# Words of History, Bits of Advice

Steve Epstein
ABS Consulting
sepstein@absconsulting.com
SKYPE woodyep

21 years ago, risk software boldly stepped out to go where no risk software had gone before …

# … to the PC.

CAFTA, RISKMAN, Saphire, SETS, FTAP,
and NUPRA in a group photo, circa 1986

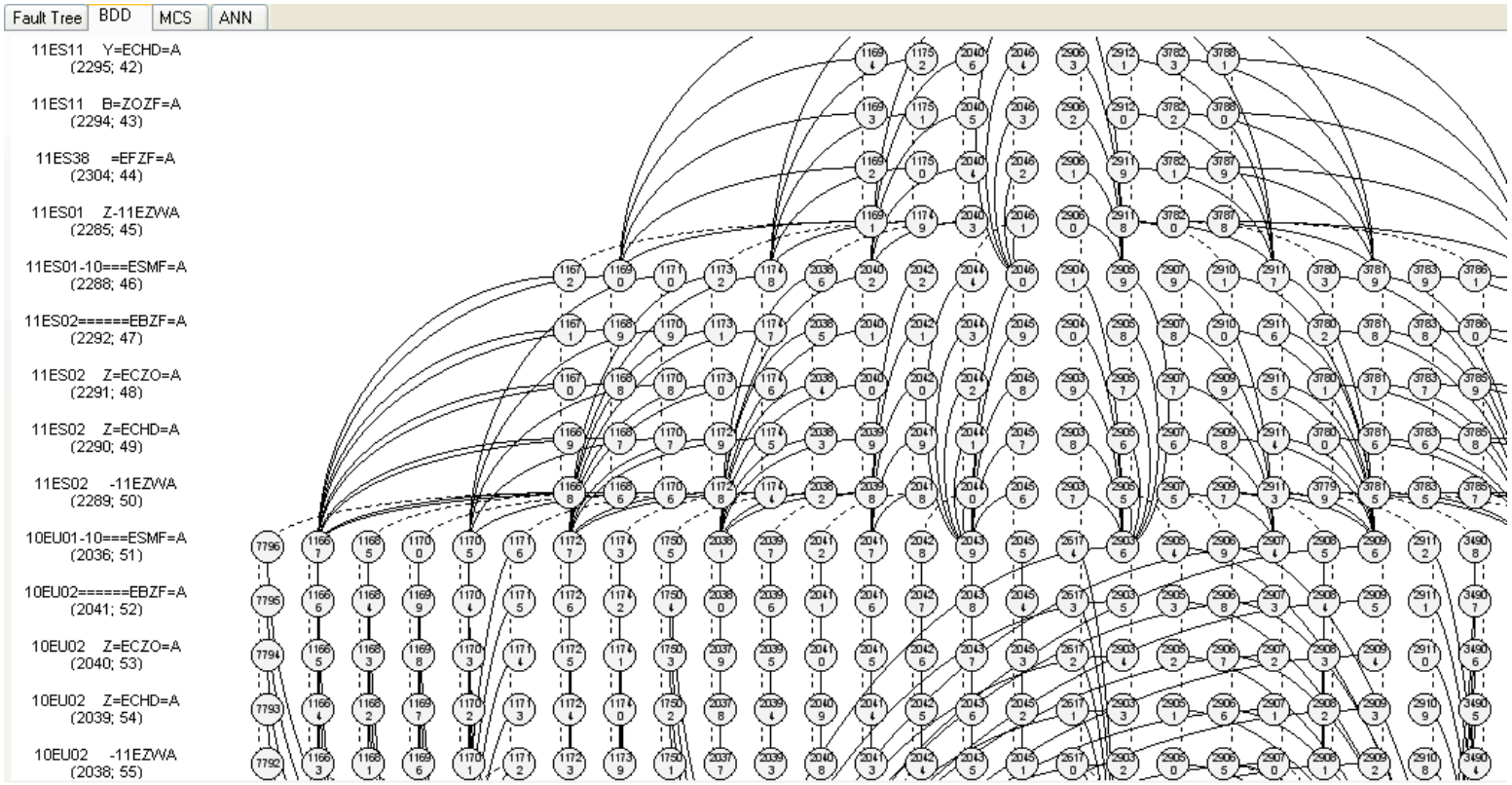
# … and over those 21 years, our abilities in and demands of PRA analysis has grown …

- Safety Monitors;
- Model size;
- On Line Maintenance;
- Risk Informed Applications
- Seismic, fire, BOP, and flood analyses;

… we have made strides in computer software as well…

# Alternative Data Structures
# Directed Acyclic Graph (DAG) and BDD

- BDD complexity is not related to the number of prime implicants of the encoded formula
- This small BDD (37620 nodes) encodes a total of $10^9$ cutsets



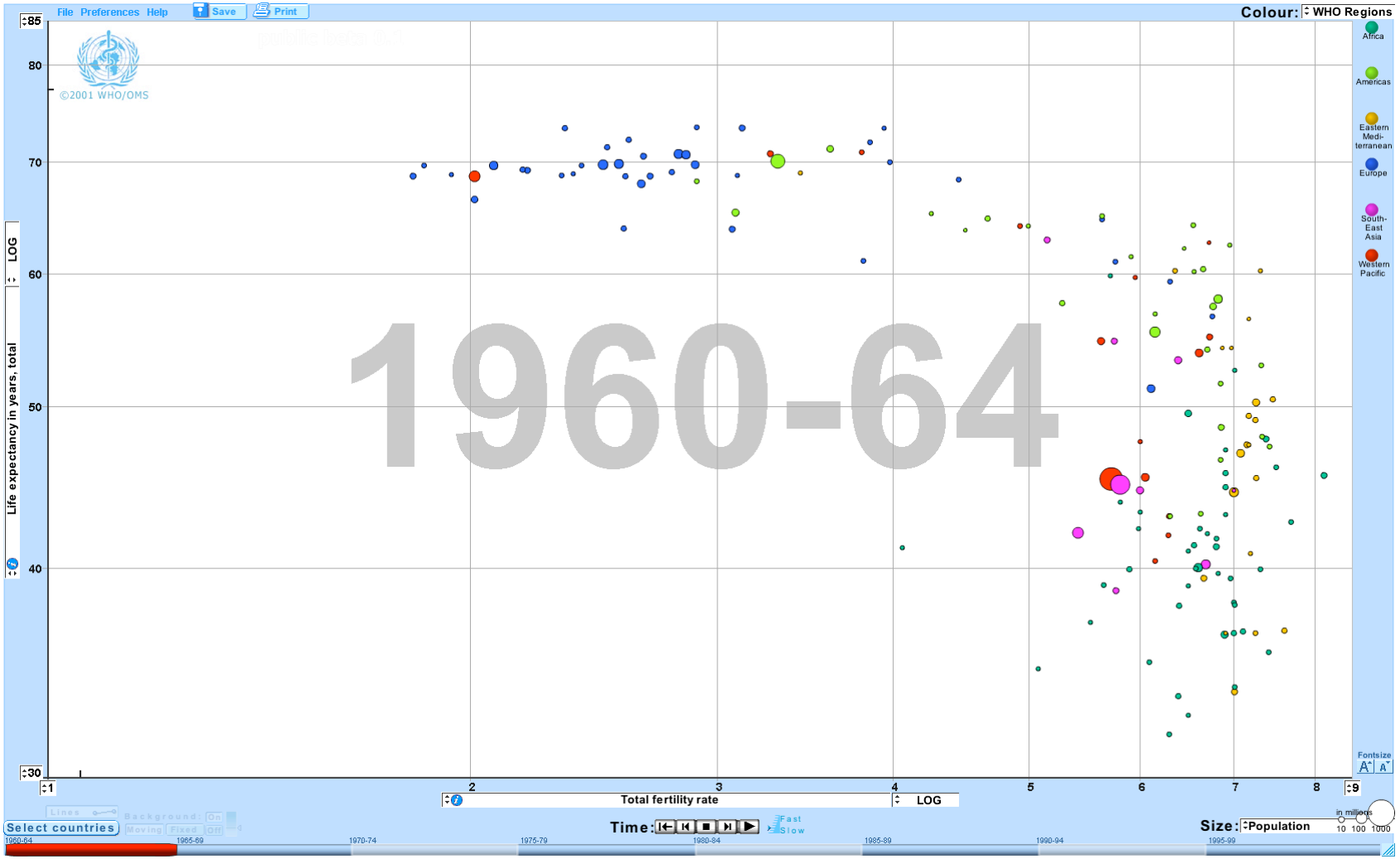
# Coding Breakthroughs

In a recent PhD thesis concerning nuclear PSA* large FT models could be solved analytically for >3000 basic events, with no truncation.

