From justification requirements elicitation to their continuous production

Application in a medical technology company

Clément DUFFAU

PhD candidate and Lead developer
Our context
Critical domains

1. produces
2. contextualize
3. produce
4. reviews
5. develop
6. V&V
7. audits

Standards
Company's experts
Internal practices
Deliverable product
Product
certified

Regulatory authority
Medical technologies -

Various disciplines
- Clinical
- Electronics
- Software
- Mechanics

Standards
- IEC 62304
- ISO 14791
- IEC 62366

Tests
- Hardware
- Software
- System

Traceability
- Feasibility
- Architecture
- Development
- V&V

Human expertises

01/10/18 - duffau@i3s.unice.fr
Challenge: Confidence in justification

1. produces
2. contextualize
3. produce
4. reviews
5. develop
6. V&V
7. audits

Standards

Company’s experts

Internal practices

Regulatory authority

help to produce

elicitate

capture

Delivered product

Product

01/10/18 - duffau@i3s.unice.fr
Some vocabulary

**Justification requirement** : a proof element that must be reached to be compliant with a law. It can be set through a standard or a guide

**Elicitation** : action to help experts to formalize their knowledge to keep and share them

**Justification** : an argumentation attesting that a justification requirement is fulfilled

**Justification artefact** : a data (e.g. document, result) to establish in order to construct a justification
Improve confidence in justification management from requirement to production
Justification Diagrams¹

Derived from Toulmin argumentation schema ²

Compliant with Goal-Structuring Notation (GSN)

Comprehensive notation to explain why a result is trustable

Captures the rationale logical structure of all evidence that leads to the acceptance of a high-level property

Only a notation but proved to be useful ³ ⁴

⇒ A good starting point but need to be extended

1. Polacsek, T.: Validation, accreditation or certification: a new kind of diagram to provide Confidence
2. Toulmin, S.E.: The Uses of Argument
4. Polacsek, T., S. Sharma, C. Cuiller et V. Tuloup. «The need of diagrams based on toulmin schema application : an aeronautical case study», EURO Journal on Decision Processes

01/10/18 - duffau@i3s.unice.fr
Justification Pattern Diagram (JPD)

- Give an overview of the all justification requirements
- Elicitate links between justifications requirements

⇒ A way to structure justification requirements from standards to internal practices
Justification Diagram (JD)

- Give the terminal justifications linked to artefacts

⇒ A way to guide the justifications production
JPD and JD

Legend

Conclusion Sub-conclusion Evidence Strategy Restriction Rationale Usage domain

System integration tests validated

Internal accreditation

Evaluation integration tests

ISO 62304

Integration tests execution traces

Tests validated for module

Evaluate unit tests

ISO 62304

Module

Unit tests execution traces

For each Module

Tests validated for module A

Evaluate unit tests

ISO 62304

Module A

JUnit logs

Tests validated for module B

Evaluate unit tests

ISO 62304

Module B

SoapUI logs

Internal accreditation

Evaluation integration tests

ISO 62304
A semantics for JPD and JD

Définition 5.1.1 : Relation de conformité

Soit $\mathcal{A}$ l’ensemble des assertions, $\mathcal{R}$ est une relation de conformité ssi $\forall a_1, a_2, a_3 \in \mathcal{A} :$

- $a_1 \mathcal{R} a_1$
- if $a_1 \mathcal{R} a_2$ and $a_2 \mathcal{R} a_1$ then $a_1 = a_2$
- if $a_1 \mathcal{R} a_2$ and $a_2 \mathcal{R} a_3$ then $a_1 \mathcal{R} a_3$

$a_1 \mathcal{R} a_2$ se lira $a_1$ est conforme à $a_2$.

Définition 5.1.3 : Pas de justification

Un pas de justification (pas de justification) $p$ est un tuple $(\text{supports}, \text{strategie}, \text{conclusion})$ où :

- $\text{supports}$ est un ensemble d’assertions $\subset \mathcal{A}$,
- $\text{strategie} \in \mathcal{W}$;
- $\text{conclusion} \in \mathcal{A}$

DUFAU, C., T. POLACSEK M. BLAY -FORNARINO. 2018, Une sémantique pour les patrons de justification, INFormatique des ORganisations et Systèmes d’Information et de Décision 2018 (INFORSID)
A Meta-model for JD

DUFFAU, C., T. POLACSEK M. BLAY-FORNARINO. 2018, Une sémantique pour les patrons de justification, INFormatique des ORGanisations et Systèmes d'Information et de Décision 2018 (INFORSID)
Research conclusion

- Distinction between justification requirements and justification production
- A semantics to formalize the approach
- A meta-model to go to tools

