Challenges in providing support for management of evidence-based arguments

Janusz Górski
Aleksander Jarzębowicz
Jakub Miler
Andrzej Wardziński

Department of Software Engineering, Gdańsk University of Technology, Poland
ARGEVIDE sp. z o.o., Gdańsk, Poland

IMBSA 2014
Munich, October 27-29, 2014
Structure

- Objective
- Evidence-based arguments
- Application areas
- The NOR-STA platform of services
- Selected challenges
  - what is a challenge
  - the NOR-STA response
Objective

- To review selected challenges related to application of evidence-based arguments resulting from our experience
- To present how NOR-STA tool is responding to these challenges
Evidence-based Arguments

- **Argument** is an attempt to persuade someone of something, by giving reasons and/or evidence for accepting a particular conclusion.

- This 'something' can be:
  - assurance of some important property (safety, security, privacy, reliability, …)
  - conformance to a stated set of criteria (described in a standard, norm, directive and so on)
  - ranking in fulfillment of the accepted requirements
  - …

- **Evidence** in its broadest sense includes everything that is used to determine or demonstrate the truth of an assertion.
  - Evidence can be used to support arguments – by demonstrating the truth of its premises.

**Assumption:**
Evidence is delivered in electronic documents of any form: text, graphics, image, video, audio etc.

If an argument based on evidence is used to strengthen trust relationships, we call it **trust case**.
Trust cases
Evidence based arguments
Deployment in the cloud

- Application specific packages
- Generic Argument Management Services
Deployment in the cloud

Generic Argument

Management

Services

Application specific packages
Experience

- Research & Development & Trials (years 2000-14)
  - Several international and national R&D projects (including 5. and 6. EU FR projects)
  - Several deployments for individual national and international partners
  - 120 experimental deployments in different enterprises (hospitals, businesses, public administration) where NOR-STA has been applied to support real business processes

- Commercial (since April 2014)
  - 15 real customers (including a big international player)
Challenge 1
Communication and teamwork

- Multiple viewpoints
- Different roles (developers, assessors, viewers,..)
- Vertical communication (up the decision making hierarchy)
- Integration with business processes
Challenge 2
Operating large arguments

- Large arguments difficult to handle
- Adding/modifying a node can change the graph in two dimensions
- Adding more explanatory text expands a node and gives a false feeling of growing importance of the node
Challenge 2
Operating large arguments

- Large arguments difficult to handle
- Adding/modifyng a node can change the graph in two dimensions

- C4: The parameters entered are the parameters intended by the person entering them (no user entry error)
- _S5: Argue that entering parameters via barcode readers is safe
  _R5: Justification for argument strategy
  A1: GIP is equipped with a barcode reader. Patient wears a barcode wristband. Drugs are labeled with a barcode.
  C5: Parameters are entered via a barcode reader where possible to mitigate against human error
- _S2: Argue over hazards to manually entering the parameters
  _R2: All existing hazards are identified
  C2: List of identified hazards related to manual programming
- _C6: Entry errors caused by keypad design are mitigated
- _C12: The design and implementation of the GIP mitigates against input values being misinterpreted internally
- _C13: The GIP design prevents activation if there is a missing parameter
- _C15: Units errors are mitigated
Challenge 3
Managing evidence

- Integrating any electronic document as an evidence container: text, graphics, video stream, audio,…
- Providing for referencing any place the document is stored in (web pages, ftp, svn, …)
- Referencing selected fragments of bigger documents (pages, chapters, sections, …)
- Providing for protected repositories, if needed
- Providing for user selected repositories
4. **PCA Pump Function**

The PCA pump infuses at prescribed basal, bolus, or KVO rates.

#### 4.1 Basal Flow Rate

- The **basal flow rate** is prescribed by a physician and entered into the PCA pump by scanning the prescription from the drug container label as it is loaded into the reservoir. (UC1.7 §3.1.1)

- The pump shall be able to deliver basal infusion at flows throughout the **basal infusion flow range** of $F_{\text{base}} = 1$ to $F_{\text{base max}} = 10$ ml/hr. (UC1 §3.1.1)

- The pump shall deliver basal infusion at the prescribed basal rate within a **basal infusion flow tolerance** of $F_{\text{base tol}} = 0.5$ ml/hr of the prescribed basal rate. (UC1.12 §3.1.1)

- Any alarm stops basal rate9 delivery either halting pump or switching to KVO rate as defined in Table 4. (many EC)

- The pump shall maintain a **minimum KVO flow rate** of $F_{\text{KVO}} = 1$ ml/hr at all times during infusion, even during alarms, unless the alarm also stops flow, or the stop button is pressed. Table 4 defines which alarms also stop drug flow completely. (EC1.2 §3.2.7)

#### 4.2 Patient-Requested Bolus

- Upon patient’s press of the PCA pump’s patient-button, a prescribed bolus volume to be infused, $VTBI$, of the drug loaded in the pump is delivered to the patient. (UC2 §5.1.2)

- A patient-requested bolus shall be delivered at its prescribed rate, $F_{\text{bolus}}$, in addition to the prescribed basal flow rate, $F_{\text{base}}$, but no more than the maximum flow rate for the pump, $F_{\text{max}}$. (UC3 §3.1.2)

- Patient-requested bolus shall not be delivered more often than a prescribed **minimum time between patient-requested bolus**. (UC2.2 §3.1.2)

