NexTech & TrendNews

Cyber-systems Protection by Design
Cyber-related aspects: protection by-design

- Design complexity (AI, Cloud, …) (hardware, software, systems)
- Black Swan: Sudden, unexpected situation, ransomware (Keynote: Anne Coull)
- Zero-day: Vulnerabilities for which no mitigation exists (Keynote: Steve Chan)
- Autonomous systems
- Testing and validating self-adaptable systems
- Trust and explainability
• Facilitator
  Prof. Dr. Petre Dini, IARIA, USA/EU

• Invitees
  Dr. CTO, Daniel Kaestner, AbsInt GmbH, Germany
  Prof. Dr. Nader Mir, San Jose State University, USA
  Prof. Dr. Michael Massoth, Hochschule Darmstadt (h_da), Germany
Are the already-known requirements simply neglected in early system design phases?

What is the most suitable approach for tracking the consistency of features for cyber-systems protection?

Are there insurmountable challenges (time, verification, budget) for a proper cyber-protection development?

Is the deployment more critical than the preceding development phases?

How costly is a more robust and safe development process?

Is the patching process a danger (apriori adopted) for the cyber-protection by design?