*** Analytical Solutions of Linked Fault Tree Models using Binary Decision Diagrams with Emphasis on Nuclear Probabilistic Risk Assessment**
**----------  Dr. Olivier Nusbaumer, 2007**

# … new ways of visualizing data

…



# But still these benefits are eluding us…

- Quality assurance of calculations;
- Less reliance on numerical approximations and truncation;
- Portability of the models between different software;
- Clarity of the models;
- Correct uncertainty and importance calculations;
- Assurance of model completeness;
- Enable specialized software to work with the same PRA model;
- Data and software backwards and forward compatibility;
- A universal format for industry data.

Here are some comments from the PRA Community on the current state of affairs and the future …

# … from a PRA Analyst …

"PRA software will need to handle **larger models, expanded in every direction: more initiators to address external hazards and to model internal events with more fidelity; larger fault trees and more basic events to model passive components and instrumentation; more system alignments to model closer to reality;** more systems that include normal controls and secondary supports; more operator actions and recovery; and more plant operating states including low power and shutdown. Capability includes not only the capacity to model increasing size but also **to solve the model within a reasonable time**."

# …from a vendor of PRA software

…

"We must concern ourselves with **accuracy** of calculations and the **proof** of such before concerning ourselves with speed. Remember, **good cooking takes the time it takes**. "

# … a comment from an analyst ...

PRA software must be constructed to assist PRA "owners", users, and reviewers in understanding of any aspect of the model, as well as the model as a whole. The PRA analyst-owner needs to understand the model construction so that modifications can be made to reflect the intended change without some unexpected impact on other parts of the model. **Somehow the entire model needs to be checked without relying entirely on cutset or sequence reviews**.

# … from another PRA software vendor …

"For a model to be transparent, model elements must be formally defined. This means that a formal grammar must be created, as well as a semantics. For example, **where are the common cause elements of a model, what are their names, which calculation model is expected**?"

# My Comment

"The plant models must be independent of calculation engines and modeling software in order to:

**Quality assure results;**

**insure model transparency;**

**eliminate single point software failure.**"

To get a handle on, and to try to solve some of these issues, we have heard some rumblings and discussions of

**PRA SOFTWARE**
**The Next Generation**

# The “This” Generation Software for PRA

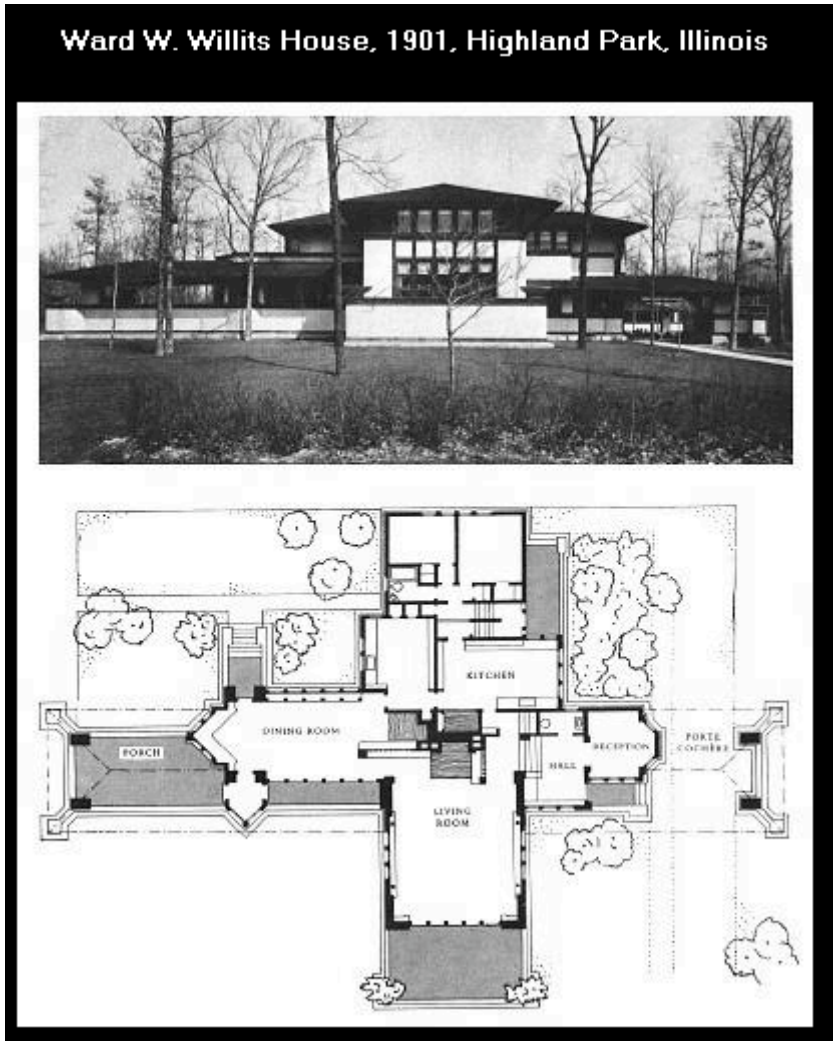
- What do we have now?
  - Risk applications like RISKMAN or CAFTA
  - Engines like ARALIA or FTRex
  - Models which are application dependent
- What do we want?
  - Deeper Calculation Capability
  - More Model Transparency
  - Tool Independence

So before beginning the "Next Generation" PRA Software (no matter how nice the vision …)

Looking at The Vision of the Next Generation PRA Software

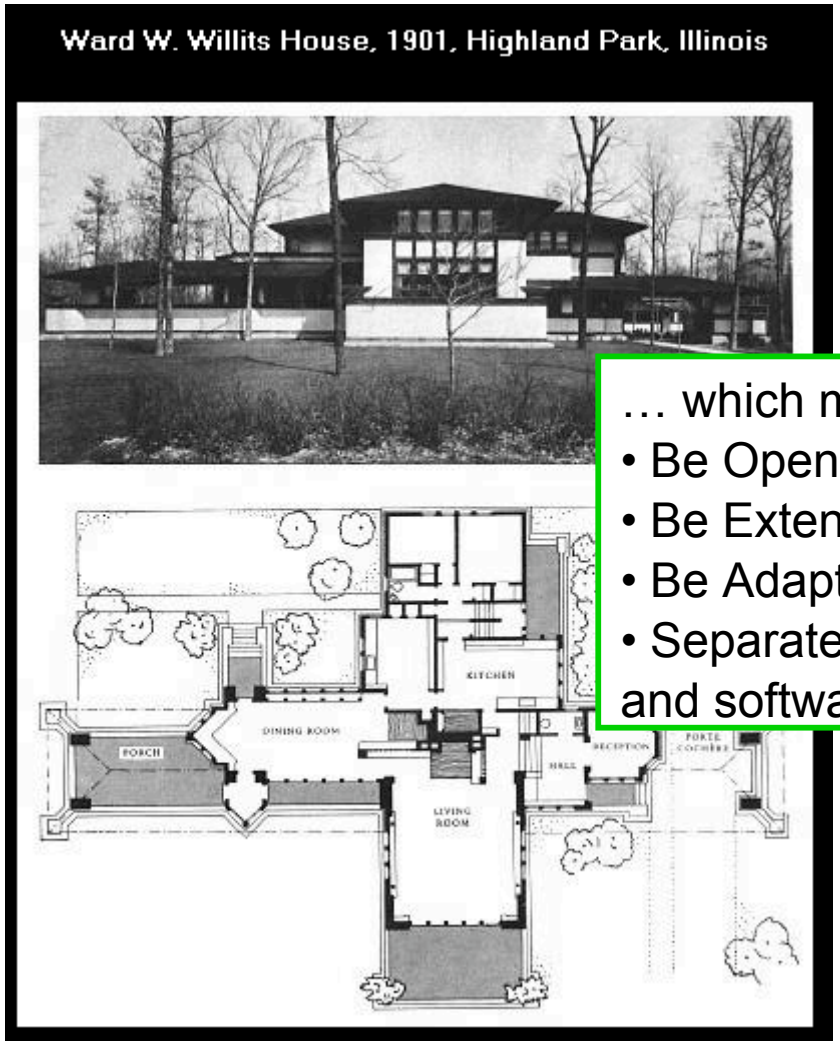
…we must create a Next Generation Software …

