UML Modeling and Formal Verification of Secure Group Communication Protocols

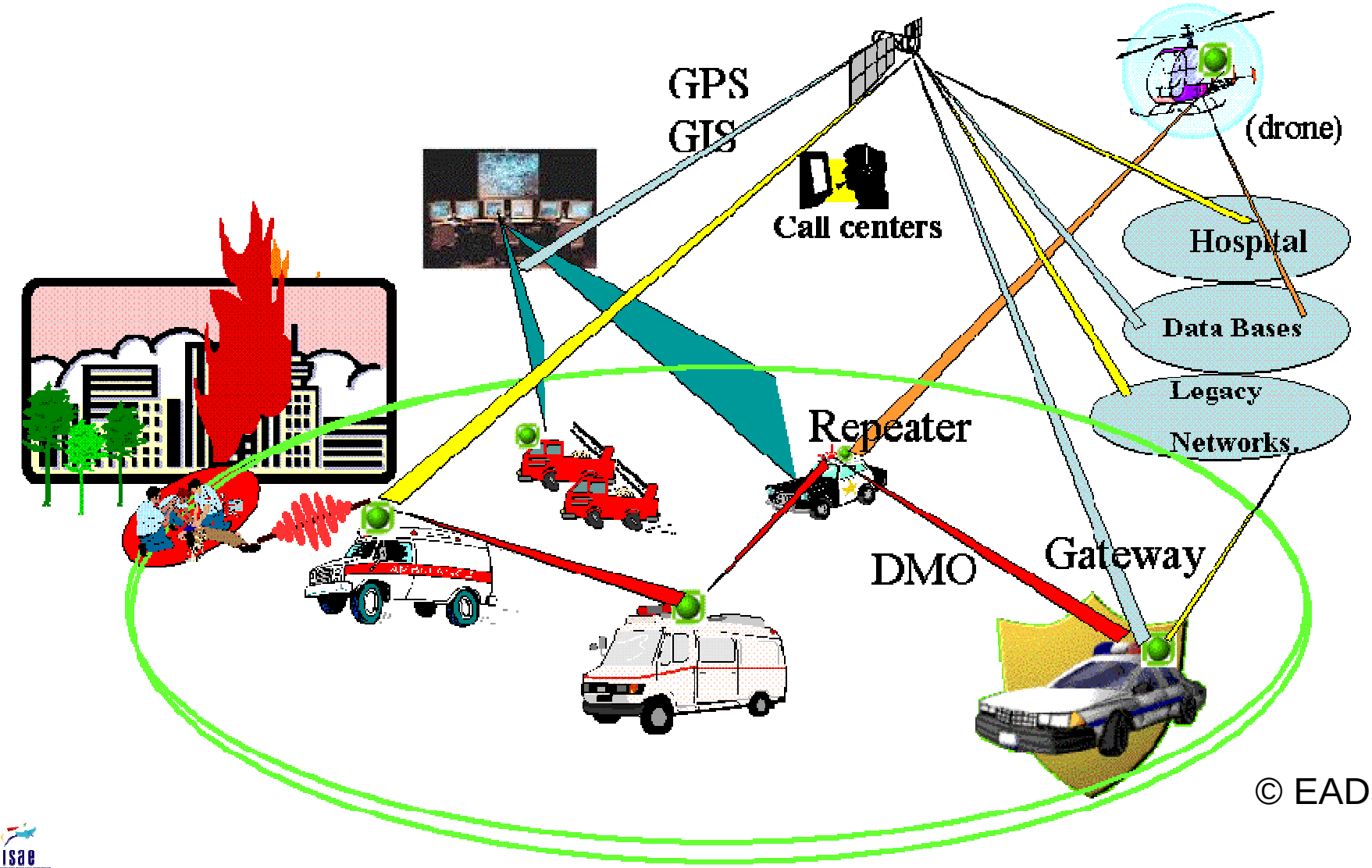
P. de Saqui-Sannes, T. Villemur, B. Fontan, S. Mota,

M.S. Bouassida, N. Chridi, I. Chrisment, L. Vigneron

pdss@laas.fr

UML-FM'09
Rio de Janeiro, RJ, Brasil
8/12/2009

Working together, a PMR terminal in hand



© EADS

© Pierre de Saqui-Sannes, 2009

Challenges and Bottlenecks

- **Secured Group Communication system (SGC)**
  - Key-based security
  - Group management
    - Dynamic group
    - Hierarchy
- **Architecture design and validation**
  - Protocol mechanisms proposed by TelecomParis, UTC, LORIA
  - Model-based validation
    - Performance evaluation by LORIA (NS) and UTC (Matlab)
    - Security flaws detection (AVISPA @ LORIA)
    - Deadline violation detection (TURTLE @ LAAS-CNRS)
- **A verification-centric UML method for SGC design**
  - Reuse of AVISPA and TURTLE

