

Webinar: Agile Design Controls Part 2

Dynamic Risk Management for Software-Intensive Medical Devices

March 2019

Arnaud Alberts

Matrix Requirements GmbH

Wolfgang Huber

Matrix Requirements GmbH

Aaron Joseph

Sunstone Pilot, Inc.

Aaron Joseph

Principal Consultant – Sunstone Pilot, Inc.



- 20+ years medical device development over a wide range of products:
 - surgical robotics systems, digital x-ray fluoroscopy system, drug inhaler devices, robotic catheter system, x-ray catheter for brachytherapy, laser eye surgery system, heart-lung bypass machine, and multiple wearable/IOT devices
- Assist clients with all aspects of design controls: risk management, requirements management, V&V testing, refining design controls procedures, and training R&D staff
- Avid promoter of lean and agile methods for medical device development
- BSEE - Rice University and MS Bioengineering - University of Washington
- Based in Silicon Valley

Arnaud Alberts

Growth Manager – Matrix Requirements GmbH



- Helping medical device companies to build their device in an agile way facilitating the management, the documentation and the certification of their product with Matrix Requirements applications.
- QA engineer and Product Management in a Startup Medical Device company
 - Hardware + software class 2 Medical Device
 - Building the QA system for market introduction
 - Validation, Risk assessment and testing
 - Product enhancement, releases, documentation
- M.Sc. Bio-Engineering – ULB Brussels
- Based in Brussels - Belgium

Wolfgang Huber

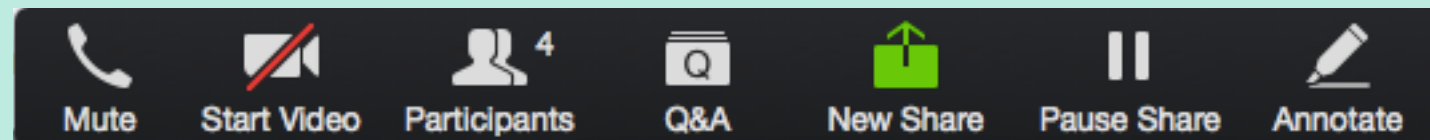
Co-Founder - Matrix Requirements GmbH



- Founder Matrix Requirements
- 15+ years managing medical device development
- 10+ years developing version control and document management systems
- 30 years experience professional software development
- Early adaptor of agile methodologies
- M.Sc. Computer Science – Karlsruhe University
- Based in Munich, Germany || Beziers, France

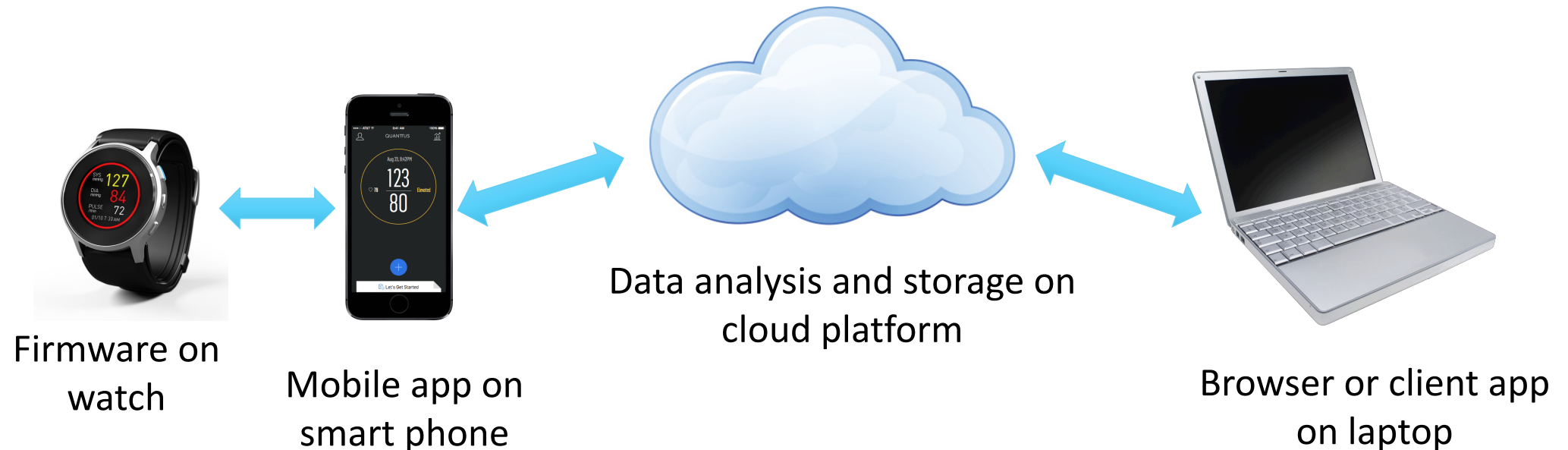
Webinar Outline

1. Requirements management
2. Basic model for risk analysis and risk controls
3. Example change scenario
4. Implementing changes with Jira and Matrix
5. Tool configurations for efficient risk and requirements mgmt
6. Q&A

