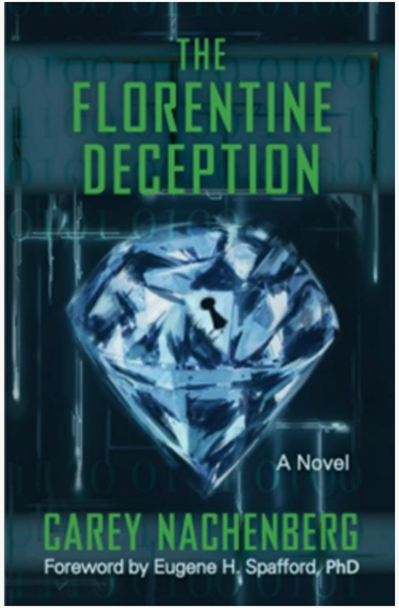
Academic excellence for business and the professions

Probabilistic modelling of cyber threats in Cyber-physical systems

Peter Popov,
Centre for Software Reliability
City, University of London, United Kingdom

18 May 2017
CricTechs seminar, KhAI, Ukraine

Separating Science Fantasy from Science facts



"If there's one disadvantage to spending more than a quarter of a century in security, it's that you become hypersensitised to ***mangled terminology and fantasy passed off as current science****"*

David Harley, Senior Research Fellow, ESET

Cyber Security Facts

- Computer systems, especially cyber-physical systems, are **complex**, and their complexity will only continue to increase.
- **Absolute cyber security is unattainable**.
- Cyber systems intended to be secure must **operate through attacks.**
- Protect the best you can, but realize that **perfect protection is impossible, so <u>resilience</u>** can only be achieved **through tolerating attacks**
  - This, in turn, **may require online detection and response**.
- **Assessment** of the “amount” of security that a particular approach to resilience provides **is essential**.
  - Even if assumptions are made that are ***difficult to justify***

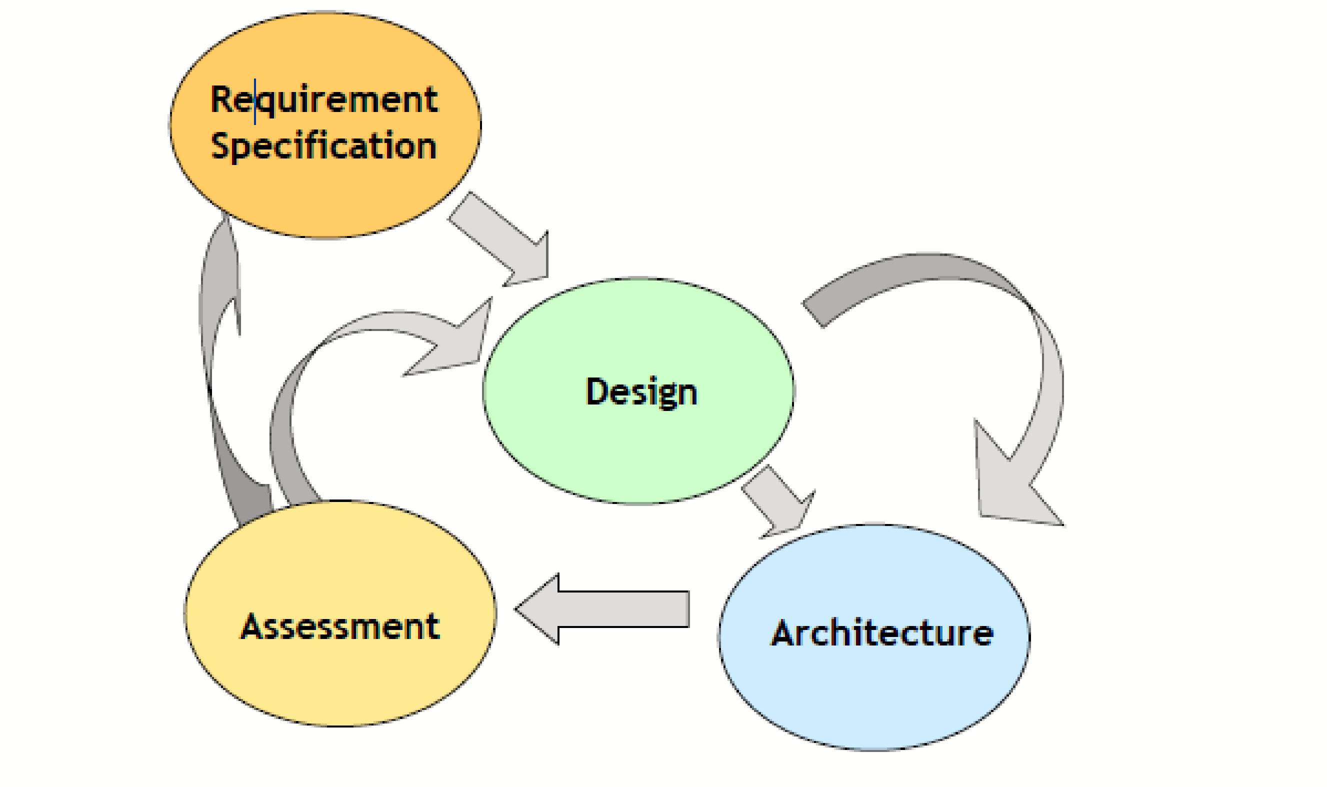
- **Perfect cyber security is science fantasy, and perfection is the <u>enemy</u> of good.**

