THE IRISH SOFTWARE
ENGINEERING RESEARCH CENTRE

Software Risk Management in Medical Device Systems

John Burton

ICSP, May 2008

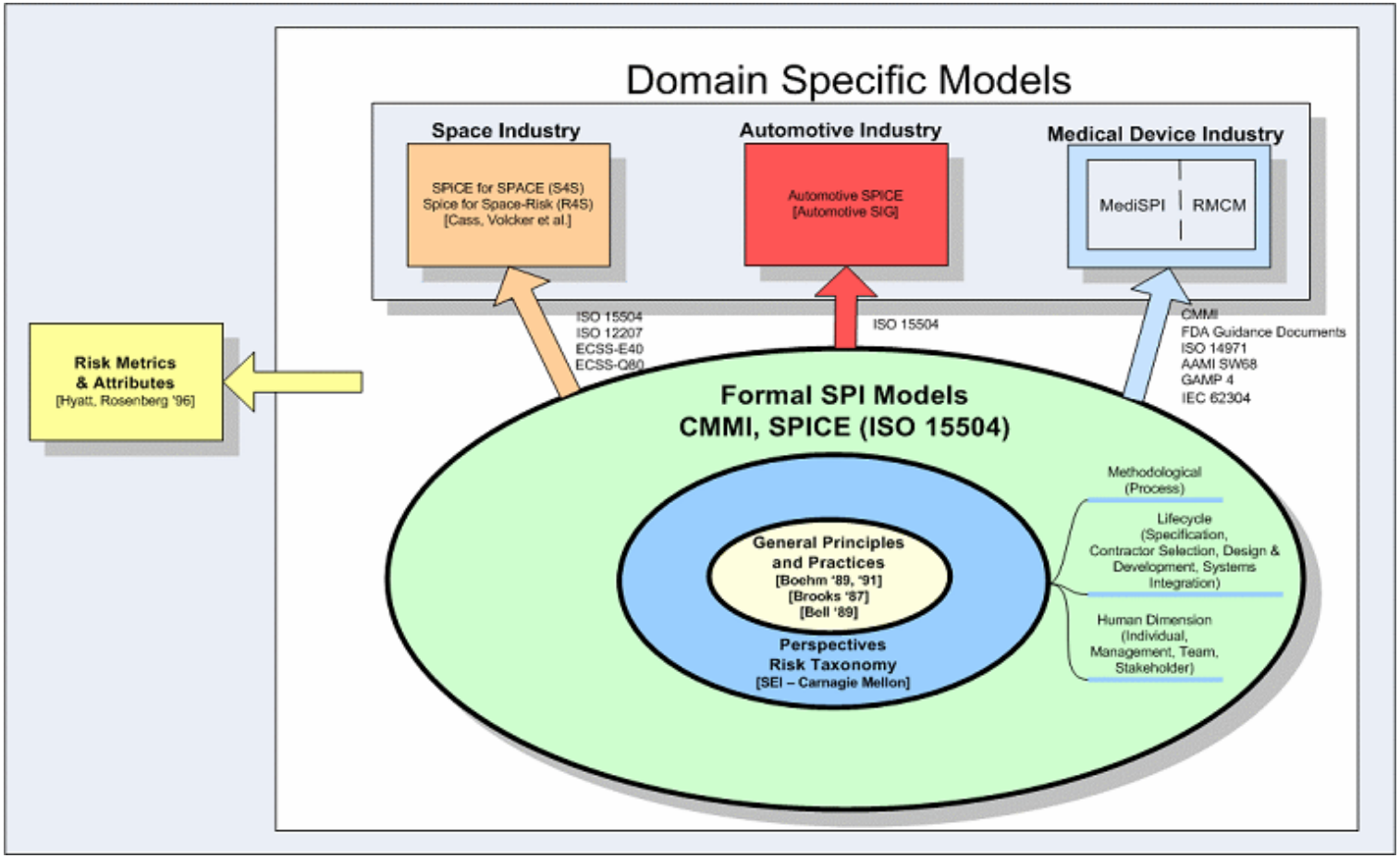
Overview

- Research Question & Objectives
- Positioning the Research
- Research Method
- The RMCM
- Evaluation of the RMCM
- Contributions of Research

Research Question and Objectives

- Research Question
  - Can the development of a new SPI Risk Management Capability Model (RMCM) assist medical device companies in improving their software risk management practices and put them on the path to regulatory compliance?
- Research Objectives
  - Develop a Risk Management Capability Model (RMCM)
  - Evaluate the Model

