0.6%			1.2%				50	0.796	2.875
Flight Testing	0.0%	2.3%		0.0%			0.3%	0.1%	0.1%	0.4%	1.5%			50	0.774	2.433
In Service		0.5%					0.0%	0.0%			0.0%	0.1%		200	0.177	1.415
Total Escapes	2.7%	25%	0.0%	0.4%	0.2%	1.1%	1.4%	0.4%	0.1%	0.4%	0.0%		31.2%	**Total:**	5.567	14.752
Total	3.2%	80%	1.4%	1.2%	0.6%	1.6%	6.4%	0.8%	1.8%	1.6%	1.5%	0.1%	100.0%	**Cost Ratio:**		**265%**

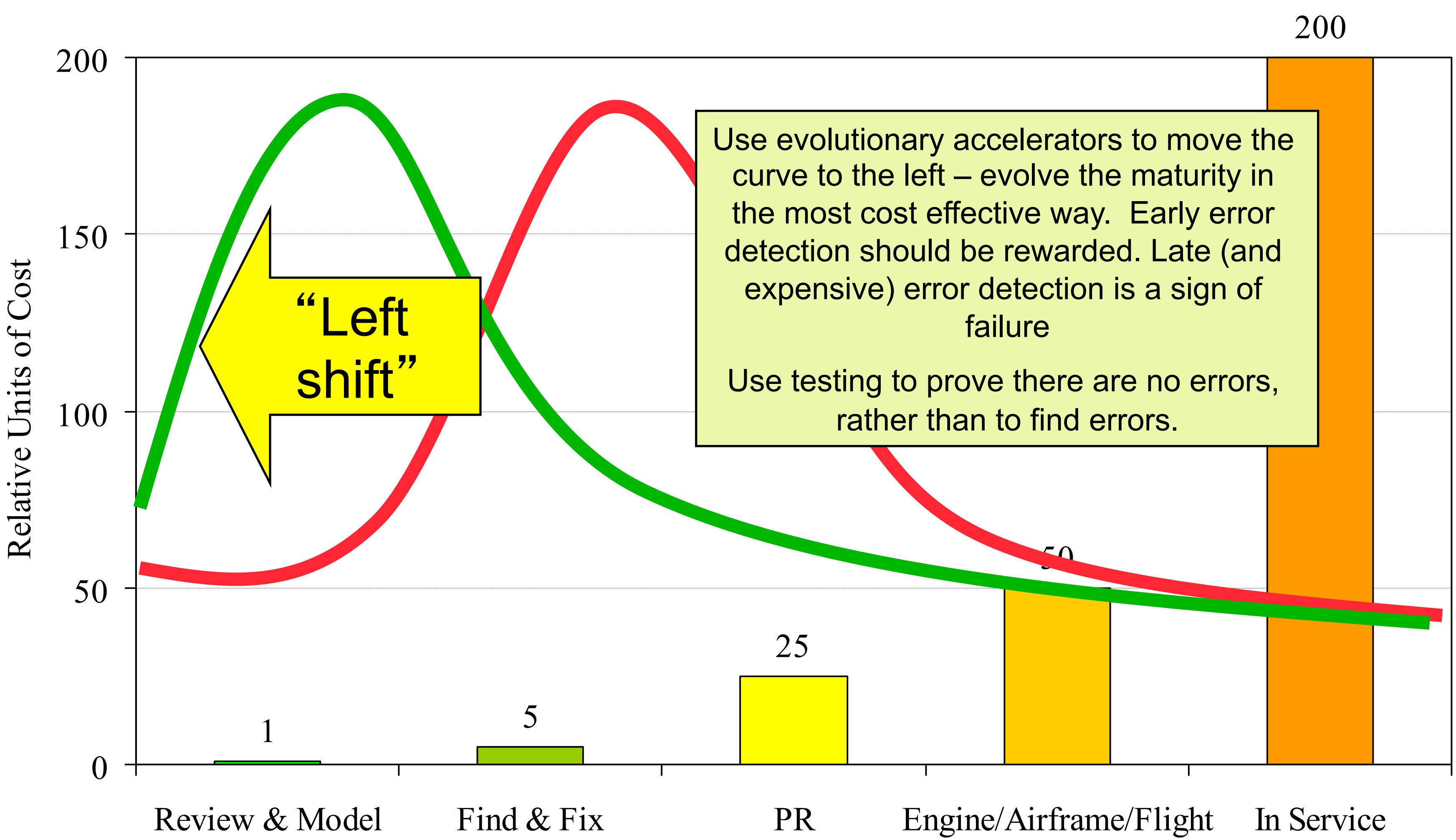
Cost of Late Detection - Example 2

Software Problem Report Analysis

Found during: / Should have been found during: -->	Requirements Validatior	Requirements review	Design Review	Code Review	Segment test	Software verification	System verification	Bench/Test Rig	Engine d'vt test	Engine cert test	Flight test	Flight in service	Key:	Cost Weight	Cost if found at right stage	Actual cost
Requirements Validation	7.2%												>= 8%	1	0.171	0.072
Requirements Review	6.2%	22%											4% to 8%	1	0.439	0.285
Design Review	1.6%	5.7%	4.3%										2% to 4%	1	0.171	0.116
Code Review	0.5%	3.8%	1.9%	5.7%									1% to 2%	1	0.115	0.119
Segment test		0.0%	0.1%	0.4%	0.2%								<1%	5	0.009	0.039
Software Verification		2.5%	4.2%	3.8%		1.5%								25	0.701	3.000
System verification	0.8%	7.0%	1.1%	0.2%		0.9%	2.0%							25	0.644	3.034