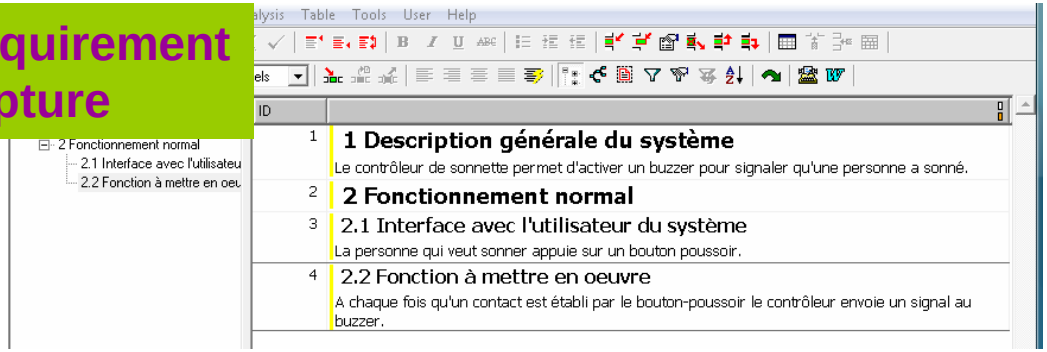
© Pierre de Saqui-Sannes, 2009

UML method for SGC design

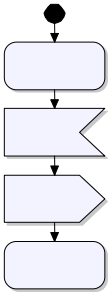
Before using UML

Using UML

Requirement capture

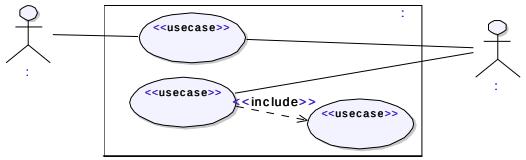


Design (behaviors)

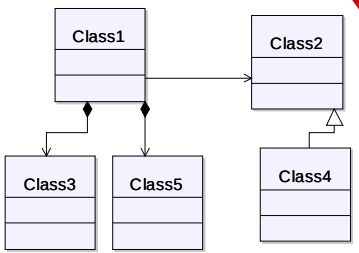


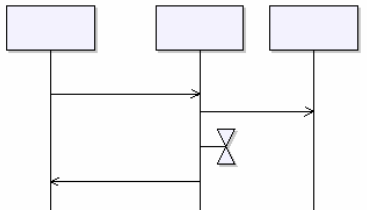
Formal verification
- security : AVISPA
- timeliness : TURTLE

Analysis (use-case)



Design (architecture)

