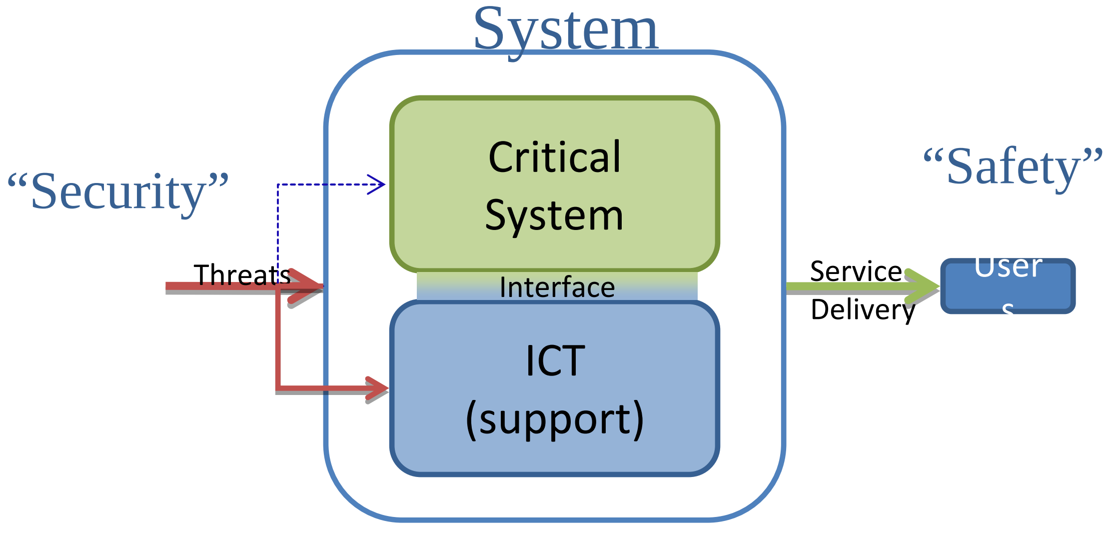
forward

Critical Systems Working Group

Scope of the Critical Systems Working Group

- Critical Systems working group considers the special requirements of ICTs when applied to critical systems and critical infrastructures.



The service delivery must not be interrupted

Background Critical Systems

- Critical systems ***control public resources*** such as electricity, water, telecommunications, banks, etc.
- The ***consequences*** of any disruption of service are severe and may result in loss of human life.
- Such systems must often consider different types of ***constraints*** compared with regular computer systems (e.g., real time).
- Interdependencies between subsystems lead to ***cascading effects*** that are difficult to foresee.
- There is an ***emphasis on safety*** and less understanding for IT security in this culture (and vice versa).

Examples of Critical Systems

forward

- ***"Traditional" critical infrastructures***
  - electricity, water, telecommunications, etc.
- ***SCADA systems***
  - Used in almost all Critical Infrastructures
  - Efforts are already ongoing to protect such systems
- ***Financial systems*** are critical infrastructures that are hardly distinguishable from their ICT supporting component.
  - Many access points
  - Availability to many and diverse users

“Emerging” Critical Systems

forward

- ***Data centers*** are becoming common and these can be seen as CIs in that they provide data necessary for more traditional CIs

amazon web services™

- ***In-vehicle automation*** and ICT, with remote diagnostics and software updates for vehicles.
  - Embedded (automobile) systems connected to open networks.
  - Some of the problems related to any embedded system are also valid for the ***connected car***.

Safety takes priority over security

- ***Problem:*** In the domain of critical systems both safety and security are important but in certain scenarios, safety takes priority.
  If the underlying process is about to become critical, security should not block or delay appropriate remedies or counteractions.

- ***Solution:*** Integrated view on safety and security, since a breach in security could provoke a breach in safety.

Unforeseen cascading effects

- ***Problem:*** Interconnected systems are difficult to model properly and interdependencies between the subsystems can lead to cascading effects that are difficult to foresee.
  - A complicating issue is that part of the system may be governed by proprietary protocols while others use open standards.
  - Different system owners may not trust each other.

- ***Solution:*** Development of appropriate models for the domain and an overall better architecture with a security baseline.

Use of new technology

- ***Problem:*** Also critical systems use new types of technology to add functionality:
  - wireless communication for remote sites and internal enterprise communication. Critical control communication will be wireless within 10 years (source: WINA and ISA).
  - New Generation Networks

- ***Solutions:*** There is a tradeoff between the advantages gained with the technology versus the security risk. This trade-off must be carefully modeled and analyzed.

The Human Factor

- ***Problem:*** The human is considered to be the weakest point in a critical system. The roles include operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development.
  ***Adversarial problem*:** Insiders with experience of and knowledge about the CS.

- ***Solution:*** Education and training, raising awareness of security risks; sound and evolving security policy; modeling the user (“cognitive modeling”) and user-interactive properties. Effective strategies for discovering an “insider” is an open research question.

Thematic Session 1

Trustworthy Network Infrastructures

http://www.ictsec-olomouc.eu

Contact persons: Edita Djambazova ead@iccs.bas.bg
Luben Boyanov lb@acad.bg