Bench/Test Rig	0.0%	0.5%	2.5%	1.3%			0.0%	0.3%						50	0.276	2.368
Engine d'vt test		0.1%	0.4%					0.1%	0.2%					50	0.207	0.414
Engine cert test	0.5%	0.4%	0.4%			0.1%	0.1%		0.1%	0.0%				50	0.092	0.828
Flight Test	0.1%	1.2%	1.1%	0.1%		0.3%	0.3%	0.0%	0.1%		0.4%			50	0.529	1.862
Flight in Service	0.2%	0.3%	1.0%				0.0%	0.0%		0.2%	0.7%	2.2%		200	4.322	9.195
Total Escapes	10%	22%	13%	5.9%	0.0%	1.3%	0.6%	0.2%	0.2%	0.2%	1.1%		54%	Total:	7.676	21.331
Total	17%	44%	17%	12%	0.2%	2.8%	2.6%	0.6%	0.4%	0.2%	1.1%	2.2%	100%	Cost Ratio:		278%

Accelerating Evolution

Cost of Correcting Errors

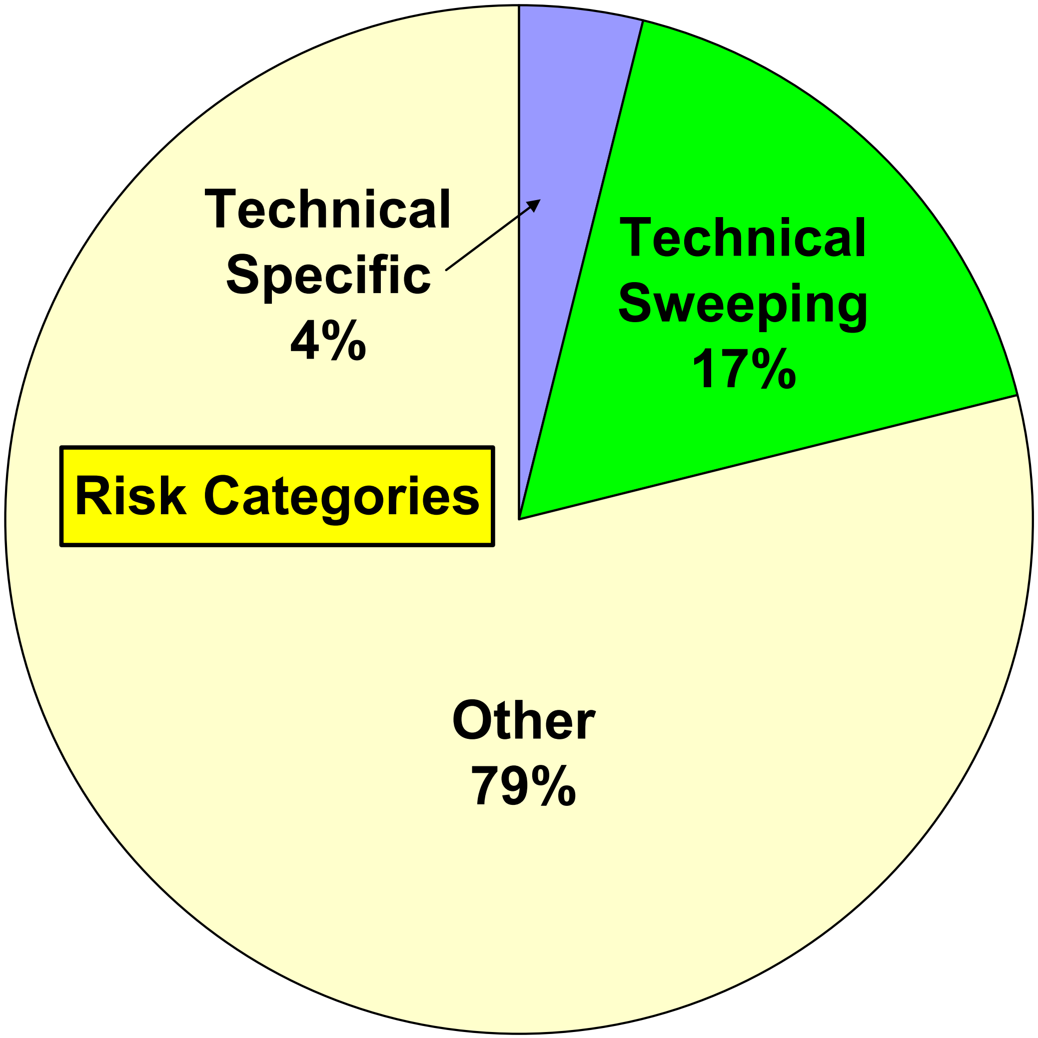


Certainty, Risk and Gambling

Behavior	Characteristics	Outcome	Mitigation
Unwarranted Certainty	"Can do" culture. Better to be certain and wrong than uncertain and right	Late change and rework	Change the emphasis at design gate reviews - the project must show rationale for certainty and a plan to manage residual uncertainty
Gambling	"Tick in the box" ... Identified - nothing done with the results		Change the emphasis ...reviews - ...t show ...ge ...and demonstrate that the plan is being executed
Technical Risk Management	Technical Risks identified and managed	Reduced rework Earlier product maturity	See later