# ARCHITECTURE



…we must create a Next Generation Software …

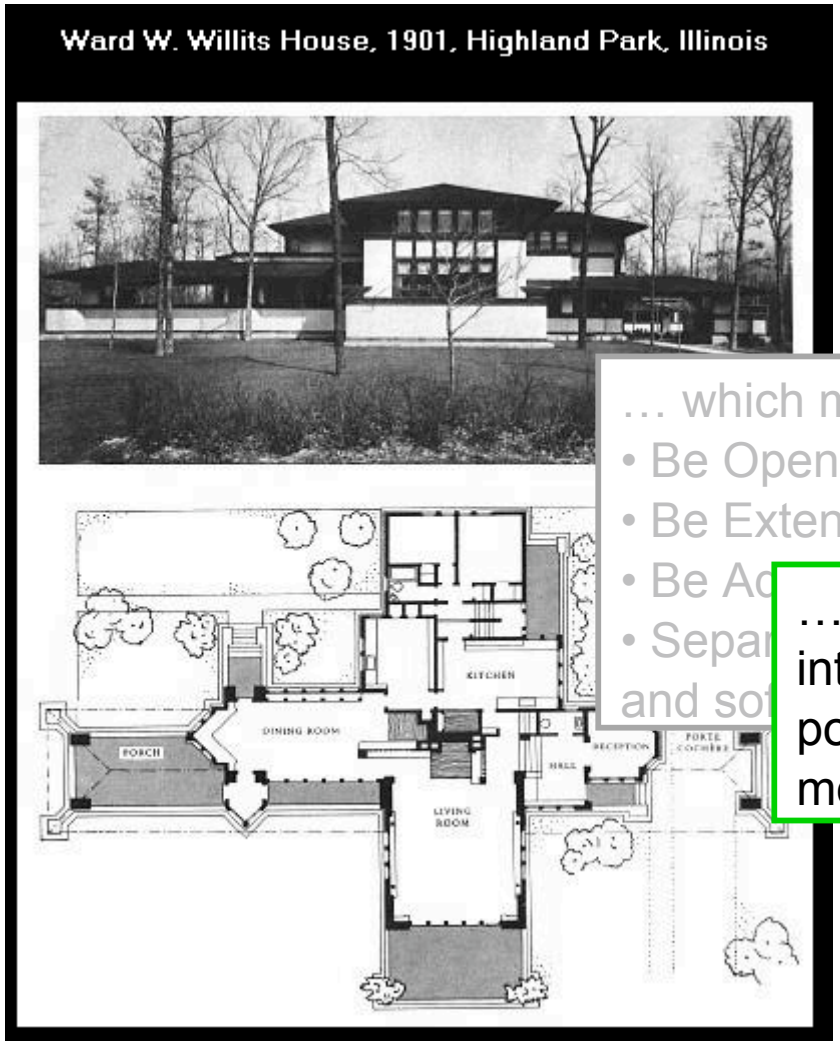
# ARCHITECTURE




… which must:
- Be Open
- Be Extensible
- Be Adaptable
- Separate data and software

…we must create a Next Generation Software …

# ARCHITECTURE




… which must:
- Be Open
- Be Extensible
- Be Ad
- Separ

and sof

… to allow the greatest inter-connectivity and portability between data, models and software.

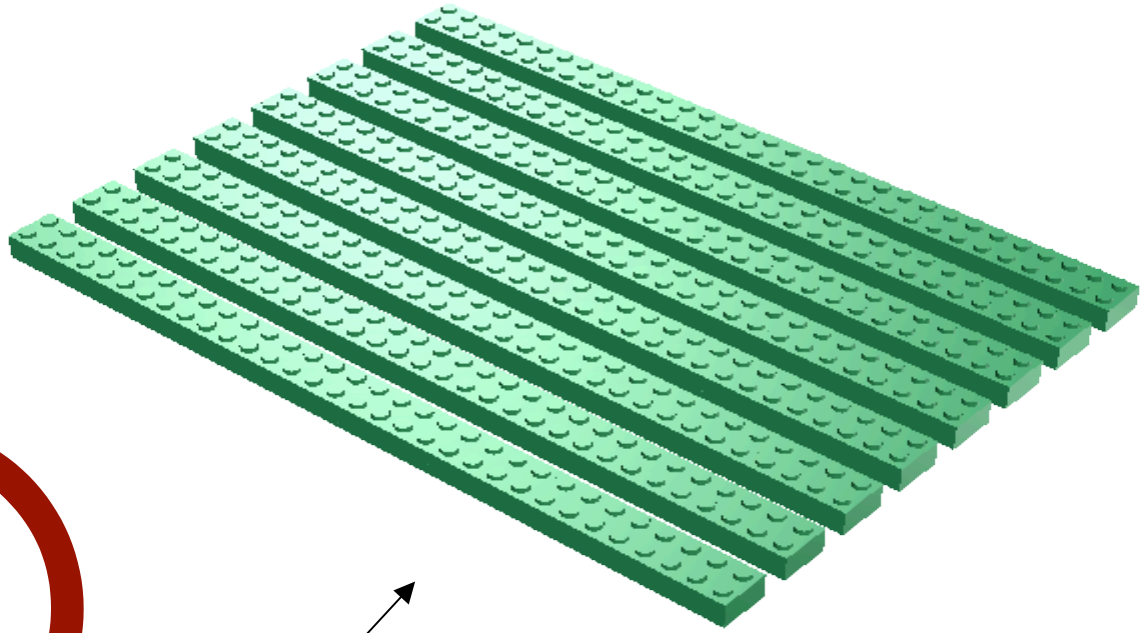
# Our Proposed PRA Software Architecture

- The foundation is a standard for representing a PRA model, therefore facilitating independence between model representations and software;
- Each risk application would generate a model in this standard from it's own internal representation;
- Viewers and calculation engines would interface with models via the standard representation.