What is needed?

Assured Trustworthy System Operation in Hostile Environments

- **Trustworthy operation**
  - System does what it is supposed to do and nothing else.
  - Requirements are met – Reliability/Availability, Security, Safety (when applicable), Performance, etc.
- **Tolerate (to a degree) a hostile environment**
  - Accidental failures, Design flaws, malicious cyber attacks.
  - Consider the cyber, physical and social aspects
- **Provide assurance through assessment**
  - Provide justification (evidence, argument) that the system is ***fit for purpose***, remaining risks are acceptable for ***anticipated environment***
  - Compare design alternatives and choose the most resilient (trustworthy) system design.
    - This must be done *before* the system is deployed and ***continuously reviewed***.

Engineering for resilience



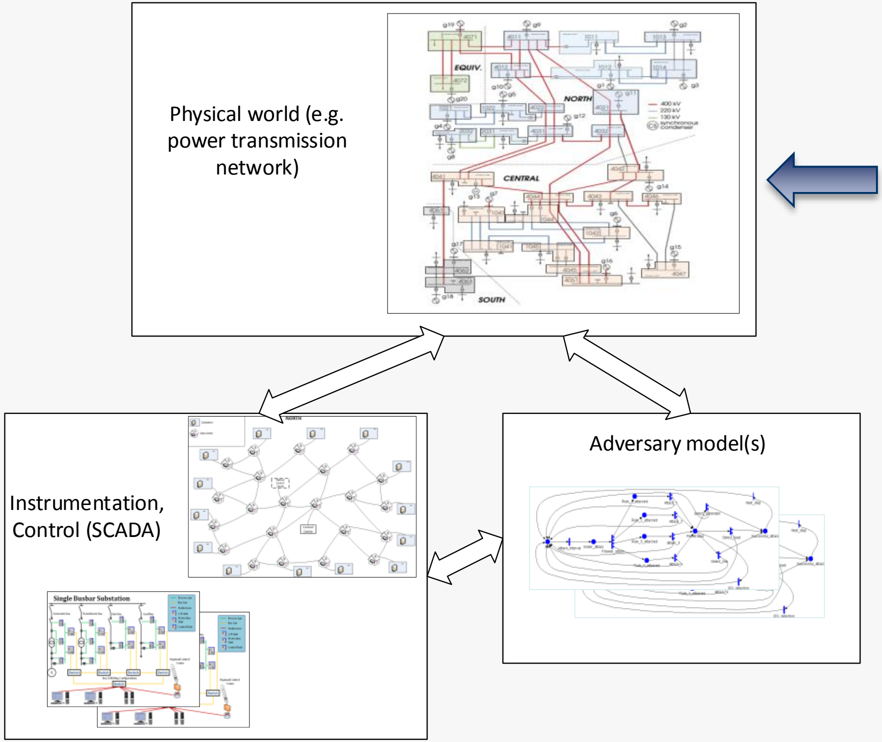
Sabbatical Leave: Oct 2016 – Sept 2017

- Visits of US with the financial support from UK GCHQ
  - Duke University (Prof Kishor Trivedi)
    - A recognized authority in solving ***Markov chains*** (CTMC) and semi-Markov processes. Invented Stochastic Petri Nets, etc.

  - University of Illinois at Urbana-Champaign (Prof Bill Sanders)
    - A recognized authority in ***model-based assessment*** (performance, reliability, security). Creator of the popular stochastic modelling tool, Mobius.

  - Johns Hopkins University (Prof Yair Amir)
    - A recognized authority in distributed systems, especially in ***protocol for reliable communication*** (reliable multicast, Byzantine agreement protocols, etc.) Created popular tools for reliable communication such as Spread and Spines overlay.