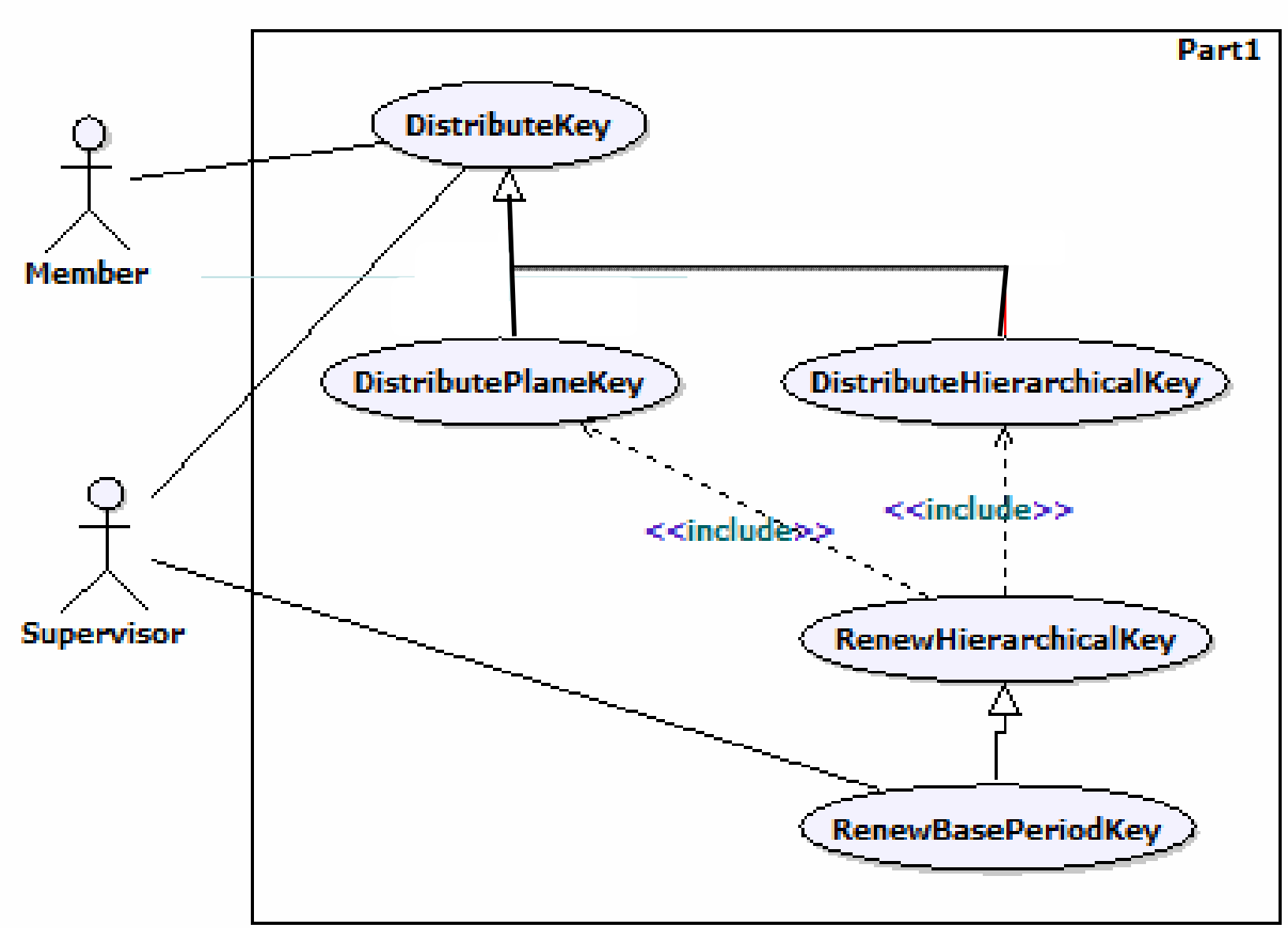




Analysis (scenarios)