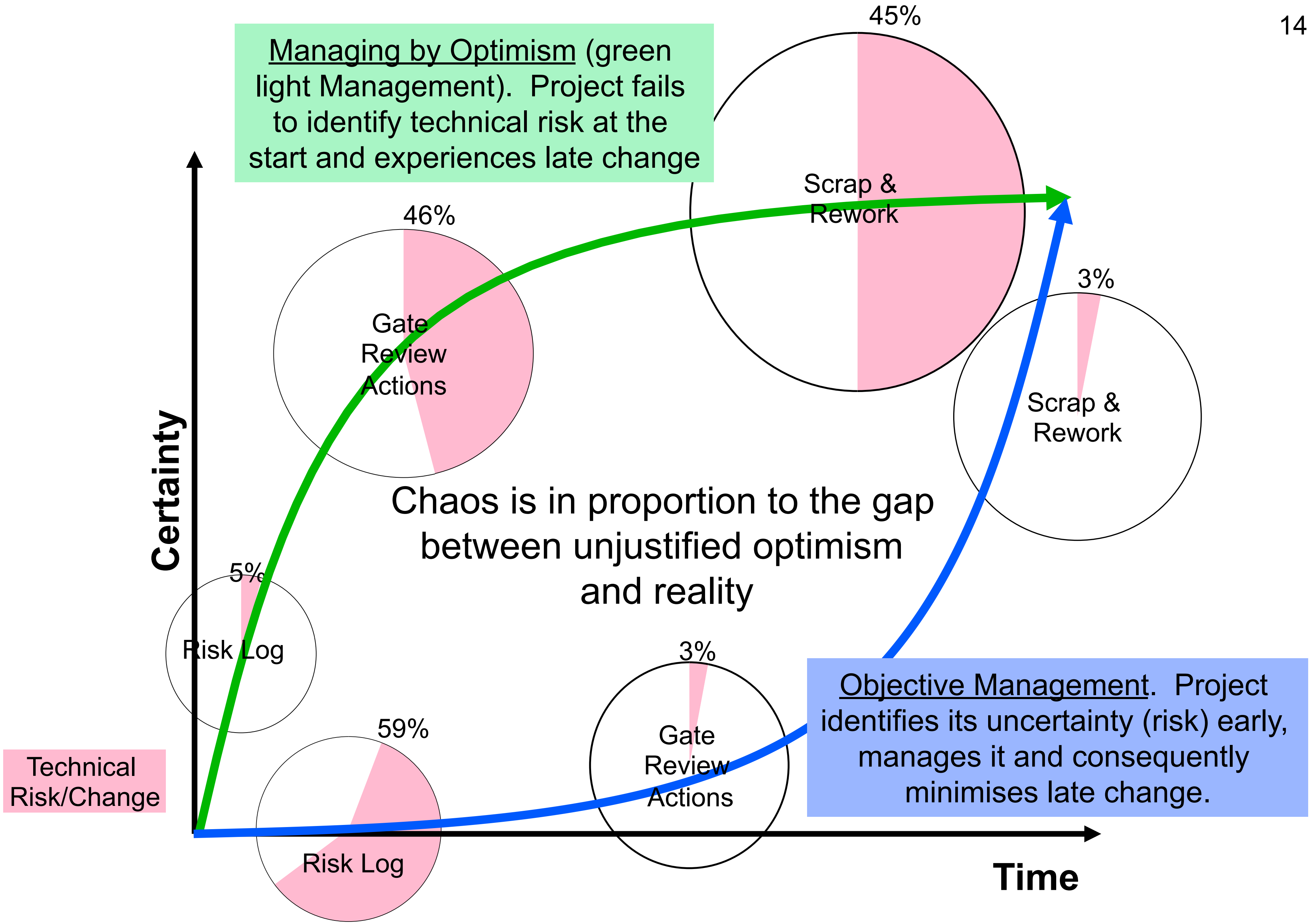
In general Scrap & Rework is the manifestation of un-mitigated risk