- Prescribed bolus rate shall not exceed the **maximum VTBI** limit set by the drug package from the hospital pharmacy for the drug loaded in the PCA pump. (EC3 §3.2.3)

---

**Claim 1.1: PCA pump is effective**

- **Argue over all behavior**

  - **Divide into individual**

  - **Claim 1.1: Combo**

  - **Claim 1.1.2: PCA Pump**

  - **Strategy 1.1.2.1**

  - **Rationale 1.1.1.1**

  - **Base Rate R**

  - **Require**

  - **Base Rate S**

  - **Claim 1.1.3: Upon**

  - **Claim 1.1.4: Clinician may command VTBI to be infused over a specified period of time**

  - **Claim 1.1.5: Pressing Stop Button stops pumping**
Challenge 4
Argument assessment and visualization

- Providing for argument assessment
- Support for different assessment methods
- Automatic aggregation of local assessments
- Assessment results visualisation
- Supporting multiple assessments
Challenge 4
Argument assessment and visualization
Challenge 5
Change control and state reporting

- Support for representing argument, assessment and evidence evolution
- Support for forming baselines
- Support for rollback
- Support for accountability of changes
Challenge 5
Change control and state reporting

- Support for representing argument, assessment and evidence evolution
- Support for forming baselines
- Support for rollback
- Support for accountability of changes
Challenge 6
Argument reuse

- Supporting specification of reusable argument patterns
- Supporting creation of patterns libraries
- Supporting easy export/import of patterns
- Supporting relative comparisons of patterns implementation
Challenge 6
Argument reuse

CL1: Conformance to Regulation (EU) No 994/2010 - measures to safeguard security of gas supply

ARG1: Argument by regulation actions

W1: Regulation requirements

CL1.1: Initial actions

ARG1.1: Argument by article requirements

W1.1: Requirements of Article 2, 3 and 13(6)

F1.1.1: 3 December 2011: Definition of "Protected customers"

F1.1.2: 3 December 2011: Designation of a Competent Authority

F1.1.3: 3 December 2011: Definition of roles and responsibilities

[EXAMPLE] Definition of roles and responsibilities

F1.1.4: 3 December 2011: Information about intergovernmental agreements

[EXAMPLE] Information about intergovernmental agreements - a map

[EXAMPLE] Information about intergovernmental agreements - another map

CL1.2: Risk Assessment

CL1.3: Preventive Action Plan

CL1.4: Emergency Plan

CL1.5: Bi-directional capacity

Source documents

Evidence

Calendar of Events

Risk Assessment Template based on JRC Guidelines
Challenge 6
Argument reuse

Projects
- TEMPLATE: Conformance to Regulation (EU) No 994/2010 - measures to safeguard security of gas supply
- CountryA
- CountryB
- CountryC
- Austria
- Belgium
- Bulgaria
Challenge 7
Data security
# Challenge 7

## Data security

### Permissions Table

<table>
<thead>
<tr>
<th>Username</th>
<th>Real name</th>
<th>Global role</th>
<th>Project role</th>
<th>Account disabled</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mfrank</td>
<td>Mary Frank</td>
<td>Global Developer</td>
<td>Project Assessor3</td>
<td></td>
<td>Auditors Ltd.</td>
</tr>
<tr>
<td>rgreen</td>
<td>Robert Green</td>
<td>Global Assessor</td>
<td>Project Assessor3</td>
<td></td>
<td>Auditors Ltd.</td>
</tr>
<tr>
<td>abrown</td>
<td>Adam Brown</td>
<td>Global Developer</td>
<td>Project Administrator</td>
<td></td>
<td>Company Ltd.</td>
</tr>
<tr>
<td>jsmith</td>
<td>John Smith</td>
<td>Global Developer</td>
<td>Project Administrator</td>
<td></td>
<td>Company Ltd.</td>
</tr>
</tbody>
</table>

**Selected project:** Generic Infusion Pump Assurance Case

**Project Role:** Project Assessor3

**Permissions:**

- **General**
  - Read
  - Read Details
  - Edit
- **Folder & Project**
  - Export Folder
  - Copy Project
  - Create New Project
  - View Assessments
  - Configure Repositories
  - Configure Assessment
  - Manage Snapshots
  - View Snapshots

**Node**

- New Node / Paste Node
- Attach & Open Evidence
- View Assessment Result
- View Assessment History
- Assess
- Change Sibling Order
- Compare Assessments
Challenge 8
Argument portfolio management

- Arguments are often interrelated
  - Patterns libraries
  - Assurance cases of subsystems
  - Arguments dedicated to a specific user
  - ...

- It is useful to group them together to facilitate access and to enforce common policies
Challenge 8
Argument portfolio management

Arguments are often interrelated.

- Patterns libraries
- Assurance cases of subsystems
- Arguments dedicated to a specific user

It is useful to group them together to facilitate access and to enforce common policies.
IF YOU WANT TO LEARN MORE ABOUT:

- NOR-STA argument model
- Creating arguments
- Assessing arguments
- User management and export/import
- Live access to NOR-STA
- Possibility to continue at home
WELCOME TO NOR-STA TUTORIAL

BUILD YOUR SAFETY CASE ON-LINE

Join NOR-STA tutorial
Tuesday, October 28th
8:30 - 10:30 or 14:30 - 16:30
Room Munchen 2