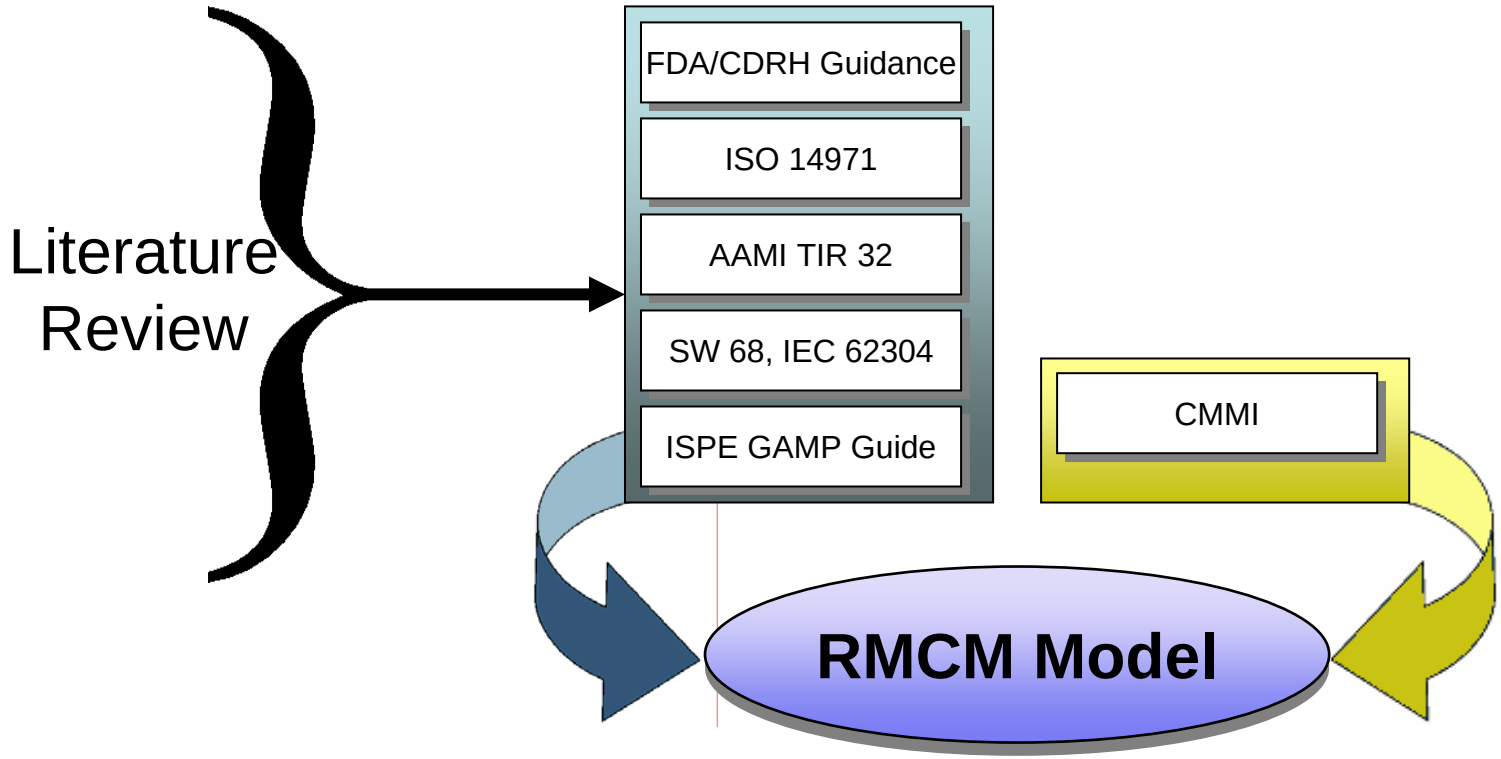
Overview of Software Risk Management Evolution



Researcher's perspective of Risk Management by Industry Sector based on Literature Review

Industry Domain	Focus of Risk Management			Drivers of Risk Management
	Schedule	Budget	Safety	
General	Primary	Primary	Secondary	Industry
Defence	Primary	Primary	Secondary	Department of Defence
Space	Spread Evenly			Industry and regulators
Automobile	Spread Evenly			Industry
Medical	Secondary	Secondary	Primary	Regulators