**… but enough words, let's look at this like engineers …**

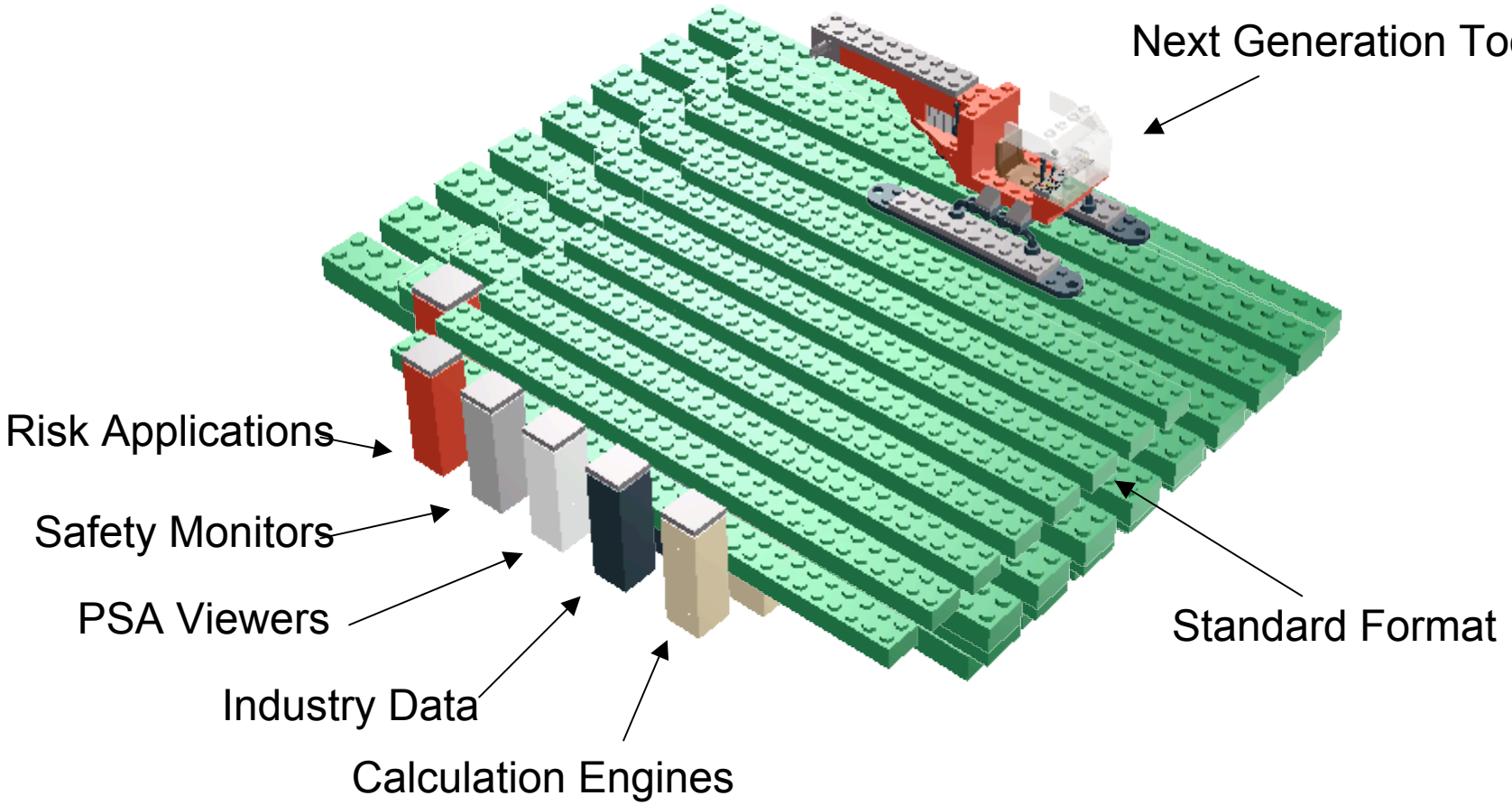
# The LEGO Model of the PRA Architecture

… first the foundation …

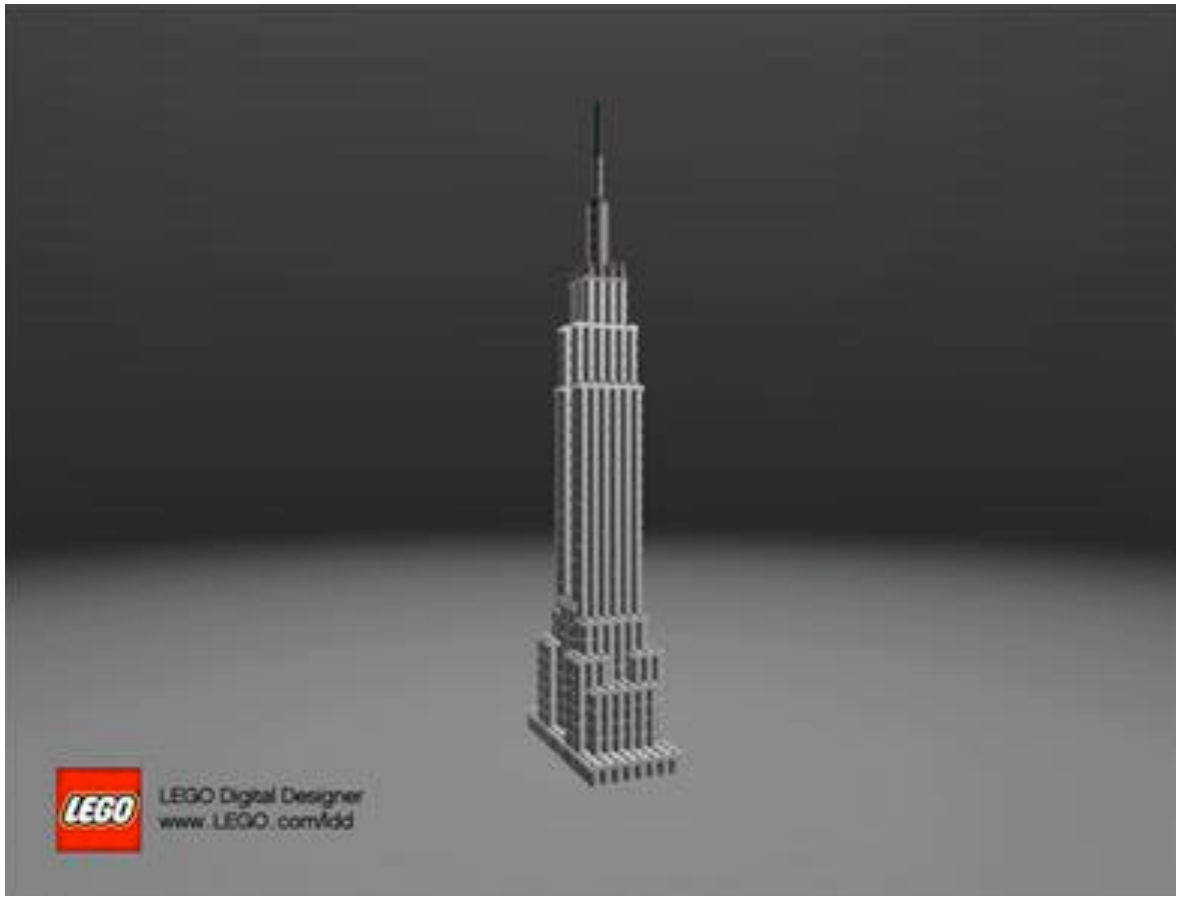


Standard Model Representation Format (SMRF)