Risk Categories

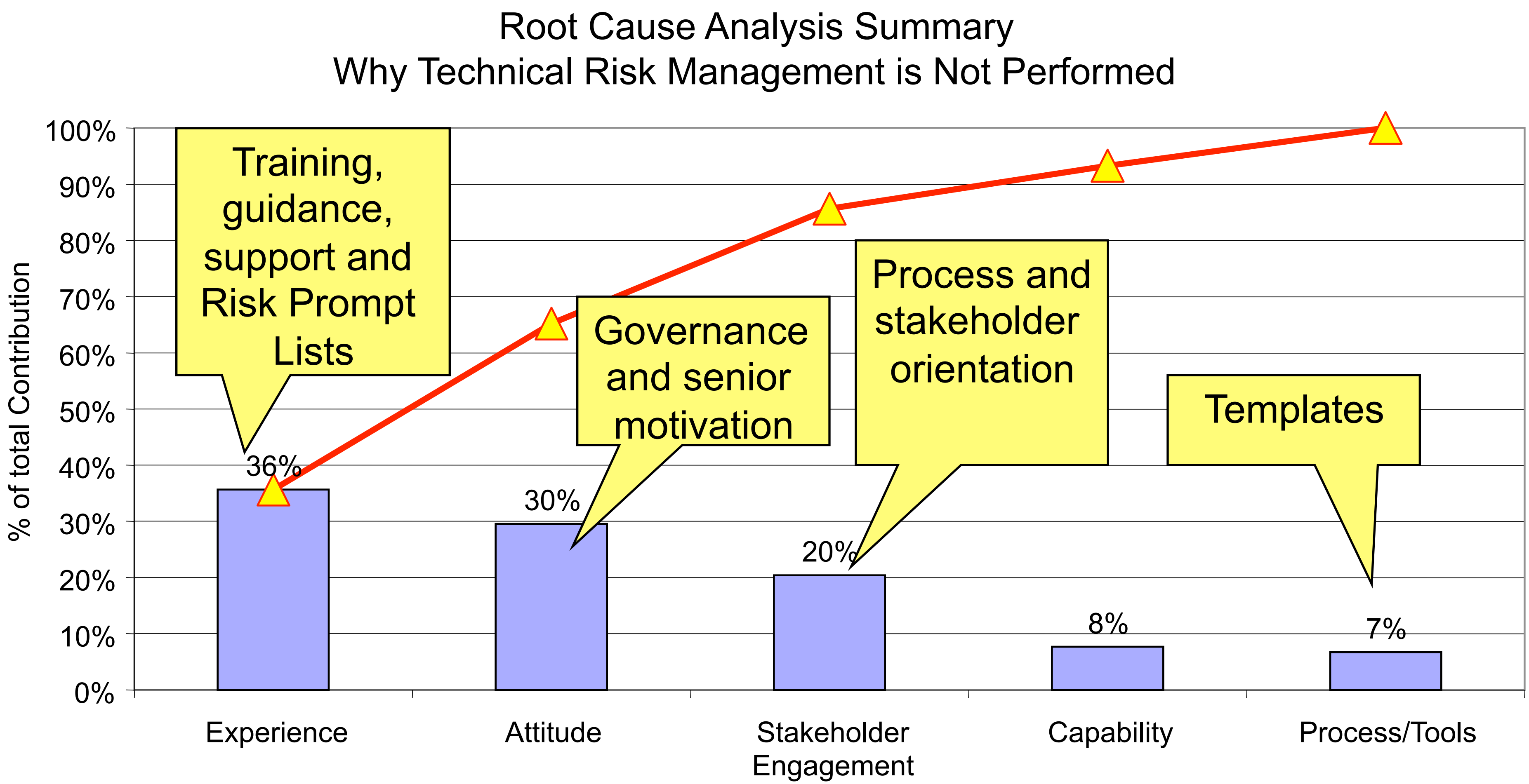


Differences Between Project and Technical Risk Management

Aspect	Traditional Project Risk Management	Technical Risk Management
Purpose	Focus is on risk (uncertainty) in the project	Focus is on risk (uncertainty) in the product
Attendees	Tends to be project leaders, managers and team leaders	Technical Leads, team members and appropriate technical experts
Measures	Risk Performance measures – are we managing the risk	Technical Maturity measures – are we reducing Scrap/Rework.
Dominant skill	Project Management & Risk Management	Technical & domain experience
Tools	Standard risk management tools and templates	Addition of product related attributes and associated risks
Granularity	Will tend to be larger risks	Will tend to look at larger number of smaller risks


Managing by Optimism (green light Management). Project fails to identify technical risk at the start and experiences late change
45%
Scrap & Rework
46%
Gate Review Actions
3%
Scrap & Rework
Certainty
Chaos is in proportion to the gap between unjustified optimism and reality
5%
Risk Log
3%
Gate Review Actions
59%
Risk Log
Technical Risk/Change
Objective Management. Project identifies its uncertainty (risk) early, manages it and consequently minimises late change.
Time

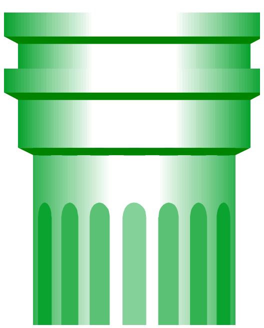
Root Cause for not performing TRM



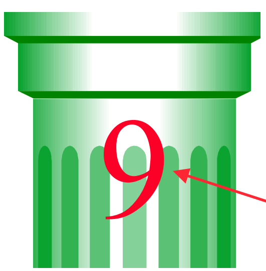
Technical Risk Maturity Levels

25 requirements based on CMMI, the Major Project Association and RR Risk Maturity model

Level 0
kids stuff
Do nothing. The project is open loop with regard to technical risks. Without evidence the project must assume it will be at level 0.



Level 1
Minimum
Do something even if it’s not planned, documented or formalised. Relies on good managers to make it happen