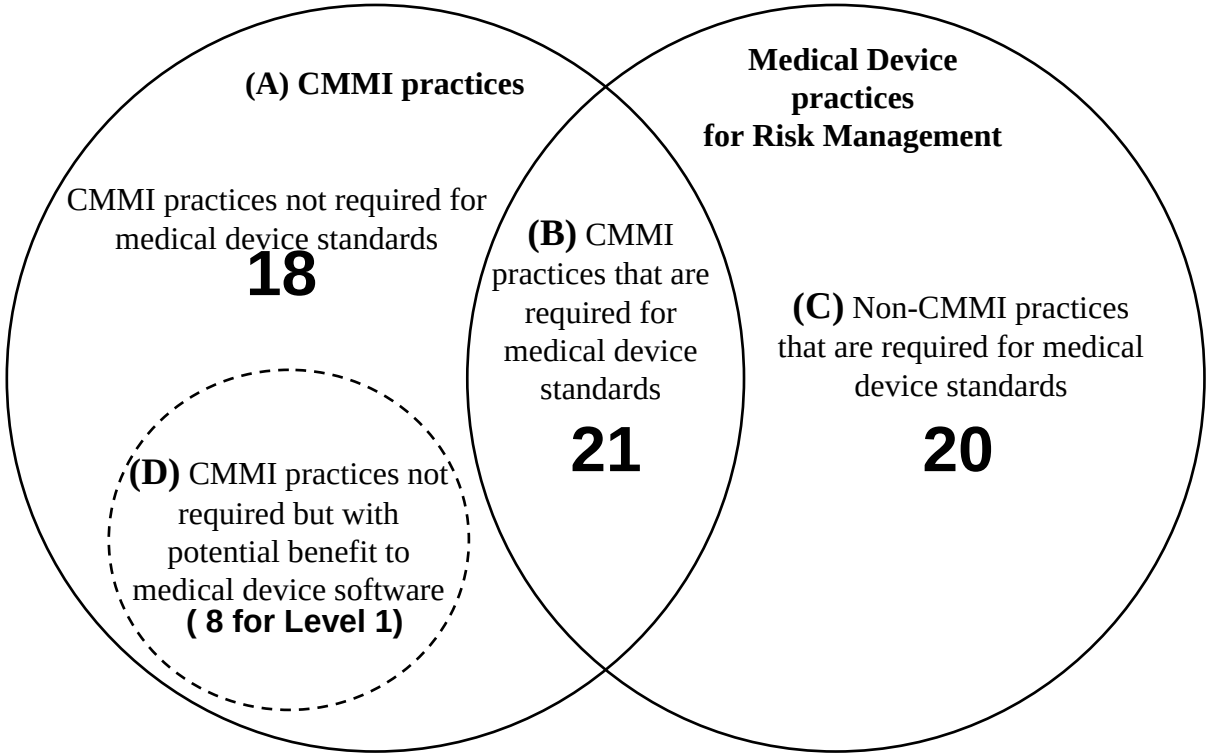
Development of the RMCM



Poposed Benefits of a Medical Device Specific RMCM

- Bring the disparate knowledge on Software Risk Management for Medical Devices together into one place
- Provide a method to quickly assess and improve Software Risk Management (RM) capability
- Incorporates both regulatory requirements and proven SPI RM practices
  - Promote SPI practices into medical device software
- "Offers the opportunity to get it right first time" – (Feedback on the RMCM from a Medical Device Company who is not directly involved in the research)

RMCM Summary



A- CMMI® Practices that are not mandatory for Medical Device standards.
B- CMMI® Practices that are required for Medical Device standards.
C- Non-CMMI® Practices that are required for Medical Device standards.
D- CMMI® Practices that are not mandatory for Medical Device standards – but if performed could contribute to the safety of the Medical Device software or enhance the company's RM practice

RMCM Summary

Goal: GG1: Perform the Specific Practices				
GP 1.1 Perform Base Practices				
Specific Goal	**CMMI® based sub-practices**	**CMMI® sub-practices to meet MD regulations**	**Additional sub-practices to meet MD regulations**	**Level 1**
SG 1: Preparing for RM	6	6	10	0
SG 2: Identifying and Analysing Risks	9	4	4	5
SG 3: Mitigate Risks	8	5	6	3
Specific Goal Totals	**23**	**15**	**20**	**8**
Goal: GG2: Institutionalise a Managed Process				**Level 2**
	10	6	0	4
Goal: GG3: Institutionalise a Defined Process				**Level 3**
	2	0	0	2
Goal: GG4: Institutionalise a Quantitatively Managed Process				**Level 4**
	2	0	0	2
Goal: GG5: Institutionalise an Optimising Process				**Level 5**
	2	0	0	2
Totals	**39**	**21**	**20**	
RMCM Level Med Sub-practices		**41**		
RMCM Sub-practices	**59**			