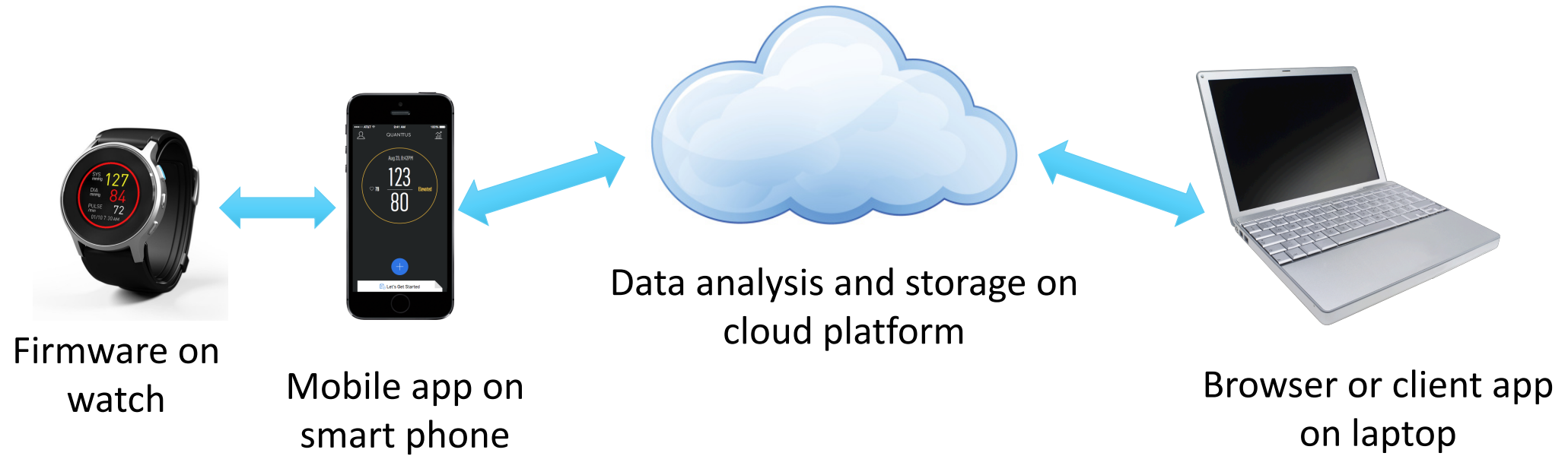


Example Connected Medical Device

- Wearable device + mobile app + cloud
- Heart monitor (including analysis of other patient data)
- Distributed architecture with multiple software platforms



Example Connected Medical Device



Change: late in development, the team discovers a problem during usability testing
→ necessitates changes to GUI on watch and smart phone and retesting

DHF documents



Example of Matrix screenshots: risk creation

The screenshot displays the Matrix Requirements application interface. On the left is a navigation tree with categories like TC (Test Cases), DO (Design and Unit Tests), SPEC (Specification), HW (Hardware), SOUP (Software Requirements), ITC (Integration Tests), and RISK (Risks). The RISK section is expanded to show 'Wrong Measurement' (RISK-13). The main area shows the details for this risk, including its hazard, sequence of events, hazardous situation, and harm. It also displays risk controls linked to requirements REQ-18 and REQ-19, and a risk matrix table.