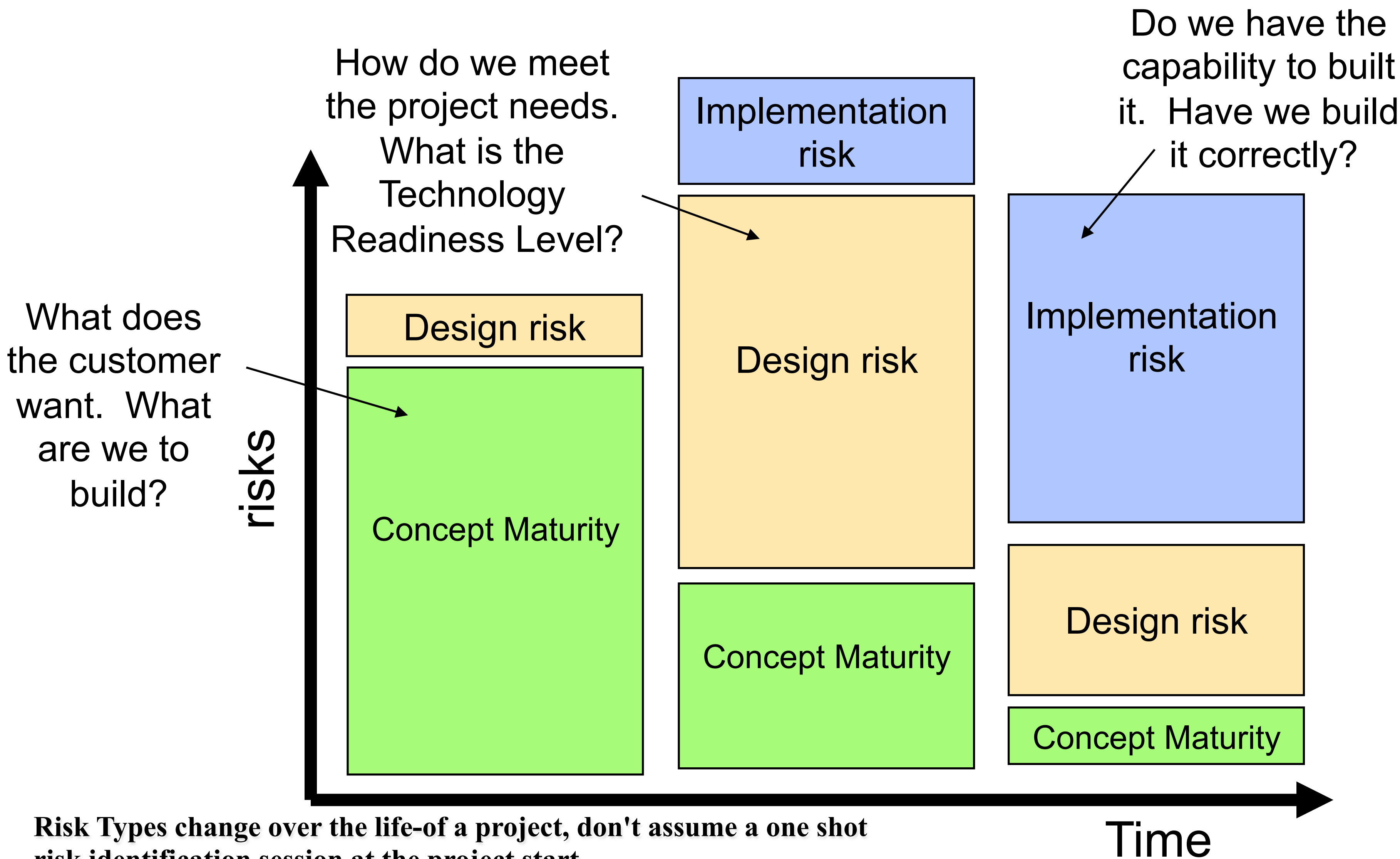


Level 2
Pragmatic
Define, plan and govern the Technical Risk Management activities – it’s not enough to do Technical Risk Management, we need to also do it in the right way.

Level 3
Ideal
Seeking high performance through the use of measurement, specialists involvement, stakeholder involvement

Number of requirements

Risk Types and Project Lifecycle



Risk Types change over the life-of a project, don't assume a one shot risk identification session at the project start

Common Risk (and Opportunity) Classes

- **Concept**
  - Airframe Maturity
  - Engine Maturity
  - Concept Maturity
  - Technology Readiness
- **Novelty & Complexity**
  - Novelty
  - Complexity
  - Number of Interfaces
  - Novel process/tools
  - New unknown supplier
  - New document structure
- **Requirements**
  - Requirements quality
  - Requirements volatility
  - Historically volatile requirements
- **Robustness to change**
  - Product robustness
  - Product configurability
  - Reuse Assumptions
  - Product Environment

- **Capability**
  - Customer Capability
  - Team Capability
  - Supplier Capability
- **Stakeholder Engagement**
  - Customer Buy Off
  - Supplier Buy off
- **Industry & Business Trends**
  - Certification changes
  - Industry changes
  - Business changes
- **Project**
  - Location of team & Stakeholders
  - Schedule stability
  - Scope stability
  - Budget to support risk management
  - Resource at the right time

Common Mitigation Classes

- **Architecture Trade Study**
  - IPT - Controls
  - IPT -- Controls & Stakeholders
  - Concept proposal review
- **Review**
  - Friendly review
  - Independent review
  - Review by Domain Expert
- **Early proof of concept**
  - Prototype - stand alone
  - Prototype in existing control system
  - Modelling - Control System
  - Modelling - Control System + Engine
  - Modelling - Control System + Airframe
- **Find & Fix**
  - Airframe Test Rig or Aircraft
  - Engine Test Rig Exposure
  - Integration Test Exposure (HSI, ES37)