Duke University: Efficient solution for complex hybrid models



For several years now with my group we have worked with a model of NORDIC – 32, a power transmission network, extended with instrumentation, compliant with IEC 61850.

I reported on this work in previous visits to DESSERT (in 2014).

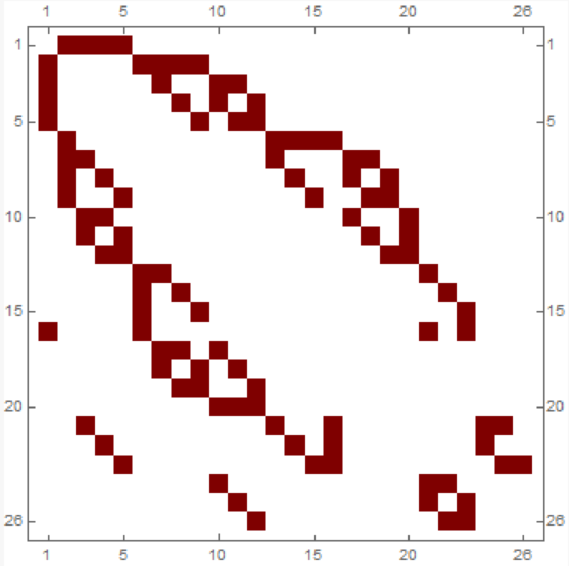
- A complex hybrid model (probabilistic and deterministic) including models of Adversary attacking the assets of transmission network.

Efficient solution for complex *hybrid* models

- Looked at various extensions of Petri nets (e.g. fluid Petri nets) to deal with *continuous* state space.
- Looked at ways of speeding up simulations:
  - It turned out that deterministic models (power-flows calculations including the optimal load shedding, ***optimal power-flow*** (OPF)) take more than 90% of simulation time;
  - Caching the OPF results led to ***dramatic reduction of simulation time***
- Looked at ***truncation of the state space*** (really very large without truncation, $\sim 2^{1500}$)
  - Limiting the number of simultaneous accidental failures
  - The effect of deterministic models was captured.
    - a set of elements might be ***switched off*** (disconnected elements ***cannot fail*** until reconnected again)
    - Transition probability matrix affected by switching-off of components.

Efficient solution (2)

- Currently we are working on a numeric ***transient availability solution*** of NORDIC-32 power sub-system.
- Below is an illustration from a ***feasibility study***.