RISK-13 Wrong Measurement

RISK

Hazard: Bad data collected and analyzed by phone

Probability of Occurrence: 4 - Often

Sequence of Events: User puts phone on table
User sits in chair next to table
User starts measurement

Hazardous Situation: Distance phone to watch too big, bad data connection

Probability of Harm: 2 - Probable

Harm: Watch shows normal ECG in abnormal case

Severity: 4 - Critical

RBM: $4 * 2 * 4 = 32$

RISK CONTROLS

- REQ-18 Data transfer shall have checksums reduces exposure to hazardous situation by 2
- REQ-19 App shall only show results if correct and complete data arrives reduces exposure to hazardous situation by 2

Create Software Requirements | Create Specification | Create System Requirements | Select Existing

Cannot be reduced any further

Benefits outweigh remaining risk

COMMENTS

JIRA

RAM	$1 * 2 * 4 = 8$
-----	-----------------

2.2.118.14276

Or we can focus on RISK without mitigation first

RISK-13 Wrong Measurement ↩ 👤 🕒 🗑️

RISK

Hazard:	Bad data collected and analyzed by phone	Probability of Occurrence:	4 - Often
Sequence of Events:	User puts phone on table User sits in chair next to table User starts measurement		
Hazardous Situation:	Distance phone to watch too big, bad data connection	Probability of Harm:	2 - Probable
Harm:	Watch shows normal ECG in abnormal case	Severity:	4 - Critical
		RBM	4 * 2 * 4 = 32

The mitigation

RISK CONTROLS

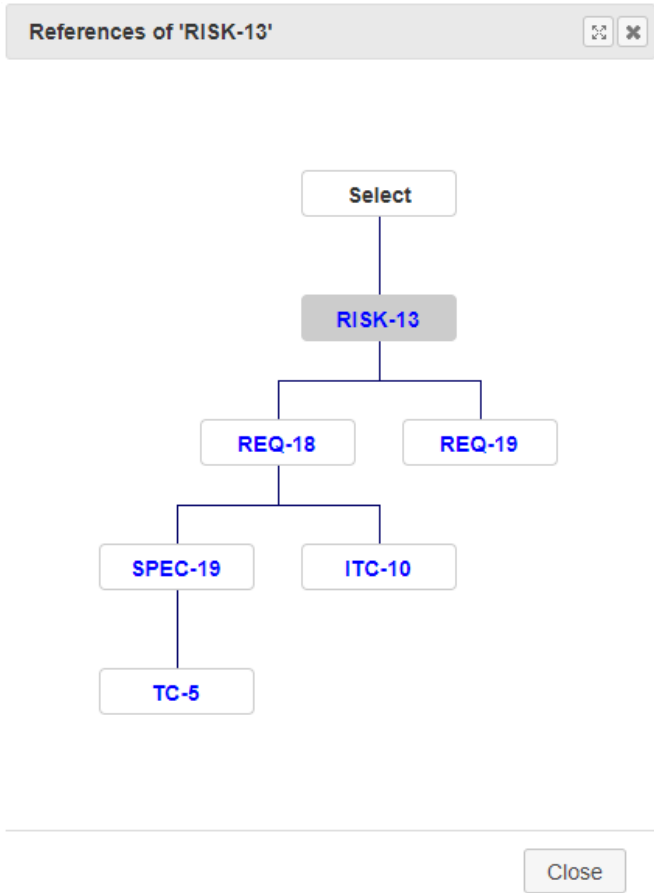
- **REQ-18** REQ-18 Data transfer shall have checksums ⌵
 - **REQ-19** REQ-19 App shall only show results if correct and complete data arrives ⌵
-
- no effect
reduces exposure to hazardous situation by 1
reduces exposure to hazardous situation by 2
reduces exposure to hazardous situation by 3
reduces exposure to hazardous situation by 4
reduces probability of harm by 1
reduces probability of harm by 2

- Cannot be reduced any further**
- Benefits outweigh remaining risk**

RAM

$$2 * 2 * 4 = 16$$

traceability



REQ-18 Data transfer shall have checksums

DR REQ DR RISK

DESCRIPTION

When sending data from watch to phone the data shall have checksums so that it can be ensured that all and the correct data arrives on the phone

REFERENCES

- SPEC-19 Checksums for data transfe
- ITC-10 Bad connection test

Create Specification Create Integrat

JIRA

- no tasks linked

SPEC-19 Checksums for data transfer

DR SPEC DR CODE DR RISK SPEC

DESCRIPTION

The checksum is computed by adding up the values. Every 5th value should be the checksum of the previous values e.g.

values	checksum
1 3 4 5	13
2 5 6 2	15

REFERENCES

- TC-5 Test Checksums

TC-5 Test Checksums

DR TC Alpha Beta Sample

DESCRIPTION

Verify that checksum computation is correct

JIRA

- no tasks linked

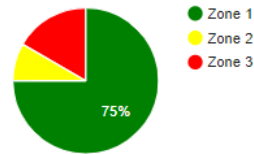
STEPS

	Action	Expected Outcome	
1	Run algorithm with 1 2 3 4	Result is 10	
2	Run algorithm with -1 2 3 4	Result is 8	