Risk Mitigation

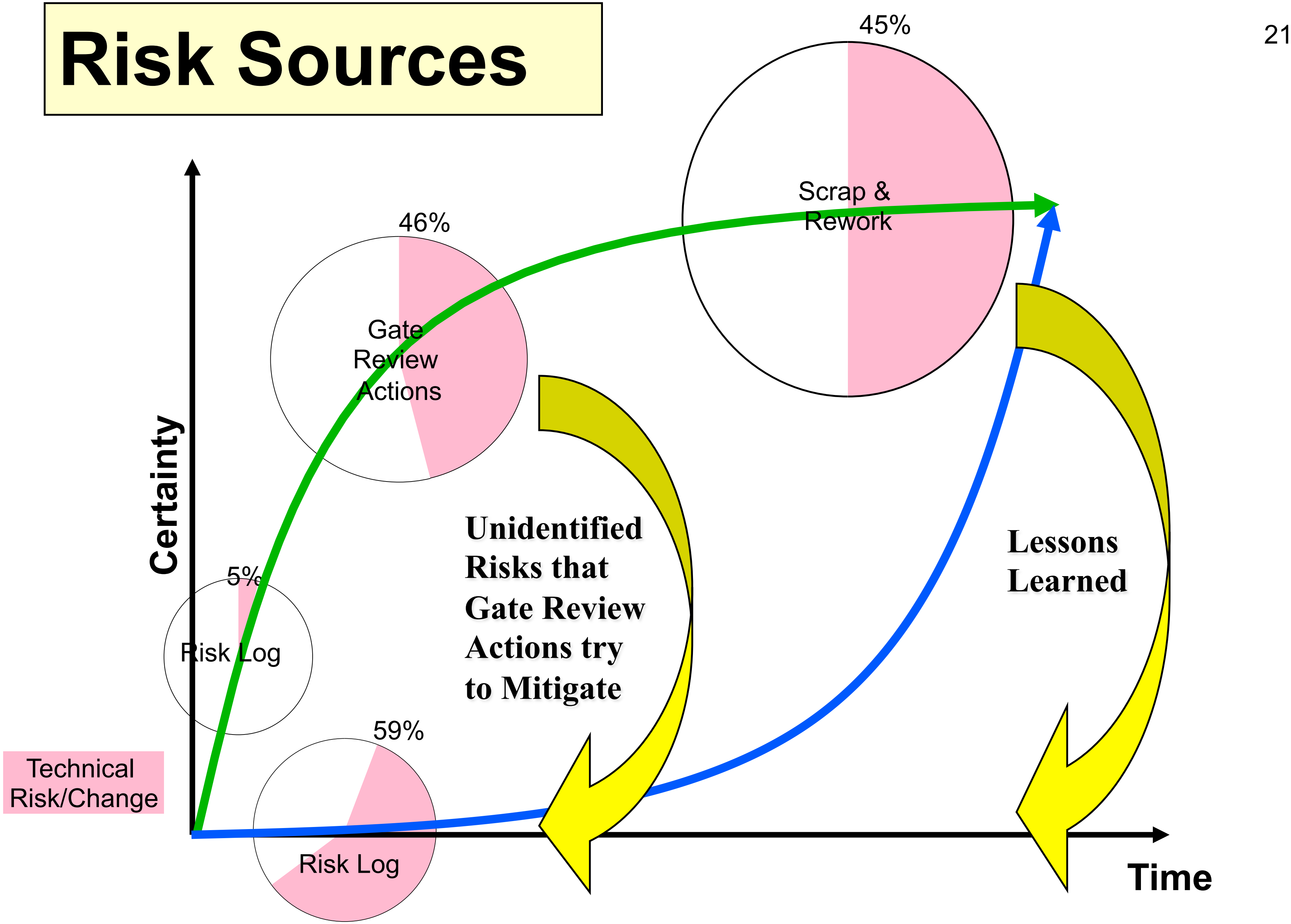
- **DFX - Design for volatility**
  - Robust Design
  - Configurable design
  - Plug & Play architecture
  - Auto code generation
- **Design Guidance**
  - Design Guide
  - Lessons Learnt
  - Learn from historic projects
  - RIPL
- **Stakeholder engagement**
  - On site stakeholder representation
  - Visibility of stakeholder risks
  - Joint risk management sessions
  - Stakeholder reviews
- **Plan for volatility**
  - Delay the Function
  - Plan for design iteration
  - Delay freeze of design/requirements
  - If all else fails, plan in contingency

Target mitigations around the risk class

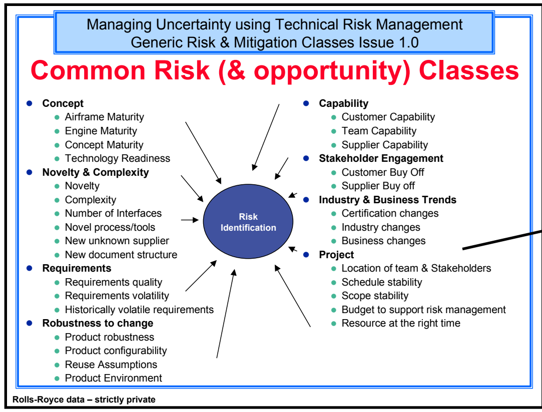
Risk Class	Mitigation
Engine/Airframe Maturing	Delay until mature or develop configurable functions or form an IPT
Implementation risk	Reviews, Verification & Validation
Complex function	Prototype or use Find & Fix
Novel function	Establish IPT or seek precedence from other areas.
Lack of experience	Use design guides, Lessons Learnt or hold a review with experts outside of the team

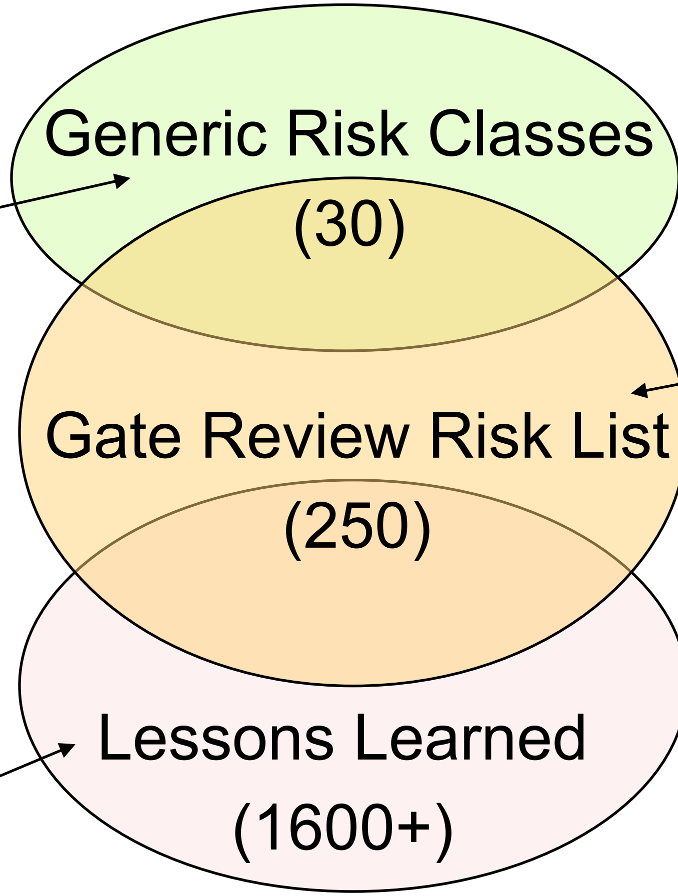
The more precisely you can define a risk, the more precisely you can target a viable mitigation