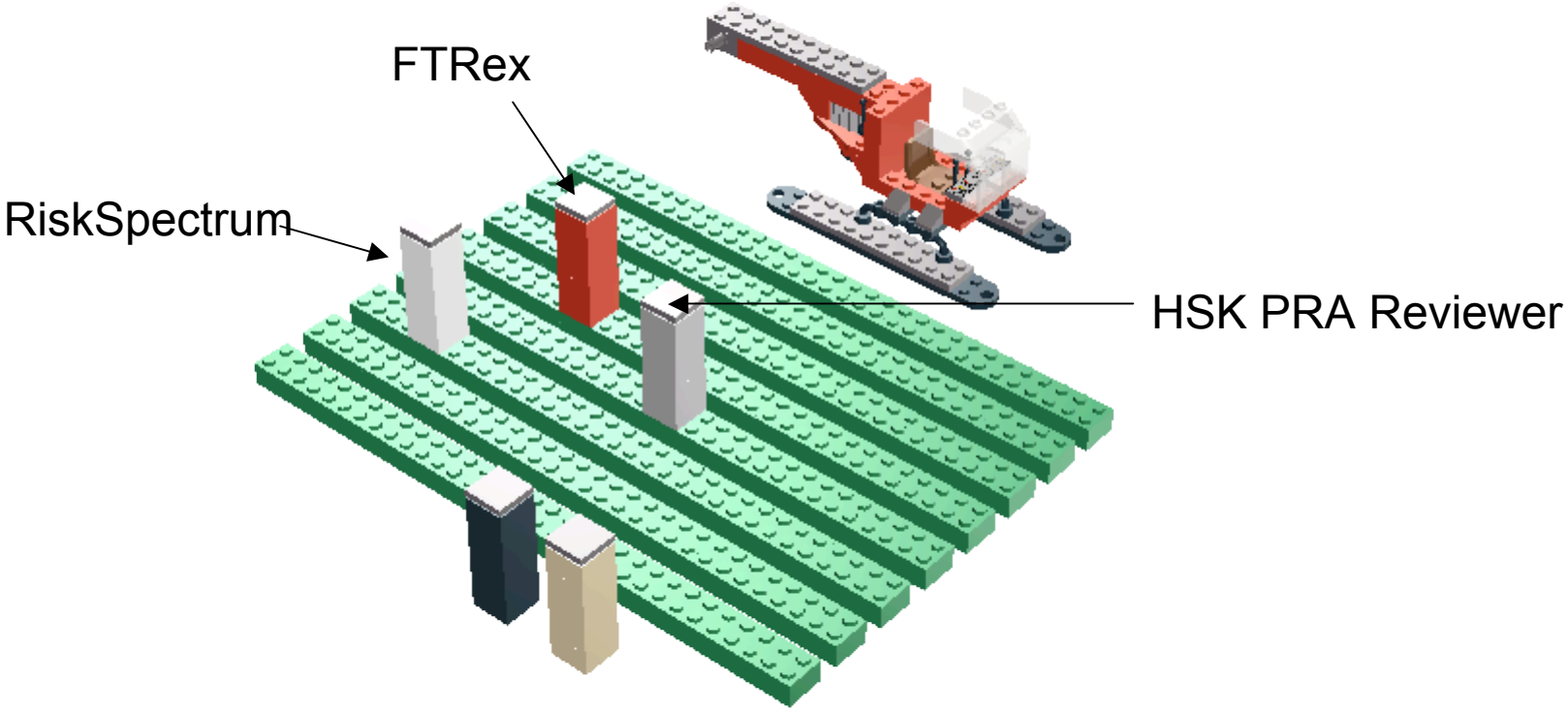
# … now assemble the risk applications and data .



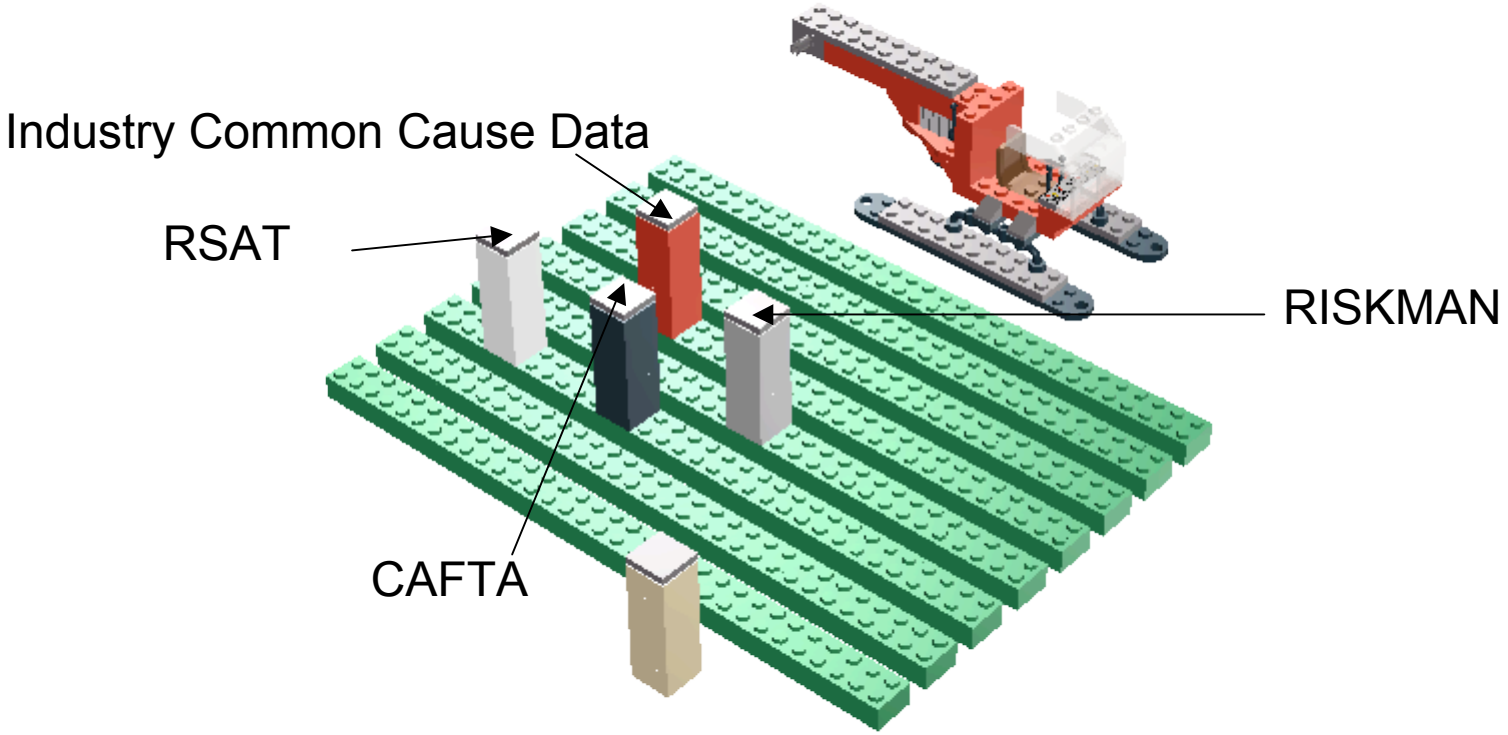
# … and then build upon the foundation …