Doc (short video better to go through them)

Summary - Risk levels before controls

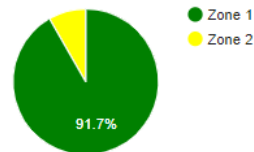
- 9 risks in zone 1 - no need for mitigations
- 1 risks in zone 2 - need for mitigation or justification
- 2 risks in zone 3 - need for mitigation



Risk levels after controls

Summary - Risk levels after controls

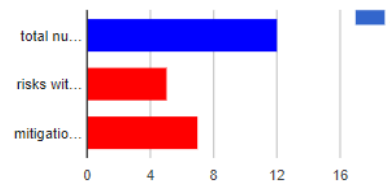
- 11 risks in zone 1 - no need for mitigations
- 1 risks in zone 2 - need for mitigation or justification
- 0 risks in zone 3 - need for mitigation



Test coverage overview

Summary - Test coverage overview

- 12 total number of risks
- 5 risks with mitigations without test cases
- 7 mitigations without test cases



Traces from risks to tests

- RISK-9 Invalid Data Recorded
- RISK-10 False Alarm
- RISK-11 No Data Recorded
 - REQ-7 Battery discharge control
 - Missing tests
 - RISK-4 Battery Rapid Discharge
- RISK-12 Not Enough Data Recorded
 - SPEC-4 Four Specification
 - Missing tests
 - SPEC-9 ROW 3
 - Missing tests
- RISK-13 Wrong Measurement
 - REQ-18 Data transfer shall have checksums
 - ITC-10 Bad connection test
 - SPEC-19 Checksums for data transfer
 - TC-5 Test Checksums
 - REQ-19 App shall only show results if correct and complete data arrives
 - Missing tests
- RISK-5 ageing housing
- RISK-4 Battery Rapid Discharge
- RISK-3 Kill patient by overdosing
 - SREQ-5 Prevent entry of lethal prescribed dose
 - Missing tests
- RISK-2 ageing housing
 - REQ-1 One Software Requirement
 - Missing tests
 - SPEC-1 One Software Unit
 - Missing tests
 - REQ-2 Another Software Requirement
 - Missing tests
- RISK-6 ageing housing
- RISK-7 Kill patient by overdosing
- RISK-8 Battery Rapid Discharge

Excel export

Ref	Folder	Title	Hazard	Sequence of Events	Hazardous Situation	Harm	Probability of Occurrence	Probability of Harm (b)	Severity (b)	RBM	Probability of Occurrence	Probability of Harm (a)	Severity (a)	RAM	Cannot be reduced
RISK-9	App ECG Measureme	Invalid Data Recorded	Bad data				3	2	4	24	1	2	4	8	
RISK-10	App ECG Measureme	False Alarm	False alarm sent to the				2	2	3	12	2	2	3	12	
RISK-11	App ECG Measureme	No Data Recorded	No data sent to the wat				2	2	1	4	2	1	1	2	
RISK-12	App ECG Measureme	Not Enough Data Reco	Data partially recorded				3	3	4	36	1	2	4	8	
RISK-13	App ECG Measureme	Wrong Measurement	Bad data collected and	User puts phone on tat	Distance phone to watc	Watch shows normal E	4	2	4	32	1	2	4	8	
RISK-5	App Blood Pressure M	ageing housing					4	2	1	8	4	2	1	8	
RISK-4	App Blood Pressure M	Battery Rapid Discharg					1	2	4	8	1	2	4	8	
RISK-3	App Temperature Mea	Kill patient by overdosir					1	3	4	12	1	1	4	4 X	
RISK-2	App Other	ageing housing		Sequence of Events:	Hazardous	Harm	1	3	3	9	1	3	3	9 X	
RISK-6	Portal	ageing housing		Sequence of Events:			1	2	3	6	1	2	3	6 X	
RISK-7	Data	Kill patient by overdosir					2	2	1	4	2	2	1	4 X	
RISK-8	Watch	Battery Rapid Discharg					2	2	2	8	2	2	2	8	

Q & A

Arnaud Alberts
Wolfgang Huber

Matrix Requirements GmbH - matrixreq.com

Aaron Joseph

Sunstone Pilot, Inc. - sunstonepilot.com