Ingénierie dirigée par les modèles pour structurer et partager un référentiel d'exigences de sûreté dans la durée

Nicolas Sannier

Ingénierie dirigée par les modèles pour structurer et partager un référentiel d'exigences de sûreté dans la durée

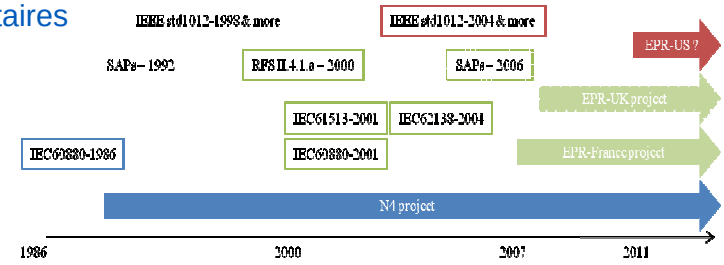
Nicolas Sannier* **

** EDF R&D STEP P1A – 6 quai Watier 78401 Chatou cedex*

** Inria Rennes EPI Triskell – Campus de Beaulieu 35042 Rennes cedex*

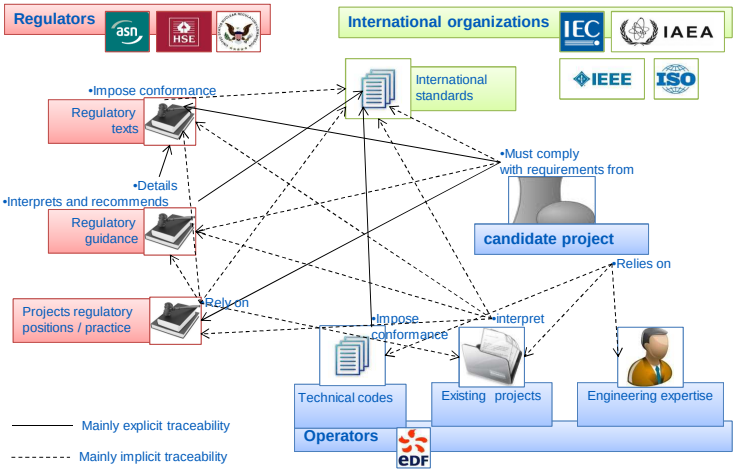
Variabilité et traçabilité des exigences réglementaires

- Une pratique non formalisée sur des projets à longue durée de vie
- Des exigences volontairement ambigües pour certaines et potentiellement interprétées différemment d'un pays à un autre
- Des corpus réglementaires différents et réévalués
- Des attentes et des approches différentes des autorités de sûreté
- Comprendre et rapprocher ces différences



Variabilité des exigences dans le temps et dans l'espace

Publié à Model-driven Requirements Engineering (MoDRE) 2011



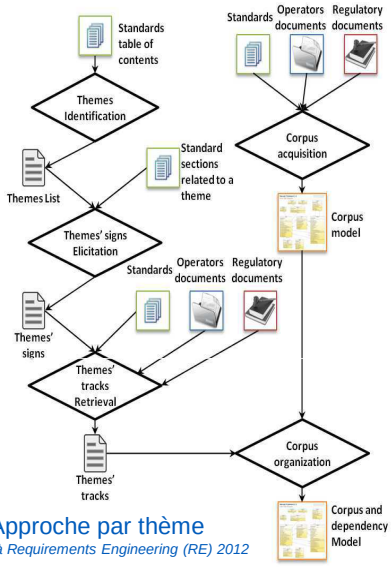
Sources d'exigences dans les projets et traçabilité

soumis à Requirements Engineering (RE) 2012

Ingénierie des exigences dirigée par les modèles

Un métamodèle pour :

- exprimer les concepts clés du monde réglementaire
  - Différents types de textes, différents types d'exigences, contextes …
- organiser la connaissance en un ensemble de relation
  - Références, pratiques acceptables …
  - Représenter différemment les connaissances (support à une interface et à analyse)



Approche par thème

soumis à Requirements Engineering (RE) 2012

Des actions centrées sur les documents et sur les expertises métier

- Acquérir un corpus d'exigences
- Capturer et Représenter ce corpus dans un modèle d'exigences
- Déterminer et représenter les premiers éléments de traçabilité dans le modèle
- Déterminer les grandes préoccupations (les thèmes) dans ce corpus
- Déterminer les régions du corpus qui sont relatives à ces thèmes
- Rendre la main aux experts pour continuer à enrichir le modèle
- Aider à retrouver certaines pratiques non formalisées et connaissances tacites

6.2 Self-supervision

6.2.A The software of the computer-based system **shall** supervise the hardware during operation within specified time intervals and the software behaviour **(A.2.2)**.
This is considered to be a primary factor in achieving high overall system reliability.

6.2.B Those parts of the memory that contain code or invariable data **shall** be monitored to detect unintended changes.

6.2.C The self-supervision **should** be able to detect to the extent practicable:
- *Random failure of hardware components;*
- *Erroneous behavior of software (e.g. deviations from specified software processing and operating conditions or data corruption);*
- *Erroneous data transmission between different processing units.*

6.2.D **If** a failure is detected by the software during plant operation, the software **shall** take appropriate and timely response. Those **shall** be implemented according to the system reactions required by the specification and to **IEC 61513** system design rules.
This **may** require giving due consideration to avoiding spurious actuation.

6.2.E Self-supervision **shall not** adversely affect the intended system functions.

6.2.F It **should** be possible to automatically collect all useful diagnostic information arising from software self-supervision.

Partitioning, **definition**, **reference**, information, scope, *composition*, characterization

Possibles acquisitions d'information sur les textes

présenté à Model-Driven Requirements Engineering (MoDRE) 2011

Contributions

• **Défis pour la variabilité et la traçabilité des exigences en ingénierie système**, Nicolas Sannier & Benoît Baudry, *in INFORSID 2011*, Lille, 24-26 may 2011

• **Formalizing standards and regulations variability in longlife projects. A challenge for model-driven engineering**, Nicolas Sannier, Benoît Baudry & Thuy Nguyen, *in 1st workshop MODRE Model-Driven Requirements Engineering*, Trento, Italy, 29th august 2011.

• **Retrieving Themes' Tracks in Nuclear International Standards**, Nicolas Sannier, Benoît Baudry & Thuy Nguyen, *soumis à RE2012*

Contact : *Nicolas Sannier – nicolas.sannier@inria.fr @edf.fr*