Risk Sources



Hierarchy of Risks - RISC



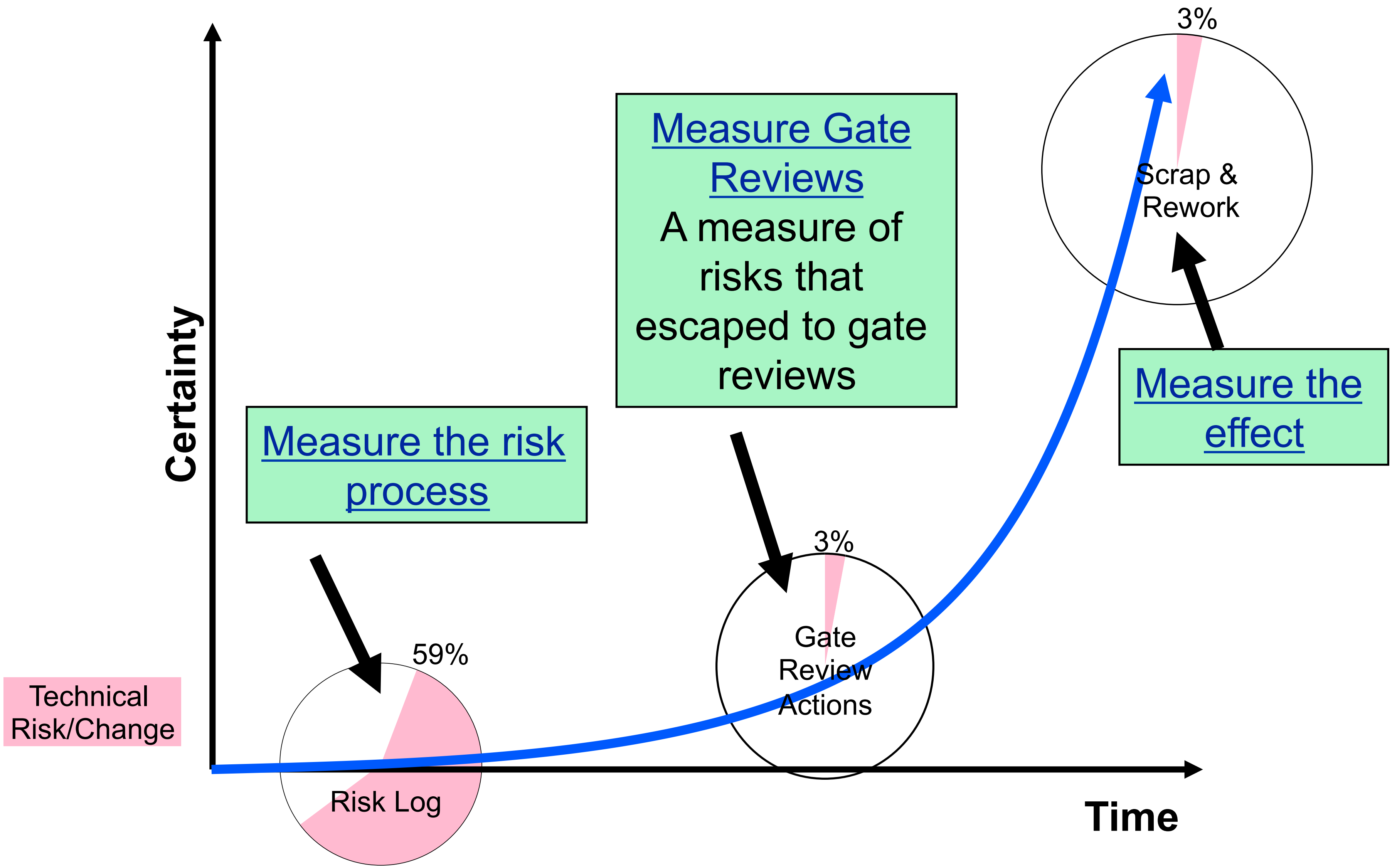


Return to Introduction | Selected Category: Sensors

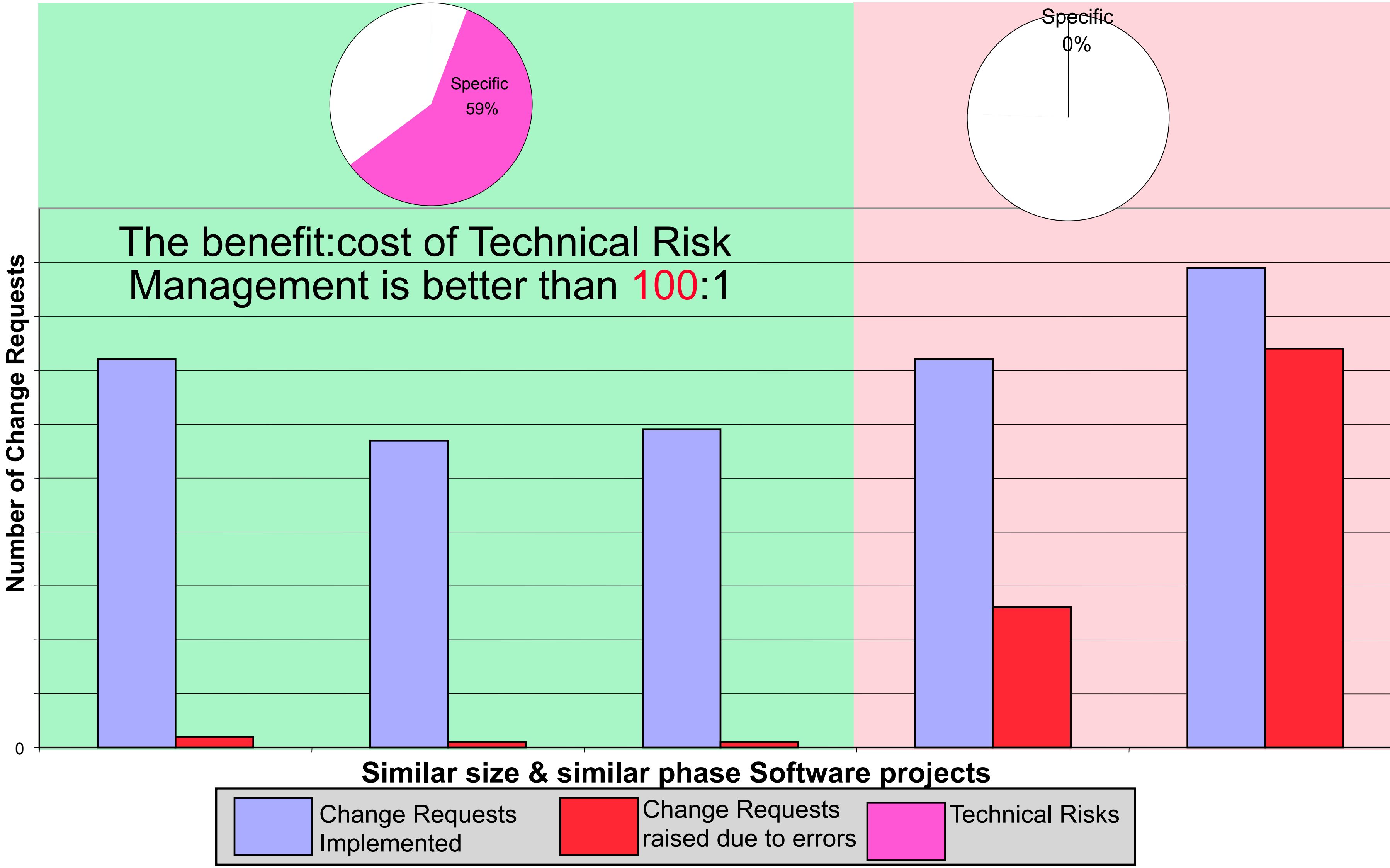
#	Risk/Issue	Comments/Mitigation
619	Are thermocouples with Mineral Insulated (MI) cable being used?	Low readings associated with oxidation of KP wires. Investigation showed that preferential oxidation can occur in MI cables that have thermocouple materials as conductors and Silicon Dioxide as the MI insulator. Note - Copper conductors are not affected by this corrosion problem. Consider a change in insulator material - for instance, Magnesium Oxide
639	Has radiated heat been considered in the design of a thermocouple?	An end cap was fitted which shielded the thermocouple from the combustor whilst still allowing a gas flow past the thermocouple.
644	Have pressure switch settings been validated using early flight test pressure data?	The LP pressure feedback switch setting was higher than required and resulted in inappropriate cockpit cautionary messages during engine idle and anti-ice system activated on. Ensure that the anti-ice low pressure switch point is captured in the system ICD and validated in the flight test program.
645	Are any welds specified in the design of sufficient strength to meet structural loading requirements consistently without failure?	Pressure switches failed at partial penetration edge welds during 30 hours/plane endurance testing. Changing to an inherently stronger full penetration butt weld allowed the 30 hours/plane vibration requirement to be met. Ensure that the configuration of welds and their load profiles have been considered before CDR.