⇒ Usefulness of JPDs and JDs
JPD and JD in action: application in the medical technologies company
- SME - a dozen of people
- Strong legacy - first french cochlear implant
- Focus on advanced R&D
- Agile development from hardware to software
Stakeholders:

1 researcher/practitioner, 2 quality system managers, 3 technical leaders

Study guideline for a stage:

1. The researcher designs a JPD according to quality management team and technical leader requirements

2. The technical leaders
   a. Identify justifications items that must be produced
   b. Develop tools to produce them

3. During the development step, the technical leaders
   a. Possibly define new activities
   b. Produce the necessary justifications

4. During the deployment step, the quality managers and the researcher analyze the differences between the original JPD and the JDs

5. During the audit, JPD and JDs are one of the supports of discussion with the authority

Prototyping

![Diagram showing the process flow for Prototyping]

- **Internal accreditation**
- **Assess software safety**
  - **Specifications validated**
  - **Feasible hard points**
- **Review specifications**
  - Requirements
- **Review feasibility**
  - Functional specifications
  - Feasibility studies
- **Technical specifications**
- **Validate hard points**
- **Software safety validated**
- **Credentials for IEC 62304**
Moving to development
Problem: For the company, good starting point but yet another way to abstract
Real industry need:
Use JPD and JD as a way to automate production and verification of justifications
Industrial needs

- Automate the production of justifications from justification requirements and artefacts in existing tools
- Help the verification and validation of justifications regarding requirements
- A seamless approach from the point of view of the quality management department
- Open source project management software
  - Roadmap
  - Issues
  - Documentation

- Used as Quality Management System (QMS)
  - Justifications from specifications to product V&V
  - The main software during audit
Continuous Integration platform
  ○ Integrate code all together on a daily basis
  ○ Automate compilation, unit tests, integration tests, deployment, ...

Daily at AXONIC
  ○ 5 tangled projects
    ■ Desktop software
    ■ Embedded software
    ■ Internal software
  ○ 6 compilation and unit tests x5
  ○ 6 integration tests x8
  ○ 2 quality analysis x1
Justification Factory

• Internal software developed during my PhD

• Management justification from the requirements to the production
  ○ Design JPD
  ○ (Automate) construction of JD
  ○ (Automate) verification and validation conformance

• Expose justification seamless services and justification services
Justification Factory
Going further with Jenkins

DUFFAU, C., B. GRABIEC M. BLAY-FORNARINO. 2017, Towards embedded system agile development challenging verification, validation and accreditation: Application in a healthcare company, ISSRE 2017-IEEE International Symposium on Software Reliability Engineering

01/10/18 - duffau@i3s.unice.fr
Justification Factory with Jenkins

DUFFAU, C., B. GRABIEC M. BLAY-FORNARINO. 2017, Towards embedded system agile development challenging verification, validation and accreditation: Application in a healthcare company, ISSRE 2017-IEEE International Symposium on Software Reliability Engineering

01/10/18 - duffau@i3s.unice.fr
JPD for system validation
### About the usefulness in

<table>
<thead>
<tr>
<th>Artefacts de justifications</th>
<th>Automatisation avant Justification Factory</th>
<th>Automatisation après Justification Factory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tests unitaires (~2000)</td>
<td>OUI (mais seulement les artefacts)</td>
<td>OUI</td>
</tr>
<tr>
<td>Tests d’intégration (~100)</td>
<td>OUI (mais seulement les artefacts)</td>
<td>OUI</td>
</tr>
<tr>
<td>Tests systèmes (~50)</td>
<td>NON</td>
<td>OUI</td>
</tr>
<tr>
<td>Tests exploratoires (~10)</td>
<td>NON</td>
<td>NON</td>
</tr>
<tr>
<td>Sanity check (13)</td>
<td>NON</td>
<td>NON</td>
</tr>
<tr>
<td>Traçabilité livraison (6)</td>
<td>NON</td>
<td>OUI</td>
</tr>
</tbody>
</table>
Scale up: JPD for design dossier

- Under industrial properties

- JPD tracing all the justifications for ISO 13485 for AXONIC including
  - ISO 14971 - Risks management
  - IEC 62304 - Software in medical devices
  - IEC 62366 - Usability engineering
  - IEC 60601 - Safety and performance of medical electrical equipment

- Some metrics to give a hint
  - 184 documents on Redmine used as justification artefacts
  - 300 evidences
  - 175 conclusions
Codification: [hidden]
Edition: B
Nom du projet: [hidden]
Référence du projet: 022_[hidden]
Diffusion: AXONIC

