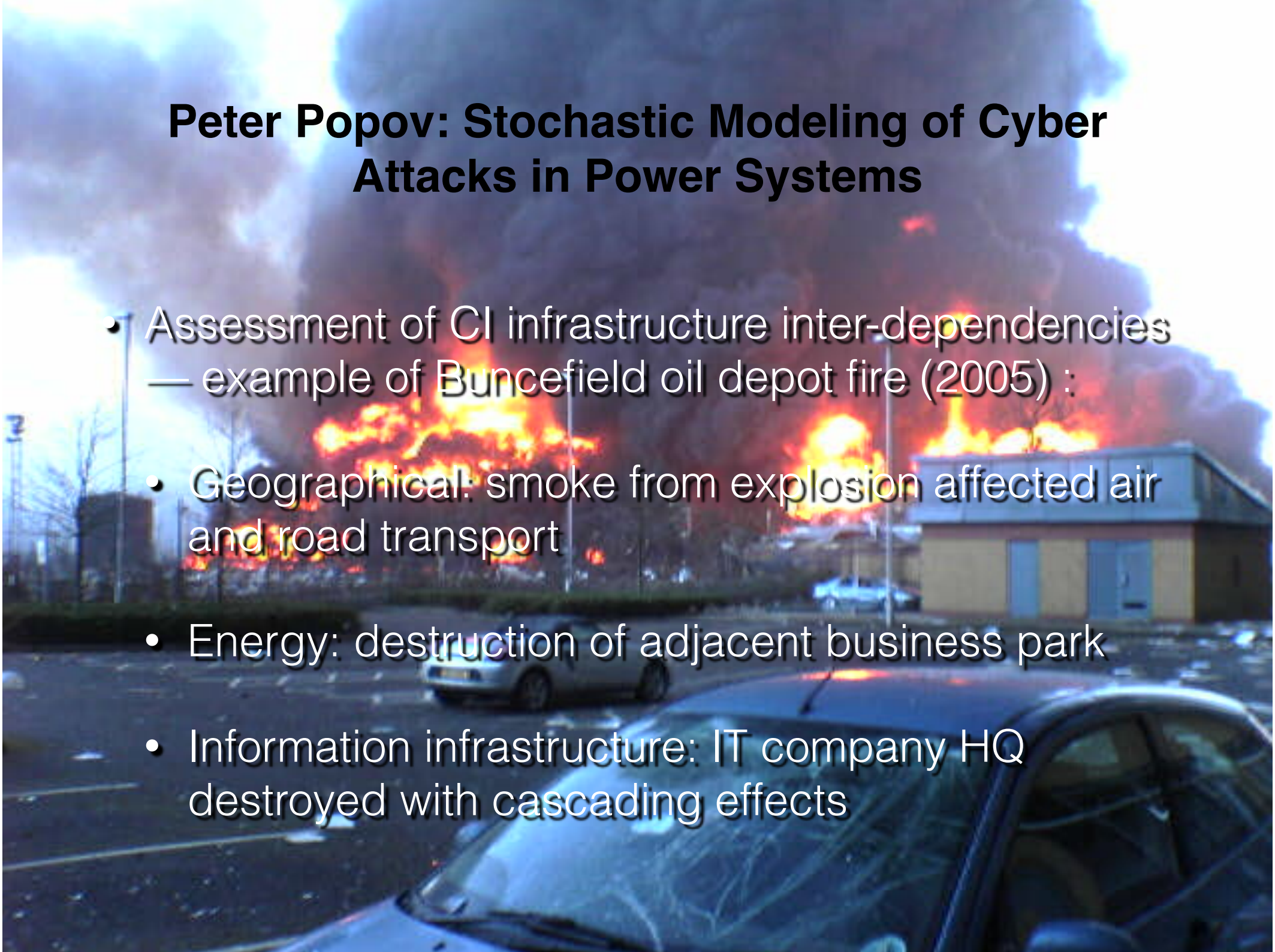
IFIP WG 10.4 workshop

Smart Grids: Security and Dependability

26-29 June, 2014, Amicalola Falls Lodge, Dawsonville, Georgia, USA

Session 1 summary

- **Peter Popov**: Stochastic Modeling of Cyber Attacks in Power Systems
- **Bill Sanders**: NP-View: Automatic Analysis of Process Control Network Firewall Configurations