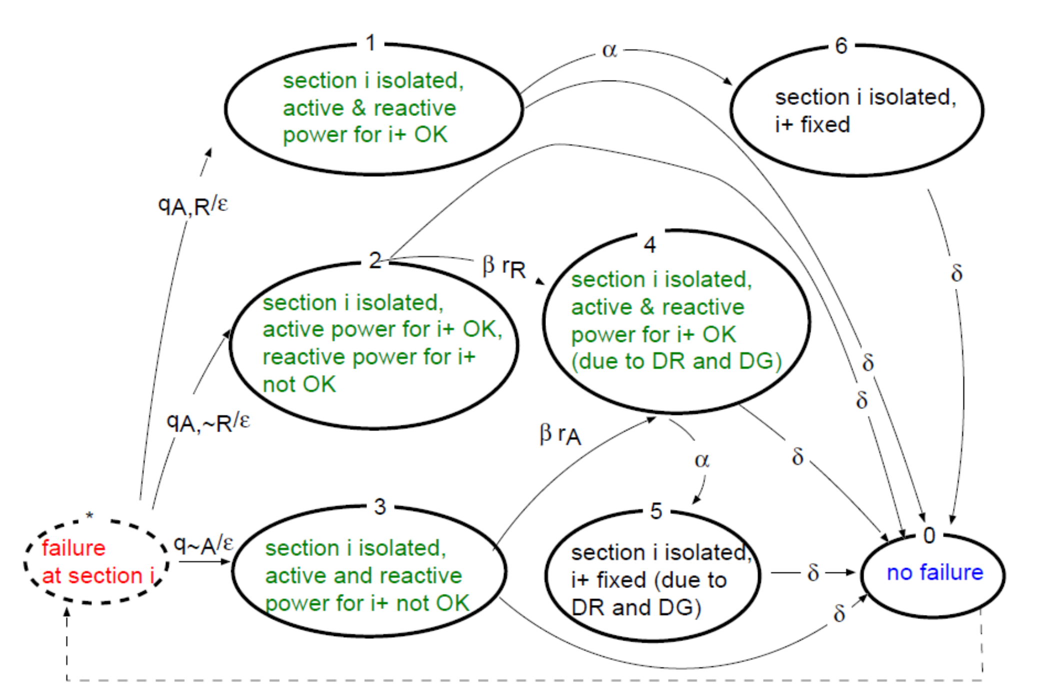
$$\begin{pmatrix}
0 & \lambda_1 & \lambda_3 & \lambda_4 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\leftarrow\mu_1 & 0 & 0 & 0 & 0 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\leftarrow\mu_3 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & \lambda_4 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\leftarrow\mu_4 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & \lambda_3 & 0 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\leftarrow\mu_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & \lambda_3 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & \lambda_4 & \lambda_5 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \leftarrow\mu_3 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & 0 & \lambda_4 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \leftarrow\mu_4 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & \lambda_3 & 0 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \leftarrow\mu_5 & 0 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & \lambda_3 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \leftarrow\mu_4 & \leftarrow\mu_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & \lambda_5 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \leftarrow\mu_5 & 0 & \leftarrow\mu_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \leftarrow\mu_5 & \leftarrow\mu_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & \lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \leftarrow\mu_3 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \leftarrow\mu_4 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 \\
\leftarrow\mu_2 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & 0 & \lambda_5 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_4 & \leftarrow\mu_3 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & 0 & \leftarrow\mu_3 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & \leftarrow\mu_4 & 0 & 0 & \leftarrow\mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & \leftarrow\mu_4 & \leftarrow\mu_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & \leftarrow\mu_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_4 & \lambda_5 & 0 \\
0 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & \leftarrow\mu_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & 0 & 0 \\
0 & 0 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & \leftarrow\mu_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & \lambda_4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_4 & \leftarrow\mu_3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & 0 & \leftarrow\mu_3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \leftarrow\mu_5 & \leftarrow\mu_4 & 0 & 0 & 0
\end{pmatrix}$$

Efficient solution (3)