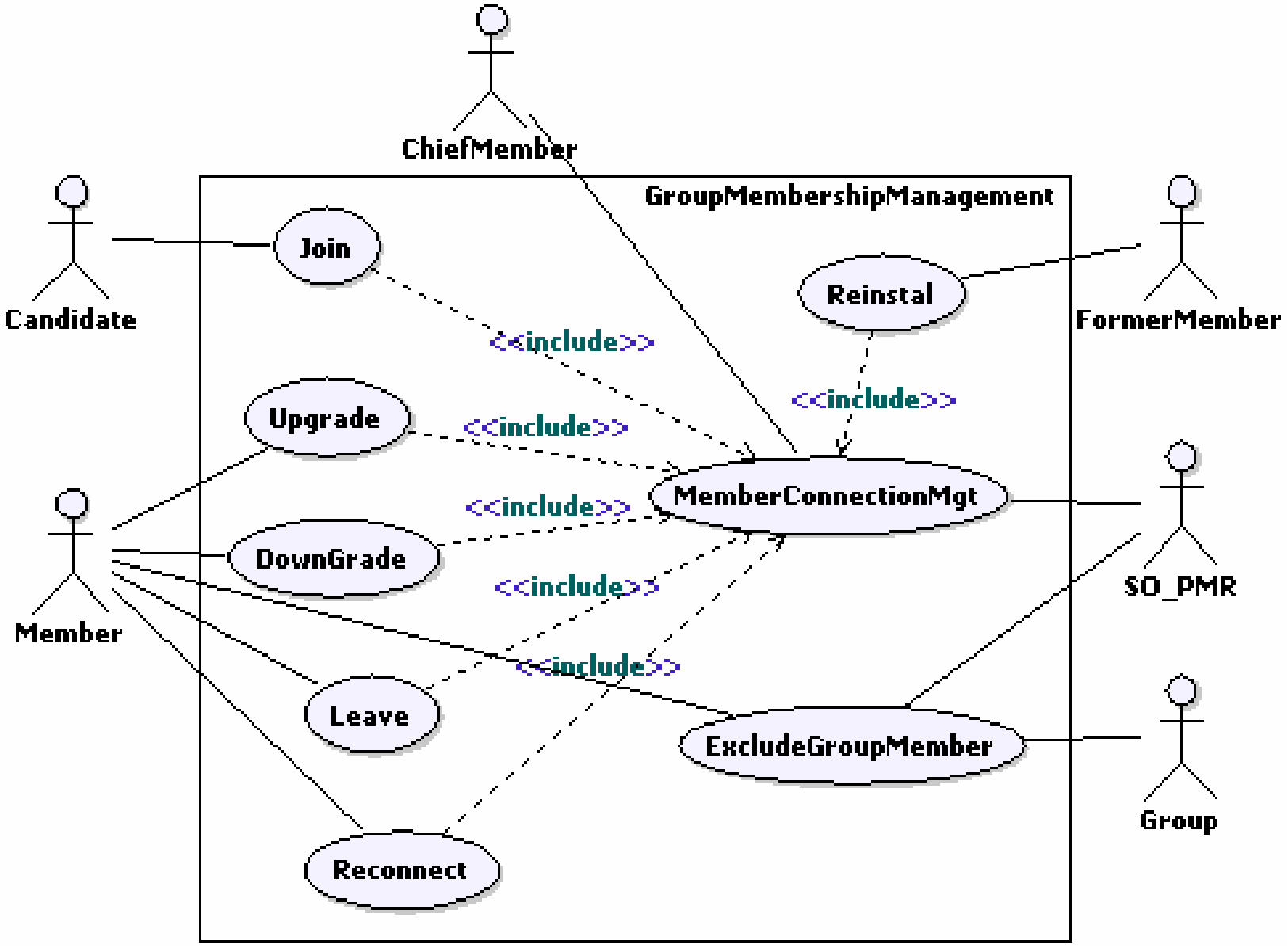
© Pierre de Saqui-Sannes, 2009

Pattern – Key Management



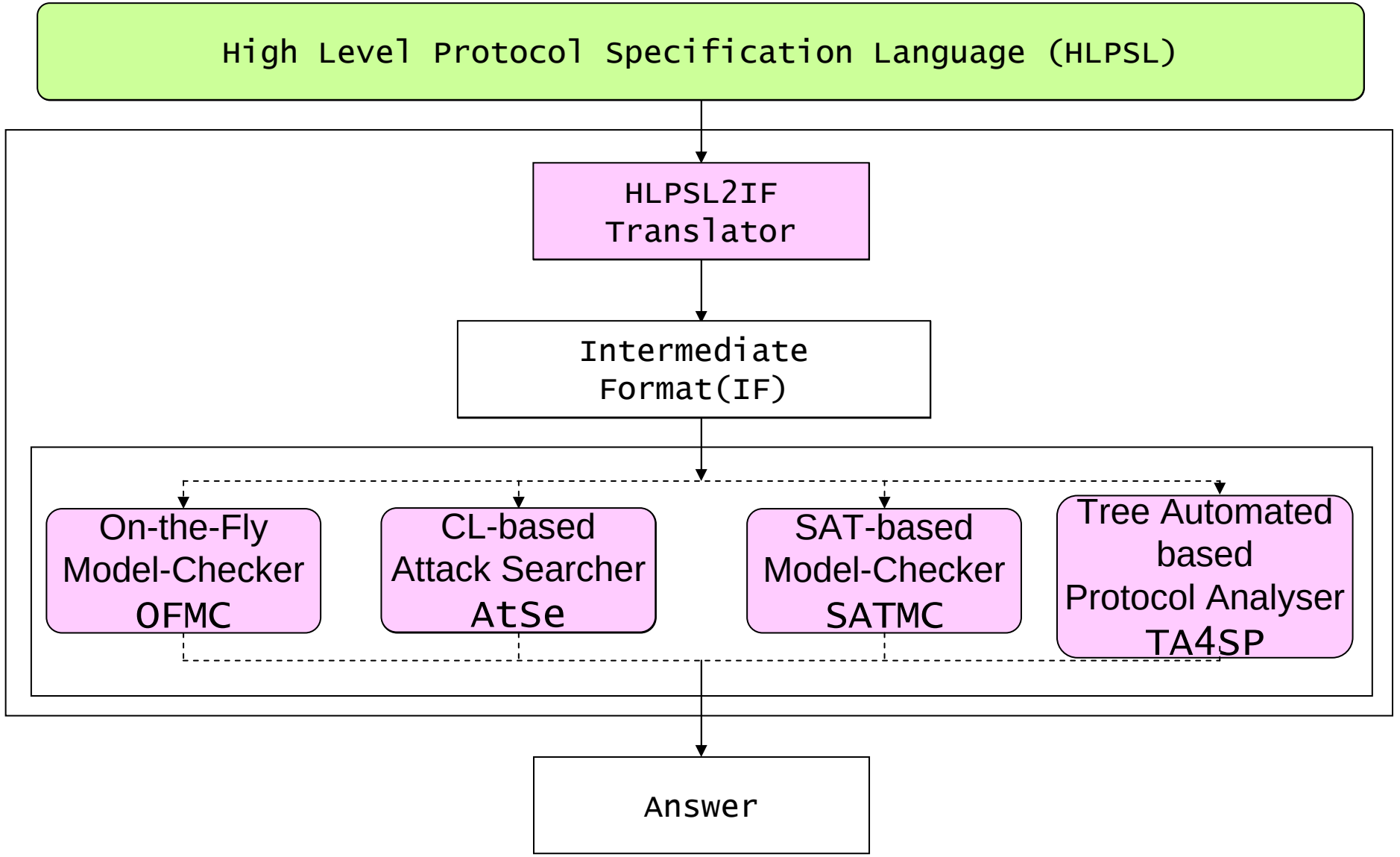
© Pierre de Saqui-Sannes, 2009

Pattern – Group Management



© Pierre de Saqui-Sannes, 2009

AVISPA



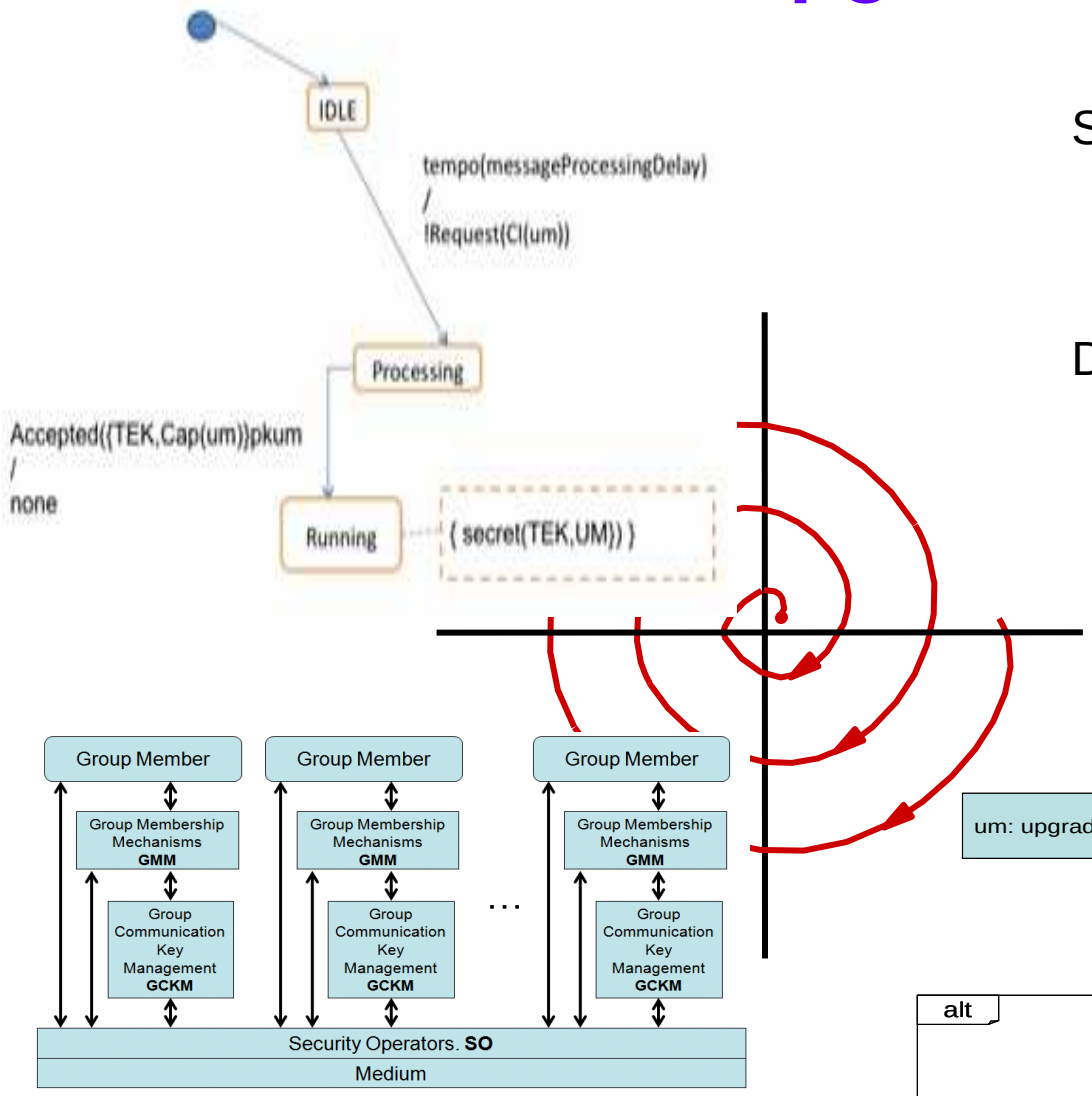
© Pierre de Saqui-Sannes, 2009

TURTLE : a Formal UML profile supported by TTool

Requirement capture	SysMLrequirement diagrams, chronograms
	Automatic synthesis of observers
Use-case driven analysis, scenarios	Rendezvous and FIFO, Time intervals
	Formal verification (RTL, CADP, UPPAL) Automatic synthesis of design diagrams
Object-oriented design Architecture , Behaviors	Object composition (process algebra) Synchronization actions, Time intervals
	Formal verification (RTL, CADP, UPPAL)
Rapid prototyping Components, deployment nodes	Java annotations