**Historique**

<table>
<thead>
<tr>
<th>Edition</th>
<th>Date</th>
<th>Motifs</th>
<th>Auteur</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24/07/2017</td>
<td>Création</td>
<td>BG</td>
</tr>
<tr>
<td>B</td>
<td>21/11/2017</td>
<td>Modification</td>
<td>BG</td>
</tr>
</tbody>
</table>

**Modification**

- Edition B:
  - Modifications suite aux modification dans [hidden] _ST_0001
  - [#7373](#)

**Objet**

Le présent document décrit [hidden]

**Références**

- [hidden] _ST_0001_B : Spécifications techniques (ticket principal #7217)

**Approbation du document**

<table>
<thead>
<tr>
<th>Auteur</th>
<th>Vérificateur : LW</th>
<th>Vérificateur : FS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: 21/11/2017</td>
<td>Date: 23/11/2017</td>
<td>Date: 27/11/2017</td>
</tr>
<tr>
<td>Acceptation numérique : OK -- BG</td>
<td>Acceptation numérique : OK -- LW</td>
<td>Acceptation numérique :OK -- FS</td>
</tr>
</tbody>
</table>
## Master file for design dossier

### INITIALISATION

<table>
<thead>
<tr>
<th>Phase projet</th>
<th>Type</th>
<th>Référence</th>
<th>Intitulé</th>
<th>Lien</th>
<th>Date</th>
<th>Auteur</th>
<th>Approuvé</th>
<th>Verrouillé</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialisation</td>
<td>RIN</td>
<td>_RIN_0001_A</td>
<td>Revue d'initialisation</td>
<td>_RIN</td>
<td>14/06/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 26/06/17 rev.3</td>
</tr>
<tr>
<td>Initialisation</td>
<td>RIN</td>
<td>_RIN_0001_B</td>
<td>Revue d'initialisation</td>
<td>_RIN_0001_B</td>
<td>27/10/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 30/10/17 rev.6</td>
</tr>
<tr>
<td>Initialisation</td>
<td>RIN</td>
<td>_RIN_0001_C</td>
<td>Revue d'initialisation</td>
<td>_RIN_0001_C</td>
<td>27/11/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 05/12/17 rev.6</td>
</tr>
<tr>
<td>Initialisation</td>
<td>RIN</td>
<td>_RIN_0001_D</td>
<td>Revue d'initialisation</td>
<td>_RIN_0001_D</td>
<td>22/02/18</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 19/03/18 rev.8</td>
</tr>
</tbody>
</table>

### DONNÉES ENTRÉE

<table>
<thead>
<tr>
<th>Données d'entrée</th>
<th>Type</th>
<th>Référence</th>
<th>Intitulé</th>
<th>Lien</th>
<th>Date</th>
<th>Auteur</th>
<th>Approuvé</th>
<th>Verrouillé</th>
</tr>
</thead>
<tbody>
<tr>
<td>Données d'entrée</td>
<td>EE</td>
<td>EE_001_A</td>
<td>Exigences essentielles</td>
<td>EE_001_A</td>
<td>04/07/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 18/07/17 rev.16</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>EE</td>
<td>EE_001_B</td>
<td>Exigences essentielles</td>
<td>EE_001_B</td>
<td>27/07/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 31/07/17 rev.4</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>EE</td>
<td>EE_001_C</td>
<td>Exigences essentielles</td>
<td>EE_001_C</td>
<td>27/03/18</td>
<td>JP</td>
<td>OUI</td>
<td>21/05/18 rev.62</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>DE</td>
<td>DE_001_A</td>
<td>Données d'entrée de</td>
<td>DE_001_A</td>
<td>26/06/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 07/07/17 rev.14</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>DE</td>
<td>DE_001_B</td>
<td>Données d'entrée de</td>
<td>DE_001_B</td>
<td>11/07/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 24/07/17 rev.26</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>DE</td>
<td>DE_001_C</td>
<td>Données d'entrée de</td>
<td>DE_001_C</td>
<td>11/08/17</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 11/09/17 rev.10</td>
</tr>
<tr>
<td>Données d'entrée</td>
<td>DE</td>
<td>DE_001_D</td>
<td>Données d'entrée de</td>
<td>DE_001_D</td>
<td>21/02/18</td>
<td>LG</td>
<td>OUI</td>
<td>OUI 21/03/18 rev.11</td>
</tr>
</tbody>
</table>
Justification Factory with Redmine