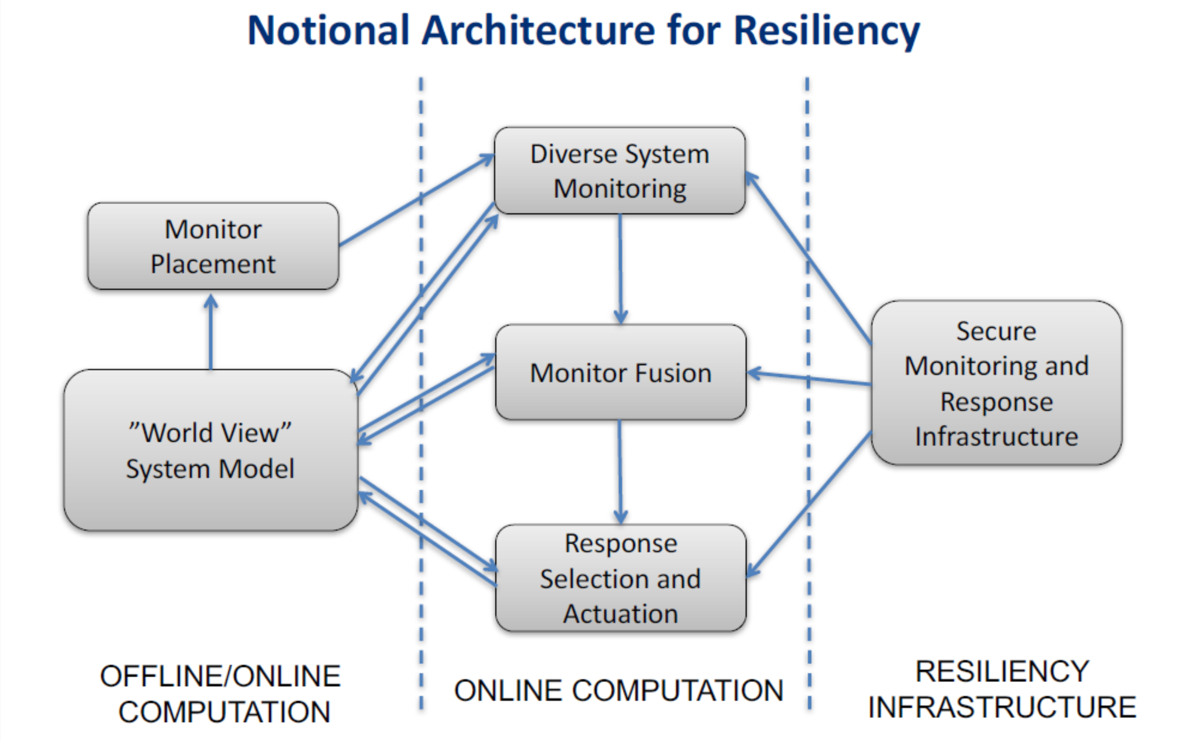
- Transient solution seems feasible if the state space is truncated to 3 or even 4 ***simultaneous failures***
  - These many simultaneous failures have never been observed in our simulations of NORDIC-32 (many elements could be switched-off though)
  - Probability of exceeding the threshold of simultaneous failures can be calculated
- Transient solution will tell us:
  - Whether ***steady-state is achievable*** within a given horizon (e.g. a year or 10 years)
  - Solution is expected to be much faster than simulation
    - Markov Decision Processes (MDP) and other artificial intelligence (AI) techniques become feasible for ***sensitivity analysis*** on model parameters.
    - ***Conservative parameterization*** of an Adversary model becomes feasible.

Other ideas from interacting with Duke

- Survivability analysis
  - Eliminates the need to define ***intensity*** of cyber attacks
  - Focus on how a power system behaves ***post successful attack.***
- Interestingly, the Duke solution depends on an ***aggregated model***, of the state of the power system
  - Own work on "risk communication models" applies.
  - Kishor suggested that we add ***transient analysis*** to our work to get additional insight.

