Future and Emerging Threats in Critical Systems

Edita Djambazova

Institute for Parallel Processing, Bulgarian Academy of Sciences

EC2ND, 11 – 12 December 2008, Dublin

Critical Systems

- Working Group on Critical Systems in the ICT-FORWARD Project

- Critical System – a working definition

- Threat Areas

- Model of a Critical System

- Goals and Impact

Working Group on Critical Systems in the ICT-FORWARD Project

- to identify and discuss future and emerging threats to those critical systems that society in general depends upon.

- to try identifying appropriate ways and developments to counter the identified threats.

- to network and coordinate the efforts between players in academia and industry that are active in these areas.

- to inform and influence decision makers about the results of our activities, something that should help them initiate necessary action to thwart the identified threats.

- to prepare a chapter in a white book that highlights the most important threats in this area. This text will contain clear recommendations for policymakers to address the identified challenges.

- to facilitate the creation of a roadmap for research in the identified areas.

Critical System – a working definition

- A system or network whose disruption of operation can lead to significant material loss or threaten human life
- Critical by application, by size, by impact, by importance to the society

Threat Areas

- Critical Infrastructures
  - ICT-related, Internet-related - e.g., telecommunications, transportation, data centers, banking and finance
  - Interdependency, cascading effects
- Critical Applications
  - Process control systems – use of COTS, Internet, more ICT applied
  - SCADA-based systems
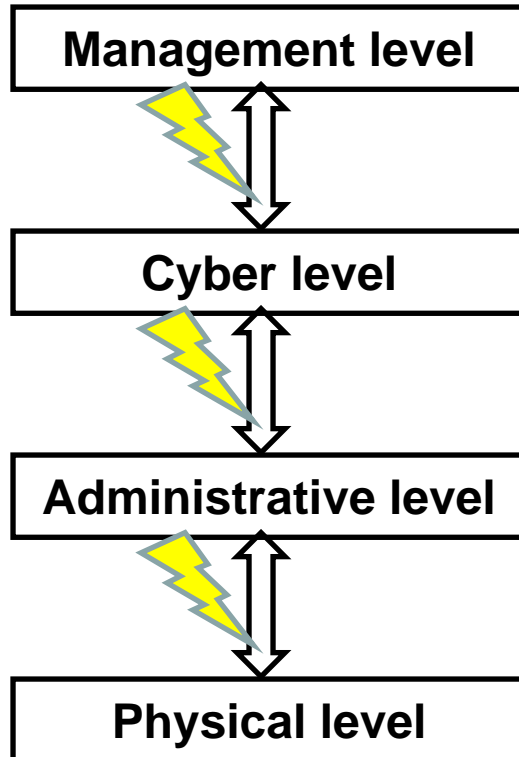 - Proprietary solutions are replaced by open and conventional protocols and networks

Model of a Critical System
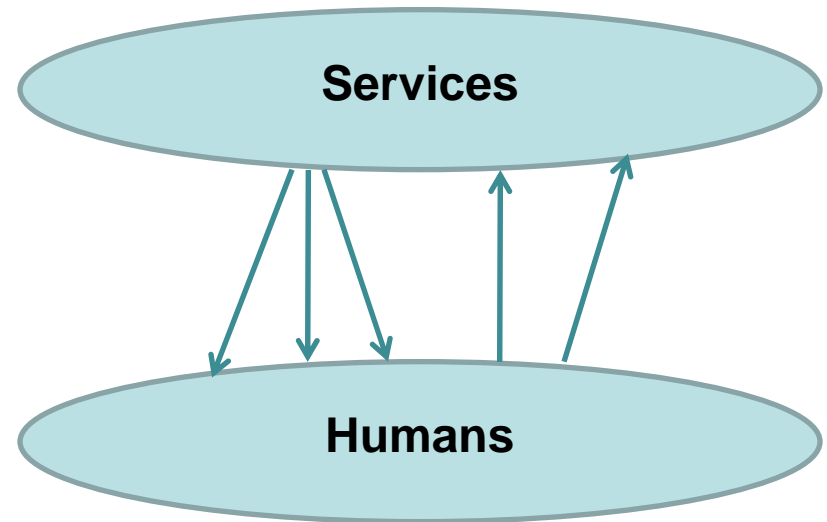
From threats' point of view

Model of a Critical System

From application's point of view

Functional Model

Management level

Cyber level

Administrative level

Physical level

Services

Humans

Some Measures and Recommendations

- Risk and vulnerability assessment tools and methods, secure control architectures and technologies, awareness and governance of risk to society

- Design diversity when using COTS, resilience approach, integrated approach to security

- Special attention to introduction of SOA to critical systems

Goals and Impact

- Threat Report
- Roadmap for future research
- Security-aware community – industrials, practitioners, researchers

Thank you

Edita Djambazova

Institute for Parallel Processing
Bulgarian Academy of Sciences
Bl. 25A, Acad. G. Bonchev St.
1113 Sofia, Bulgaria
ead@iccs.bas.bg