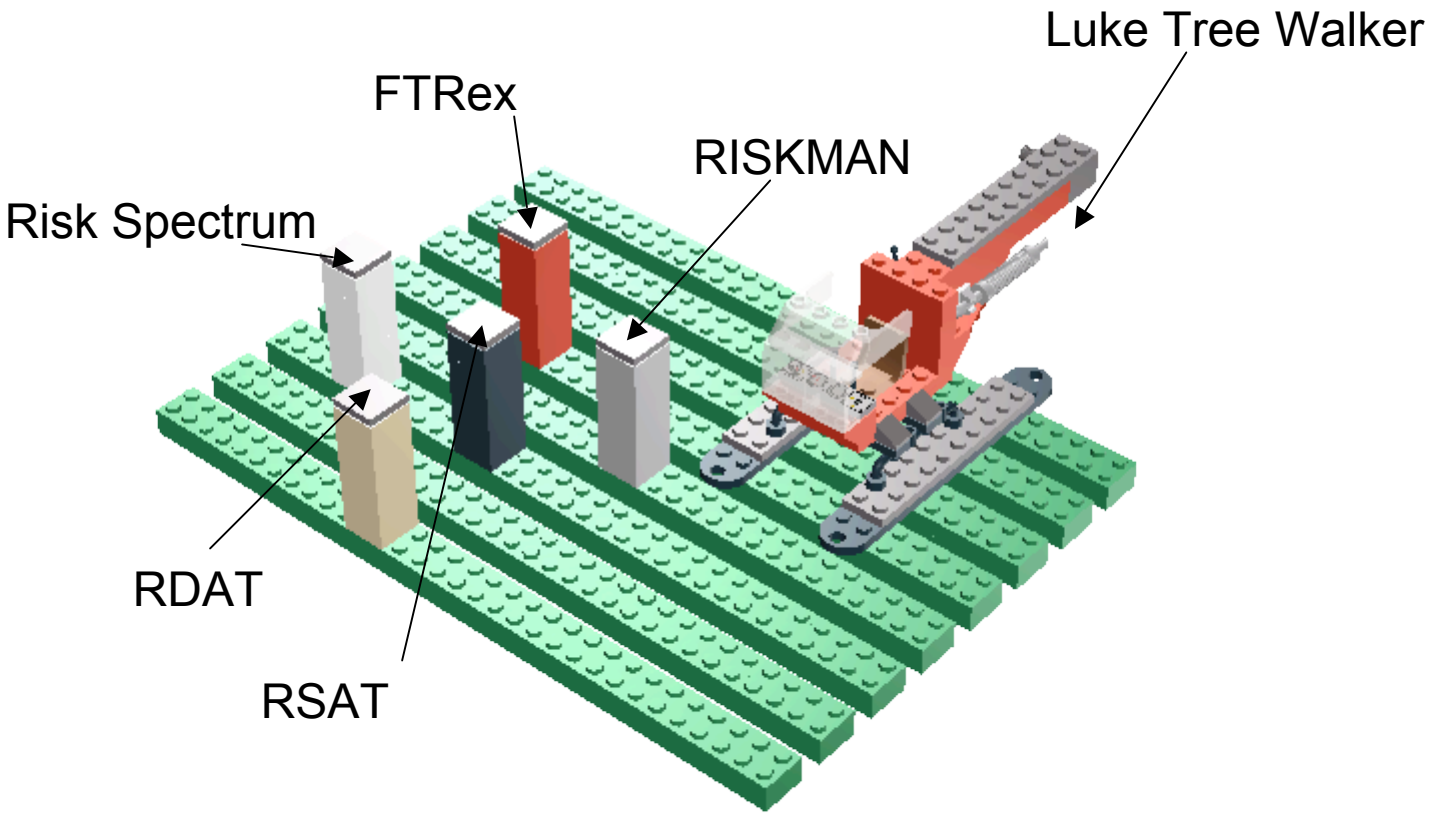
# … for example …



# … or this …



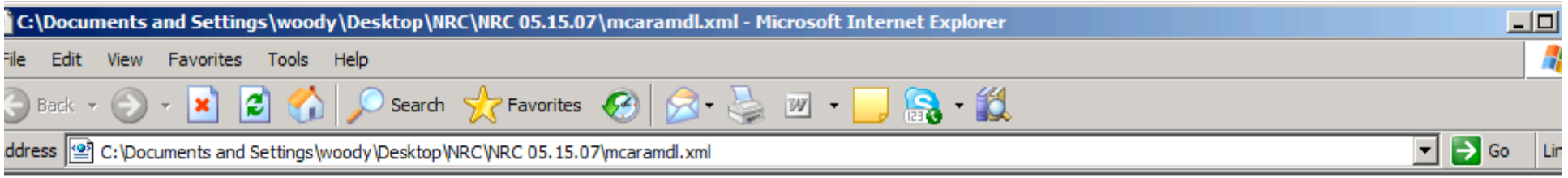
# … or even this …




… all interconnected through the foundation: a Standard Model Representation Forma

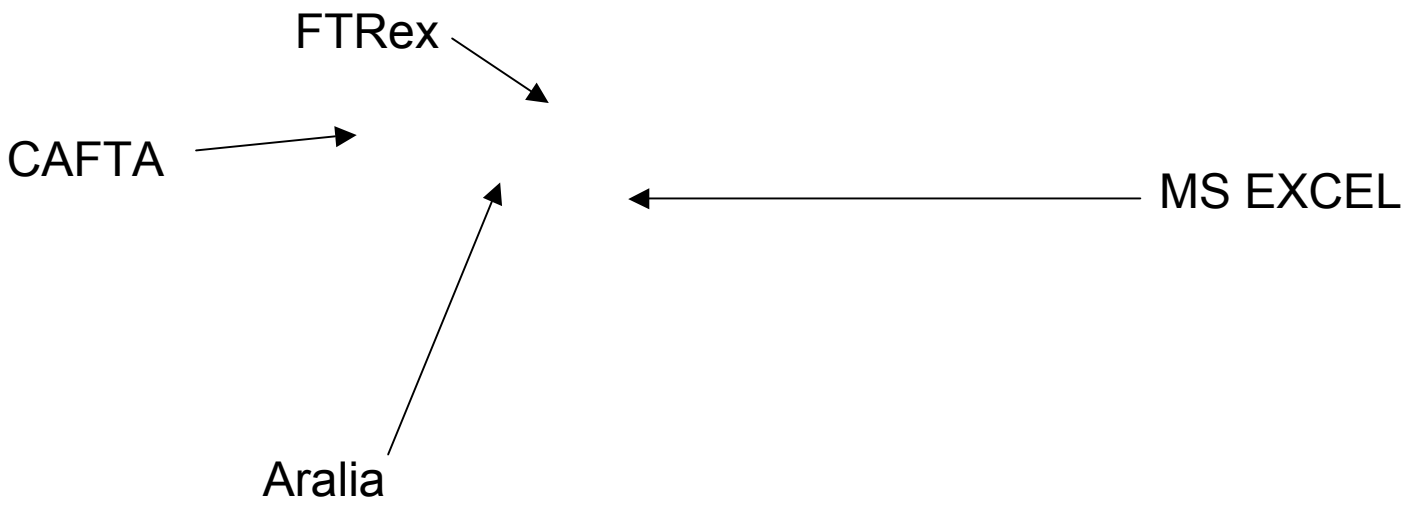
This is not just imagination.

We have actually used a prototype format like this in research and production.