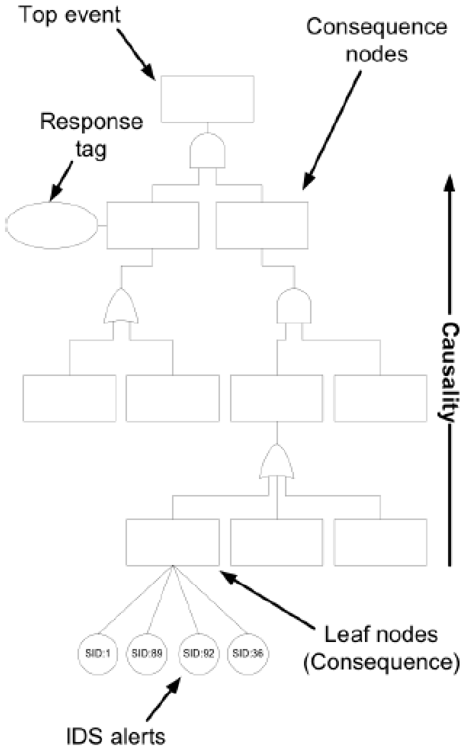


University of Illinois at Urbana Champaign (UIUC)

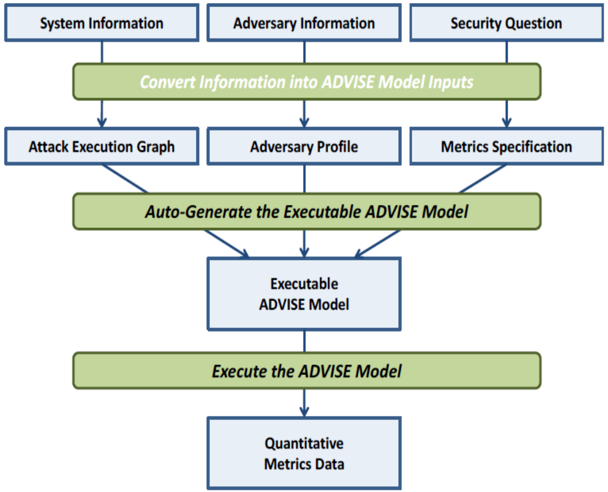


UIUC (2): Rapid Response Engine (RRE)

- **RRE: a real-time automatic, scalable, adaptive and cost-sensitive intrusion response system**
  - Accounts for planned adversarial behavior
  - Accounts for uncertainties in IDS alerts
- Models adversary behavior and responses using **Attack-Response Tree** (ART)
- Employs a game-theoretic response strategy against adversaries in a two-player Stackelberg game
- Developed distributed and hierarchical prototype implementation

