Simulation of AADL models of safety critical systems

Denis Buzdalov (buzdalov@ispras.ru)
Institute for System Programming of the Russian Academy of Sciences

ISPRAS

Modeling

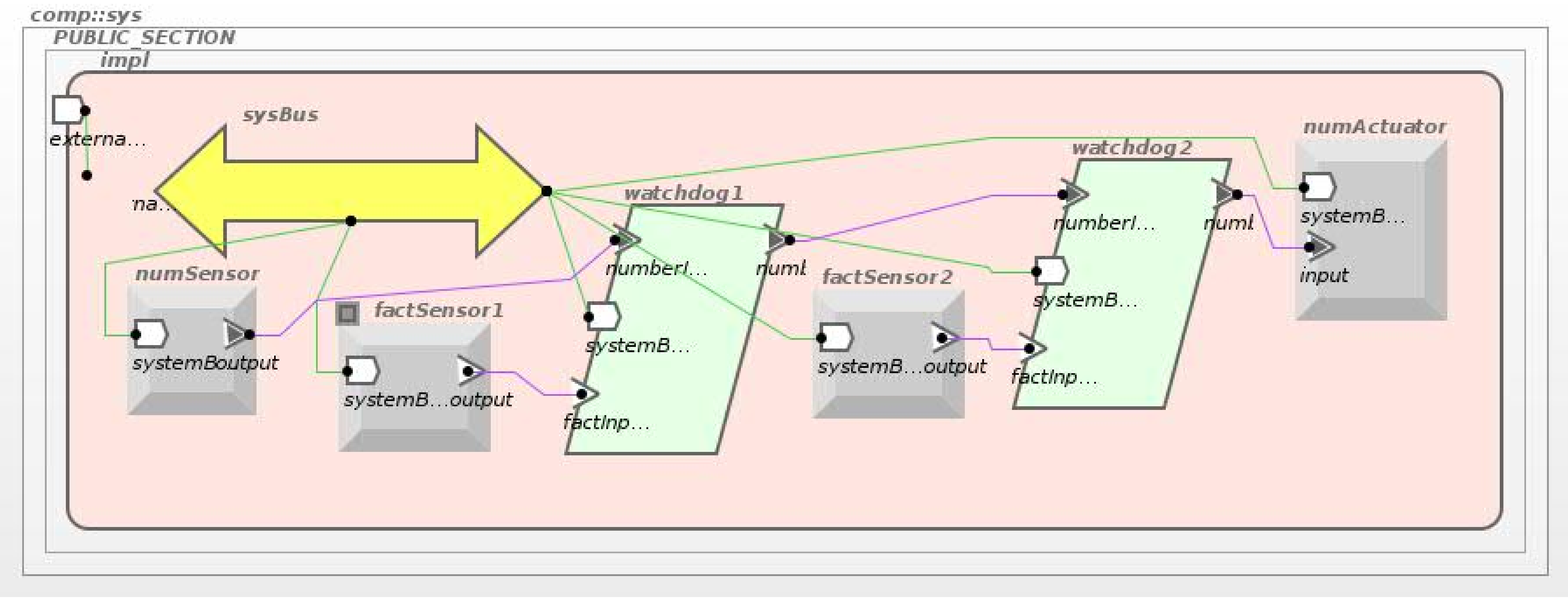
Modeling is used during development of *safety critical* systems. Special languages are used to describe models. AADL[1] is widely used in *avionics* (aviation electronics) development.

Aims

Developers of safety critical systems need to know whether developed system works as expected. Both *regular behaviour* and *failure management* of the system are considered.

Architecture Analysis and Design Language (AADL)

Here is a simple example of some system. Graphical AADL notation is used.
Both software and hardware parts of the system are represented.



Simulation

Simulation of model can help with analysis of a system under development. It can be used with partially given models or with abstract models of not fully developed system. This allows to find system building mistakes on early stages of development.