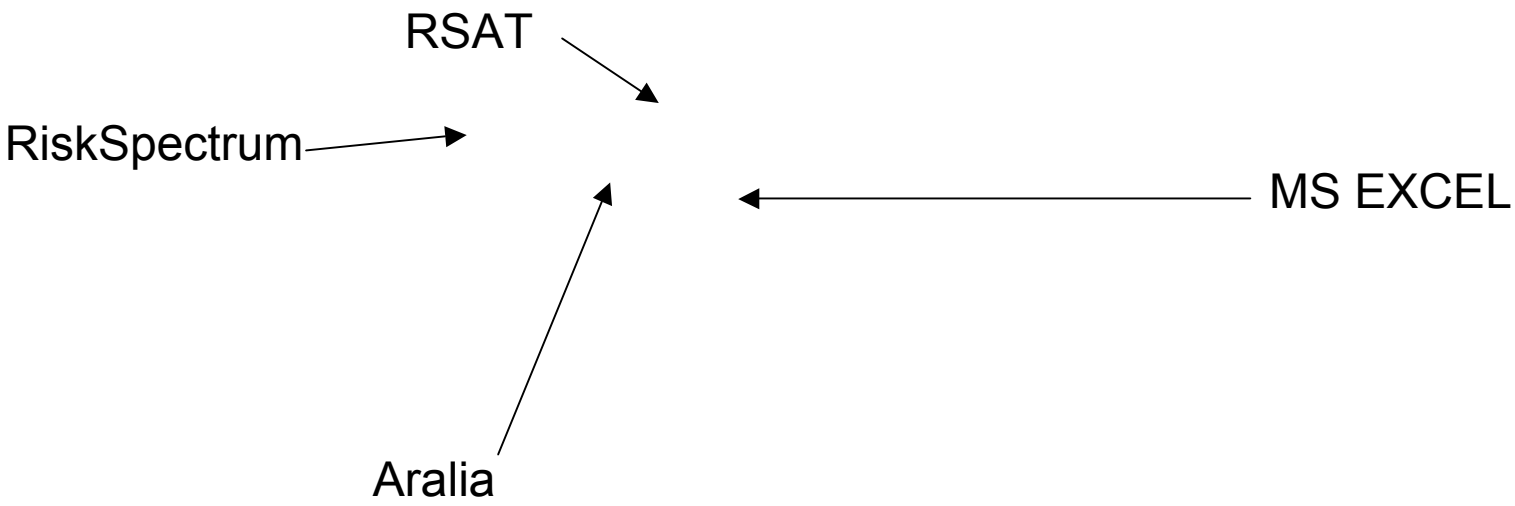

```
<?xml version="1.0" ?>
<!DOCTYPE riskman (View Source for full doctype...)>
- <riskman name="BU">
  - <faulttree topevent="BU">
      <!-- The Fault Tree -->
    - <gate name="BU" type="or">
        <fanin name="G00MAB" />
        <fanin name="G00MDB" />
        <fanin name="CHECKV4FTO" />
      </gate>
    - <gate name="G00MAB" type="or">
        <fanin name="TANKRUP" />
        <fanin name="MANUALVTC" />
        <fanin name="CHECKV3FTO" />
      </gate>
    - <gate name="G00MDB" type="and">
        <fanin name="G00MDC" />
        <fanin name="G00MJC" />
      </gate>
    - <gate name="G00MDC" type="or">
        <fanin name="MDPUMP1FTR" />
        <fanin name="MDPUMP1FTS" />
        <fanin name="CHECKV1FTO" />
        <fanin name="MOVALVE1FTO" />
        <fanin name="HETEST1" />
        <fanin name="G00MGD" />
      </gate>
    - <gate name="G00MGD" type="and">
        <fanin name="G00MGE" />
        <fanin name="CHECKV2FTR" />
      </gate>
    - <gate name="G00MGE" type="or">
        <fanin name="MDPUMP2FTR" />
        <fanin name="MDPUMP2FTS" />
      </gate>
    - <gate name="G00MJC" type="or">
        <fanin name="MDPUMP2FTR" />
```

# Example #1



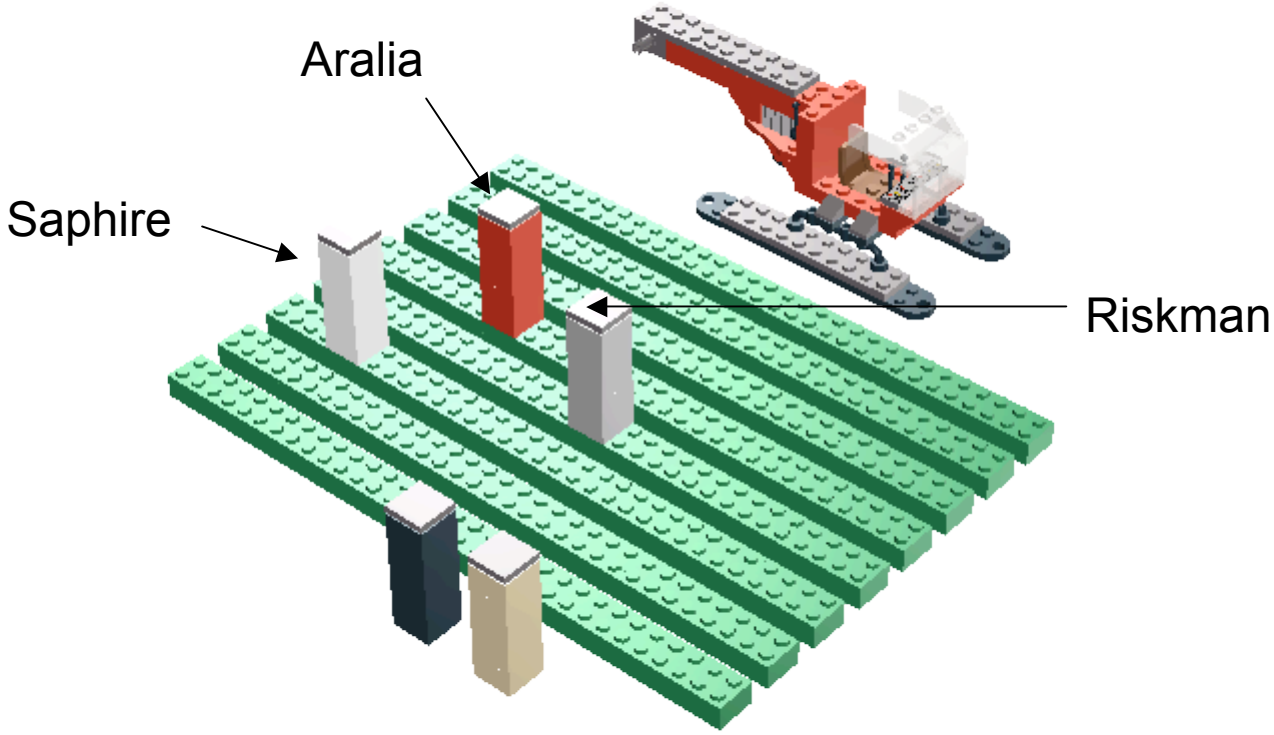

Three different CAFTA models from three different US organizations.

# Example #2



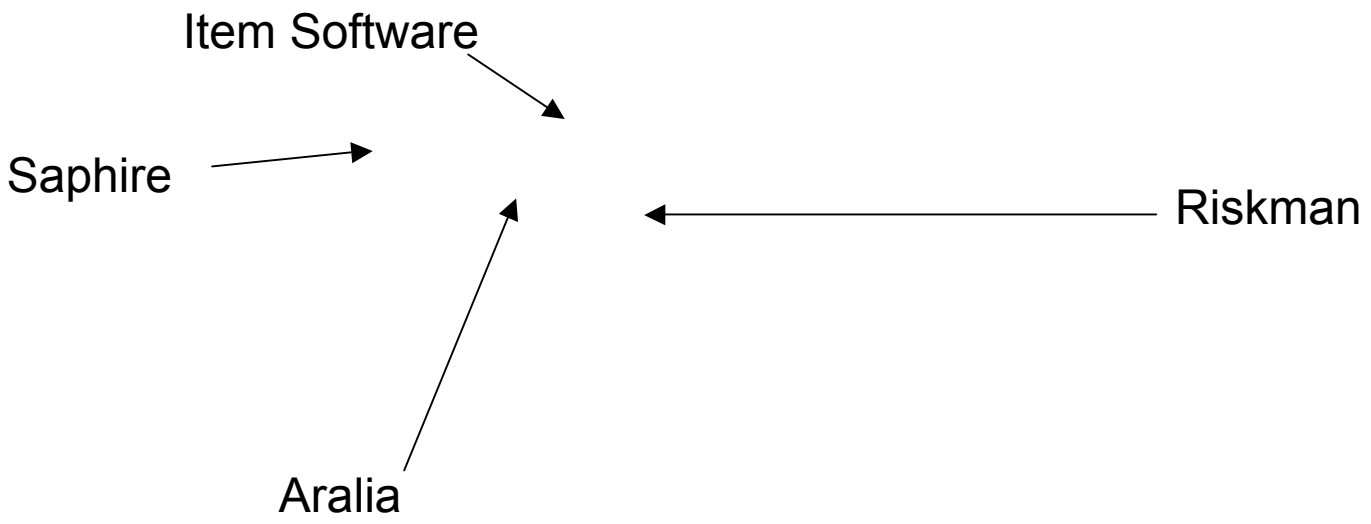

A Japanese core damage model solved exactly with BDD.