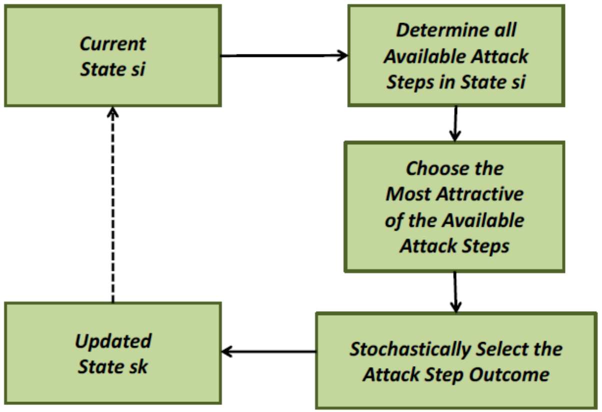


UIUC (3): ADVISE

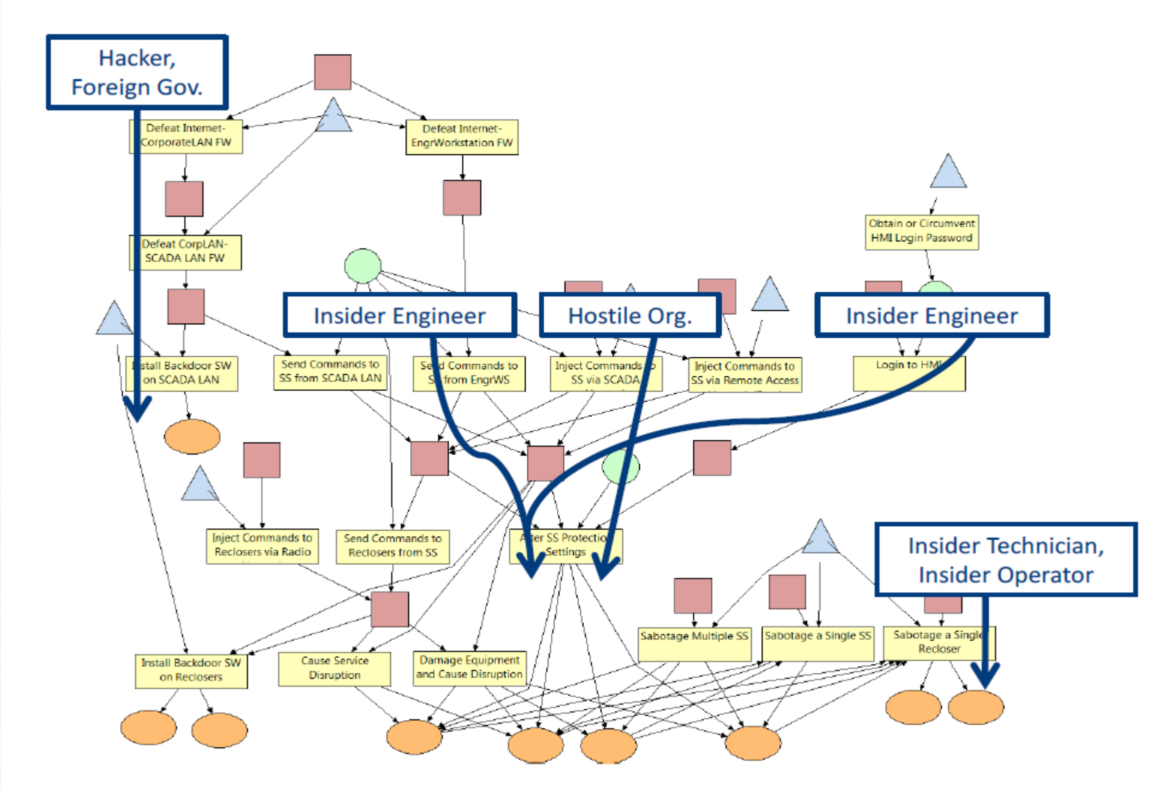


Model Execution: the Attack Decision Cycle

- The adversary selects the most attractive available attack step based on his attack preferences.
- State transitions are determined by the outcome of the attack step chosen by the adversary.



UIUC (4): ADVISE META



ADVISE META contains an ***attack ontology*** using Attack Execution Graphs (AEG).

For a given communication network all AEG are generated automatically by the tool.

Impact of actions (as in MDP) is defined by the Modeller.

City’s collaboration with UIUC

- *Contributions* to ADVISE META ontology
  - Models of attacks that we have worked with in NORDIC-32
  - Models of attacks that we have identified as interesting, e.g. on special purpose software such as SE/WAMS.
- *Integration* of ADVISE META with NORDIC-32
  - NORDIC – 32 model of power system (simulation of using the numeric solver) will compute the ***impact*** of actions taken by an adversary.
  - Initial agreement reached on this with Bill Sanders and Ken Keefe, the chief developer of Mobius (ADVISE META)
- Access to the *test bed* of industrial control systems (power system simulators and real equipment) available at UIUC.

Interaction with Johns Hopkins

- I delivered a 1-day seminar on modelling the effect of cyber attacks on reliability of a 2-channel software system
  - I am to deliver a lecture on this tomorrow, the 19th of May.
- My work is relevant to their work on ***intrusion tolerant architectures*** built with a Byzantine agreement protocol.
- Agreed to work together and validate the sufficient conditions for Byzantine protocol to be guaranteed to work correctly.

- The colleagues briefed me on their own work on a "resilient SCADA", which is currently under development. Their plan is to use the resilient communication (based on spines overlays).
  - They plan to release the resilient SCADA as open source.
  - Might be of interest here at KhAI, too.

Thank you

City, University of London
Northampton Square
London
EC1V 0HB
United Kingdom

T: +44 (0)20 7040 8963
E: p.t.popov@city.ac.uk
www.city.ac.uk/people/academics/peter-popov