GAP Analysis at Client's site using the RMCM

Goal	Practices to satisfy MD regulations	Practices satisfied by Client
SG 1: Prepare for RM	16	3
SG 2: Identify and Analyse Risks	8	3
SG 3: Mitigate Risks	11	3
GG2: Institutionalise a Managed Process	6	6
GG3: Institutionalise a Defined Process	0	0
GG4: Institutionalise a Quantitatively Managed Process	0	0
GG5: Institutionalise an Optimising Process	0	0
Total	**41**	**15**

Implementation of RMCM Practices at Client Site

- Update made to client's software risk management process
  - Re-review of updated process against the RMCM
  - Updated process released into client's Quality Management System (Controlled Environment)
- RMCM Implemented in the R&D department of a Medical Device company.
  - Embedded and Desktop application software

Evaluation of the RMCM

- Evaluation methods:
  - Documentation Analysis
  - Case Dynamics Matrices
  - Interviews
  - Content Analysis using Coding (Open and Axial)
- Evaluation Findings
  - Clients Software RM Strategy:
    - More robust - Incorporates previous missing RM practices
    - More consistent - Constant criteria used in the evaluation of severity and likelihood and overall classifications
    - More up to date/in line with the latest standards

Evaluation of the RMCM

- Evaluation Findings Continued
  - Lifecycle Phases for RM Strategy
    - Although the client's RM strategy identifies the Lifecycle Phases to which the strategy applies (sub practice 10) the risks had not been monitored throughout the lifecycle (sub practice 39)
    - This finding was also supported by interview findings
  - Training
    - The requirement to provide adequate training (RMCM Sub Practice 25) was not adequately satisfied by the client
      - Client's updated Software RM procedures identified the requirement to provide adequate training
      - Documentation Analysis and training records suggested adequate training had been carried out at client site
      - Interviews contradicted this finding – Self Training was used

Evaluation of the RMCM

- Evaluation Findings Continued
  - Prioritisation of Risks
    - Requirement to prioritise risks (RMCM sub practice 28) has had little impact, because all risks classified as unacceptable were seen equal in terms of priority by the client
    - Reason – No software could be released with unacceptable risks (irrespective of the formal priority assigned to the risks)
  - Addition of Risk Control Measures to the Software Requirements Specification Document
    - Client was following this sub practice (RMCM practice 35)
    - However…Client's procedure for software risk management did not explicitly drive compliance with this practice
    - Sub-practice 23 to provide traceability from the risks and associated mitigations to the impacted software requirement(s) drove compliance

Evaluation of the RMCM

- Evaluation Findings Continued
  - Safety Pre-Production
    - Introduce User Trials as formal practices to the RMCM
  - Safety Post-Production
    - Must be explicit in procedures about the requirement to continue to perform software RM post-production
  - Requirements Changes
    - Changes tested by QA after implementation and then updated the Software Risk Management Document
    - No traceability provision from changes through to RM and verification of the change and any RM mitigations
    - Operating Procedure for performing changes required updating to refer back to procedure for software RM as part of the change process

Contributions of Research

- The benefits of a medical device specific software risk management capability model identified
  - Strengthening of medical device risk management through adoption of formal SPI model practices
  - Identification of weaknesses in CMMI risk management practices with respect to medical device regulations
- RMCM developed and validated
  - Brings the disparate medical device practices together
  - Provides a path for CMMI certified companies to achieve medical device compliance in risk management
  - Identifies practices that medical device companies must adopt to satisfy risk management in the CMMI model
- Knowledge contributions to the client, the medical device industry and to the software engineering community

Related Publications

- Burton J., McCaffery F. and Richardson I. (2006), A Risk Management Capability Model for Use in Medical Device Companies, 28th International Conference on Software Engineering, ICSE 2006.
- Burton J., McCaffery F. and Richardson I. (2008), Improving Software Risk Management Practices in a Medical Device Company, (Accepted for publication, ICSP, May 2008).
- McCaffery, F., Burton, J., Richardson, I. (2008). Development and Evaluation of a Risk Management Capability Model (RMCM) for the Medical Device Industry, (Accepted for publication in SPICE 2008, May 26th to 28th, Nuremberg, Germany)

THE IRISH SOFTWARE
ENGINEERING RESEARCH CENTRE

Thank You