Problems

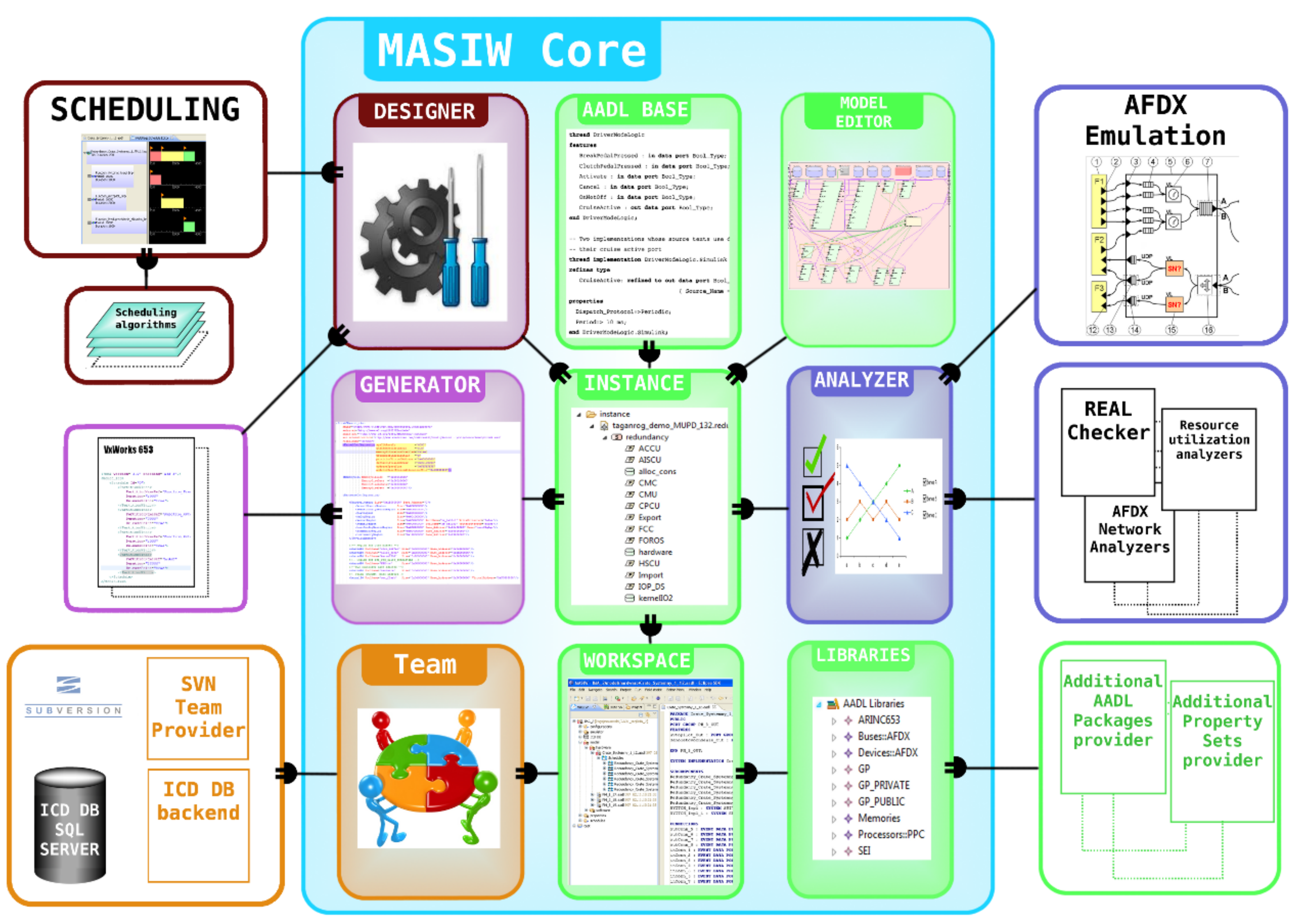
- Size of models can be really big.
- Behavior of system components can be very complex.
- Usage of analysis tool should be easy during development.
- Making a verdict by a system analysis should be clear and powerful.

Our solution

- Distributed simulation is used to manage the problem of models size. Model specific information is used for optimal job placement to minimize overhead.
- Any Java^{TM} code that fits special interface can be used to describe components' behavior. This approach allows to describe some components with non-trivial behavior and internal state (e.g. AFDX switch).
- Simulator was developed as a part of MASIW[2] project which includes tools for development and analysis of safety critical systems (especially, avionics systems).
- Aspect-oriented tracing of simulated system is used. This allows easy addition of new monitored characteristics without disturbing existing ones. Also, addition of new types of analysis of simulation results can be easily performed.

MASIW project structure

MASIW project is an environment for development and analysis of safety critical systems.



Future work

- The set of variants of components' behavior representation can be widened (e.g. probabilistic models support can be implemented).
- More useful simulation results analyzers can be implemented.
- Additional aspects of simulation traces can be developed and implemented.

References

[1] An SAE International Group. AS5506A: Architecture Analysis & Design Language (AADL)

[2] A. Khoroshilov, I. Koverninskiy, M. Olshanskiy, A. Petrenko and A. Ugnenko
Model-based Tool Chain For System Design and System Integration of IMA
In Proceedings of the International Space System Engineering Conference DASIA-2012