Diagram showing the integration of Justification Factory with Redmine, including services like JD Service, Conformance Service, and JPD Service, along with components such as Justification Engine, Patterns Library, and Justification artefacts base.
<table>
<thead>
<tr>
<th></th>
<th>Avant Justification Factory</th>
<th>Après Justification Factory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nombre total de documents</td>
<td>358</td>
<td>377</td>
</tr>
<tr>
<td>Nombre de documents de justifications (présence d'une section &quot;Approbation&quot;)</td>
<td>165</td>
<td>184</td>
</tr>
<tr>
<td>Nombres de documents de justification en erreur</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pas d'auteur</td>
<td>15</td>
<td>8</td>
</tr>
<tr>
<td>pas signé par l'auteur</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>signé par l'auteur, mais non approuvé</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>pas de date de signature</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>approuvé, mais non verrouillé</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>Taux d'erreur dans les documents de justifications (en %)</td>
<td>33.9</td>
<td>16.3</td>
</tr>
<tr>
<td>Nombre de documents de justifications dans le MasterFile</td>
<td>159</td>
<td>184</td>
</tr>
<tr>
<td>Nombre de documents de justifications verrouillés oubliés dans le MasterFile</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Nombre de documents de justifications non verrouillés présents dans le MasterFile</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>Taux d'erreur dans le MasterFile (en %)</td>
<td>13.8</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Industrial needs

✓ Automate the production of justifications from justification requirements and artefacts in existing tools

✓ Help the verification and validation of justifications regarding requirements

✓ A seamless approach from the point of view of the quality management department
Conclusion and perspectives

Usefulness of JPDs and JDs
   ➔ Distinction between justification requirements and justification production
   ➔ Formally defined

Fill industrial needs
   ➔ Automate production and V&V for justifications
   ➔ Positive feedbacks from industrials

Application to none-critical domains
   ➔ ROCKFlows : Meta-learning to predict the best workflow

Provide integration of dedicated tools with others common industrial technologies
   ➔ Requirements and documentation : Atlassian
   ➔ Code : SonarQube
Questions, Comments ?
AXONIC feedbacks

Medical technologies

● Tangled standard requirements
  ○ IEC 62304 - Medical device software
  ○ IEC 62366 - Application of usability eng. to medical devices
  ○ ISO 14971 - Medical devices risk management
    ⇒ Redundant justifications ⇒ JPDs help to identify them

● Agile development
  ○ 2-weeks sprints
  ○ Continuous Integration
    ⇒ Justification tsunami ⇒ JDs capture the incrementality

● SME
  ⇒ Justification is handle by everyone and need to be efficient
  → JPD ← JD helps to automate production
Standard evolution in JPD
Standard evolution in JD
Requirement Eng. - i*

Early-phase requirements

Focus on who and what (process oriented)

In version 2.0, replace soft-goal by quality

Extension to put argumentation on it but not to justify

⇒ They are a way to identify what we need to justify but not how

Assurance Case - SACM

Historically Goal Structuring Notation¹ (GSN) and Claim-Argument-Evidence² (CAE)

Used for safety case

New OMG standard: Structured Assurance Case Metamodel³

Focus on 3 aspects:

- Argumentation
- Artifact
- Assurance Case

⇒ A pivot conceptual model
not aiming to manage justifications

1. Kelly, T., Weaver, R.: The goal structuring notation /- a safety argument notation
2. Emmet, L., Cleland, G.: Graphical notations, narratives and persuasion: a pliant systems approach to hypertext tool design
3. OMG: Structured assurance case meta-model (sacm)
I* and JPD
Aircraft manufacturing case study

Stakeholders:

1 researcher, aircraft architects, workload experts

Study guideline:

1. The researcher goes 2 days in the product line
2. The researcher, aircraft architects, workload experts iteratively design JDs for each main project stage based on past projects
3. The stakeholders abstract the JDs to capture global practices into JPDs
During preliminary design

- List of all items validated
- Expert assessment
- Expert credentials
- Aircraft design

- Workload assessment validated
- Abacus
- Item description (not new item)
- Item description (new item)
- Ergonomic criteria validated

- New component workload assessment validated by experts
- Expert assessment
- ATA

- For each item
- For each ATA

Legend
Conclusion Sub-conclusion Evidence Strategy Rationale Usage domain
During advanced design

- Workload assessment validated
- Experts’ committee validation
- Experts credentials
- List of all items validated
- Expert assessment
- Expert credentials
- Aircraft design
- Ergonomic criteria validated
- Item description
- Component workload assessment validated by expert
- Expert credentials for ATA

Legend:
- Conclusion
- Sub-conclusion
- Evidence
- Strategy
- Rationale
- Usage domain
Early development
Justification Diagrams lifecycle

[Diagram showing the lifecycle of justification diagrams, including iterations and steps like derivation, realization, comparison, alignment, and copying.]