# Example #3

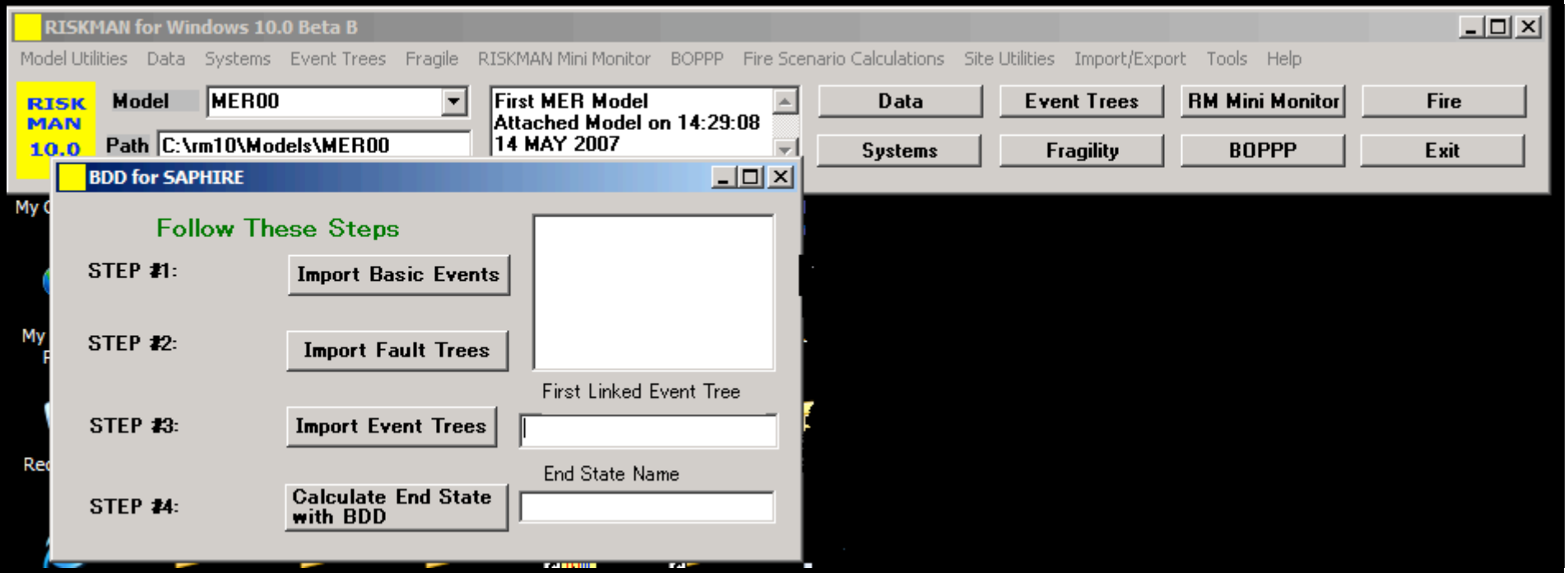



An investigation of a SPAR model.

# Example #4




A sanity check on the MER PRA done by NASA.




# Interface built for MER Sanity Check

# So what are we doing to bring these benefits into existence?

- Quality assurance of calculations;
- No need to rely on numerical approximations and truncation;
- Portability of the models between different software;
- Clarity of the models;
- Correct uncertainty and importance calculations;
- Assurance of model completeness;
- Enable specialized software to work with the same PRA model;
- Data and software backwards and forward compatibility;
- A universal format for industry data.

ABS Consulting

# Workshop Announcement

## Next Generation PSA Software, Declarative Modeling, and Model Representation Standards

June 12th, 2007

Kernkraftwerk Gösgen-Daeniken, Switzerland

**Call for Participation:** To meet and discuss efforts, visions, and future needs with regards to software, PSA analysts, and model representations in large, safety critical PSA. All attendees are encouraged to present ideas, work-in-progress, research, and production systems, especially in the following areas:

- Quantification Methods;
- User Interfaces;
- Declarative Modeling;
- Standard Model Representations;
- PSA Visualization;
- PSA Software Architectures;
- New Algorithms;
- Modeling Styles and their Effects on Clarity and Quantification;
- PSA Software Verification, Benchmarks, and Quality Assurance.

**How to Participate:** Please fill out the attached form and eMail to Steve Epstein at sepstein@absconsulting.com as soon as possible. Please put the word "Workshop" in the subject line. We will make every effort to make time for anyone who wants to talk, make a presentation, or make a demonstration. We would like to make this an open forum for the exchange of ideas.

**Organizers:** This workshop is organized by ABS Consulting, ARBoost Technologies, and hosted by Kernkraftwerk Gösgen. Please do not hesitate to contact any of the following members of the organizing committee if you have any questions:


| | |
|---|---|
| Steve Epstein | sepstein@absconsulting.com |
| Antoine Rauzy | Antoine.rauzy@arboost.com |
| Don Wakefield | dwakefield@absconsulting.com |

# A Standard PSA Model Representation Format
## Scope and Needs Statement for ASME

**Scope:** We propose that an independent international standard format be created to represent computerized PSA models and industry data in digital fiorm . We propose that an ASM E subgroup be created to (1) create a prototype S tandard Model Representation Format (**SMRF**), (2) present examples in the prototype format, and (3) deliver a report as to the efficacy of the prototype in addressing the "Needs" statement, below.

**Needs :** O ver the last 5 years, new calculation techniques, such as BDD, have been extensively studied in nuclear PSA , and research efforts made in the direction of "next generation" PSA software and "declarative modeling", which try to present a more informative vi ew of the actual systems, components, and interactions which the model represents.

The concern of these studies has been to end the use of approximations: numerical approximations for which we do not know the error factors, and modeling approximations whi ch leave out perhaps critical elements of the actual plant.

From all these investigations, some alarming issues related to large nuclear PSA models have been raised, which we feel need to be addressed before we put new calculation engines or next genera tion user interfaces into place. We believe that to address these issues enumerated below, a **SMRF** for PSA models, a representation which is independent of all PSA software, must be in place. Each software would retain their own internal representation for a model; but each software would also be able to share models and industry data by means of the SMRF .

1. **Quality assurance of calculations:** at the moment, a model built with one software, such as CAFTA, cannot be simply quantified with another software, such as SAPHIRE or RiskSpectrum, and visa versa; there are too many software dependent features used by modelers to make inter -calculation comparisons a one -step process. A standard representation will allow models to be quantified by several calculation engin es, therefore quality assuring results in a strong way.

2. **Over reliance on numerical approximations and truncation:** while this cannot be solved directly by a standard representation, as new calculation engines are completed, a standard representation will allow new engines to be snapped into new (or existing) user interfaces without changing the model or user interface software.

3. **Portability of the models between different software:** at the moment, models are essentially non -portable between calculation engi nes, as pointed out above. We would like to emphasize here that a standard representation would allow complete, whole models to be shared right now between software; the onus will be on each software to correctly interpret the model representation. We ha ve

# ASME Proposal

## Create an Open Standards Working Group

- make a preliminary design for a PRA software architecture;
- create a declarative modeling grammar;
- choose a model representation format;
- use the grammar and representation to define a standard model format;
- show examples with large existing PRAs.

# What we can do NOW

## A Test Case of the Idea

- KKL uses RiskSpectrum;
- NOK uses Riskman;
- HSK would like to review easily both model types;
- create a prototype representation format;
- create model closures using the format;
- attempt to exchange models using the format.

# Risk Software Institute

- Standard Model Format guardians;
- not for profit;
- quantification research and verification;
- measure degree of standardization;
    - software
    - models
- third party software testing;
- third party benchmarking;
- member financed;
- manpower support from industry;
- internships for universities.