Peter Popov: Stochastic Modeling of Cyber Attacks in Power Systems

- Assessment of CI infrastructure inter-dependencies — example of Buncefield oil depot fire (2005) :
  - Geographical: smoke from explosion affected air and road transport
  - Energy: destruction of adjacent business park
  - Information infrastructure: IT company HQ destroyed with cascading effects

PIA : Probabilistic Interdependency Analysis

- **Preliminary IA (Pre-IA)** — HAZOP-like discovery of interdependencies
- **Probabilistic IA (Pro-IA)** — quantitative model of interacting CIs (very large #components, hybrid models mixing probability models (MTBF, MTTR, attacks) and deterministic engineering models (e.g., flow models)
  - SANs & Möbius + tricks : “stochastic associations”
    - finite state components with rates function of states of “neighboring” components
    - embedded dynamic sub-models relating dynamics of $\{components\}_A$ to state of $\{components\}_B$
    - components coupled by spatial location and other common-mode mechanisms

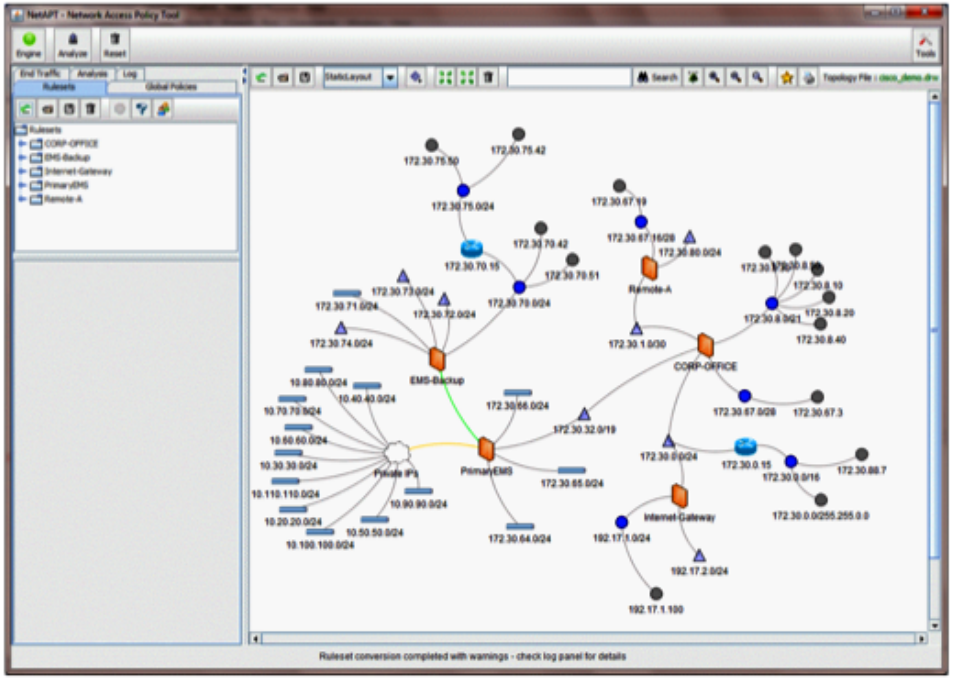
Peter's conclusions

- Methodology for interdependency analysis
- Methodology for assessing impact of cyber security on industrial systems:
  - model of adversary
  - model of ICS (e.g., protection, control, etc.)
  - model of controlled system (evaluate impact)
- Open issues:
  - how to do research on complex systems (methodology, testbeds, scaling, realism, realistic examples)
  - lack of general theory

Bill Sanders: NP-View: Automatic Analysis of Process Control Network Firewall Configurations

- **TCIPG** — Trustworthy Cyber Infrastructure for the Power Grid
  - 4-university 5-year project with many $
  - multiple technical clusters and threads
  - testbed : lab-contained but true-to-reality implementation of critical infrastructure
- **NP-view** — Network Perception view
  - tool for assessing security (access control) policies

NP-view



- **Features**:
  - automated topology inference
  - scalable and complete state space exploration to identify network access violations exhaustively
- **Inputs**: rule-sets from host-based firewalls, router-based dedicated firewalls or OS-based access control
- **Outputs**: possible paths (all, to/from endpoint, between pair of endpoints, allowed by selected firewall or rule, thru' selected tunnel…)
- **Benefits**: less $ to comply with CIP regulations, improved accuracy of security analysis, metrics to optimize network changes