	Java and System C code generators

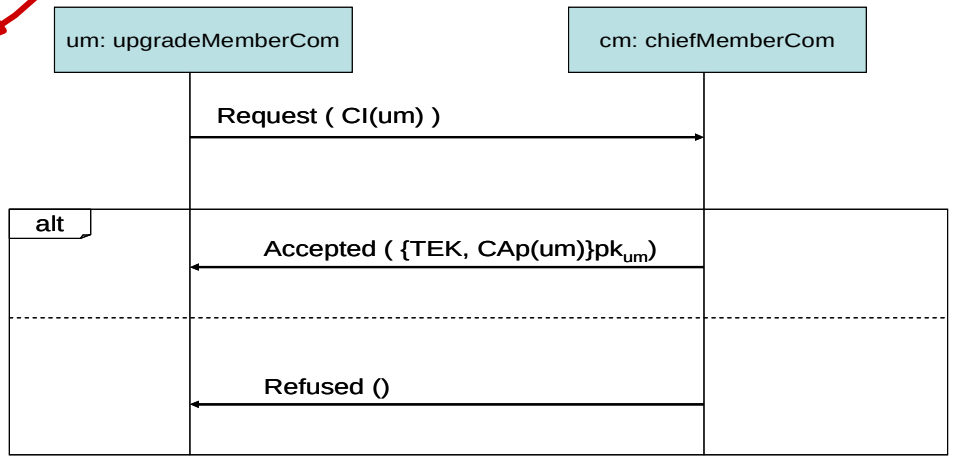
© Pierre de Saqui-Sannes, 2009

The Upgrade service



Security flaw
- Man in the Middle attack
- fixed

Does the system meet the deadline ?
- low rate PMR : no
  Forget it !
- medium rate PMR : yes
  1 requirement relaxed
  implement it !



© Pierre de Saqui-Sannes, 2009

Upgrade : Formal Verification

Requirement	**Limit duration** (ms)	**Upgrade protocol on average-rate network** (Execution time 331 ms)
Detecting an integrity violation	10 000	Widely validated
Detecting a replay	10 000	Widely validated
Accessing to a multimedia group	350	Shortly validated
Accessing to textual message groups	60 000	Very widely validated

© Pierre de Saqui-Sannes, 2009

Conclusions

- **A method for Secure Group Communication system design**
  - Requirement, analysis and design patterns
  - A verification-centric method
  - An annotated UML model with security and temporal requirements
- **SAFECAST : joint use of UML and formal verification tools**
  - UML has made communication among partners easier than expected
  - Acknowledged benefits of formal verification
    - Security flaws were detected and fixed (HLPSL, AVISPA)
    - Secured configurations were eliminated because of unmet deadlines (TURTLE, TTool and RTL)
    - EADS has saved development time
- **Future work**
  - The method is not restricted to SAFECAST system
  - Audio-video multicast streaming application within ad hoc networks
    - Quality of Service
  - TURTLE & network coding

© Pierre de Saqui-Sannes, 2009

Acknowledgements

SAFECAST partners

AVISPA developers

TTool developer