Forget your Excel worksheets!
The model based safety analysis is coming
ALL4TEC - Who we are

- Independent company established in 1998
  - 50 employees, 95% of engineers
  - People across the world

- Eclipse member since this year
  - Come and see us on booth n°15!
ALL4TEC - Who we are

- Provide a range of innovation and engineering solutions and services to various customers in different fields
  - Safety and system engineering
  - Software and system reliability
  - Model based testing
  - Process improvement
ALL4TEC - Our solutions
What is safety engineering?

“What safety engineering (…) is strongly related to systems engineering, industrial engineering and the subset system safety engineering. Safety engineering assures that a life-critical system behaves as needed, even when components fail.”

Wikipedia

- Expert assessment, but no tools available

- Most common fault modeling techniques
  - Failure mode and effects analysis (FMEA)
  - Fault tree analysis (FTA)
Why model based safety analysis?

- Complementary to model based system engineering

Diagram:
- System feared events
- Sub-System feared events
- Risks analysis
- Requirements
- Functional design
- Sub-system design
- Sub-system reception
- Integration
- Qualification
Why model based safety analysis?

- Risks analysis method developed and proven by ALL4TEC

- **Manual** local analysis
  - For each leaf block

- **Automatic** global analysis
  - For the whole system
Provides support to the implementation of FMEA and automatically deducts the FTA corresponding to the identified feared events.
Safety Architect - Principles

- Integrate safety analysis and design
- Decrease risk of error
- Focus on added value tasks
- Reduce analysis costs
Consider the safety analysis as a continuous improvement process
What are the benefits of using Eclipse RCP?

- High quality and open source framework
- Actively maintained by a vibrant community
- Common backbone for all our tools
- Off-the-shelf components
Feedbacks

- Domain Specific Language (DSL) vs UML?
  - First versions built with a complete DSL...
  - ... But need also to address users with standard vocabulary
Snippet of the components and technologies used
Open Source strategy

- Safety Architect will become Open Source!
  - Change our business model
  - Be credible for Long Term Support
  - Spread our technology and methodology involving a large community
Open Source strategy

- In accordance with the company strategy
  - Eclipse Member
  - Official Papyrus support
  - The next step: Integration with the Polarsys community