656	Is a part potentially susceptible to high frequency vibration failure of internal components?	HCU failures during vibration testing. If you have a small sealed container with internal components that are resonating, consider use of damping fluid such as 200cSt Dimethyl Silicone. Damping fluid is a known solution to this problem, at the cost of a small increase in weight.
657	Are interfaces defined purely around a convenient physical boundary, or are functional boundaries also considered?	Different teams working on either side of the interface will struggle if the interface is in an area of conflicting design freedom. Taking into account the function of the design and allocating these functions completely to one or the other side of the interface results in faster resolution of interface issues.

Risk Identification Source Checklist

Measuring Success



Technical Risk Management really works



Conclusions

- If no effort is made to control scrap and rework on a project, scrap rates of 50% can typically occur, leading to the program costing twice as much as it could have and requiring significantly more time to achieve a mature product.
- Contrary to expectations, changes in customer requirements are not a major driver of scrap and rework - most is internally generated by the development team.
- Systems Engineering and Technical Risk Management are critical in understanding and controlling the sources of scrap and rework
- Past experience (Lessons Learned, Technical Review Gate Actions) can provide a useful feedback mechanism to understand the technical risks that a new project may be facing
- Metrics are available to assess Technical Risk Management capability and effectiveness on a project
- Scrap and rework rates of less than 10% can be achieved, with benefit to cost ratios of better than 100:1