Call for papers

14th International Conference on Critical Information Infrastructures Security CRITIS 2019, will be held in Linköping, Sweden, September 23-25, and continues the tradition of bringing to forth innovative research in the field of critical (information) infrastructures protection (C(I)IP), exploring ideas that address challenges to resilience and societal safety, and fostering the dialogue with stakeholders.

CRITIS 2019 aims at bringing together researchers, professionals from academia, critical (information) infrastructure operators, industry, defence sector and governmental organisations working in the field of the security of critical (information) infrastructure systems. Moreover, CRITIS aims to encourage and inspire early stage and open-minded researchers in this demanding multi-disciplinary field of research. Outstanding research performance demonstrated by young researchers may compete for the Young CRITIS Award (YCA).

The Projects' Dissemination Session will be an opportunity of dissemination for ongoing European, multinational, and national projects, to share the experiences among scientist and experts working on different projects in the C(I)IP domain.

Conference themes

CRITIS 2019 conference has a special focus on testbeds for research and training with respect to security in critical infrastructures, encouraging participants from Europe, US and Asia to present the state of art in development of such physical and virtual environments.
The conference will also be a forum to discuss current and future energy infrastructures with participation of energy infrastructure operators and stakeholders, as well as the infrastructures for water management systems, traffic management and interdependencies therein. Topics for the conference papers include (but are not limited to):

Topic 1: Protection of cyber-physical systems,

- Critical (Information) Infrastructure Protection (CIP and CIIP)
- Vulnerability and Risk Analysis / Threat Modelling
- Cyber security in C(I)I systems
- Self-healing, self-protection, and self-management architectures for C(I)I
- Fault-tolerant control for cyber-physical systems / C(I)I
- Modelling and analysis of cyber-physical systems / C(I)I and C(I)IP approaches

Topic 2: Advances in C(I)IP organisation, management and legal aspects

- Digital forensics and attribution in attacked C(I)I
- International approaches to C(I)IP including identification of C(I)I elements
- Risk management, impact and consequence analysis regarding C(I)I
- Coherent prevention, preparedness / exercises, incident management / mitigation, and recovery approaches to C(I)I
- Resilience and survivability of C(I)I as complex cyber-physical systems
- C(I)IP policies at international, national and cross-border levels, e.g. public-private partnerships
- Cross-border issues regarding EU's Network and Information Security Directive
- C(I)IP R&D agenda at national and international levels
- Economics, investments and incentives for C(I)IP
- Defence of civilian CI and CII in conflicts with cyber warfare elements

- Infrastructure, architectural and technology changes in the energy sector which may impact the sector approach to C(I)I or challenge other C(I)I-sectors (e.g. smart grids and energy supply in smart city developments)
- Impact of geopolitical & social factors and threats

Topic 3: Emergencies and C(I)IP protection, national and cross-border

- Analysis of Human Factor and Security Awareness in C(I)IP
- Advanced decision support for mitigating C(I)I related emergencies
- Social aspects and public communication in C(I)IP
- Psycho-social dimensions of crisis management and intervention with C(I)I
- Training for C(I)IP and effective intervention
- The role of Social Media in C(I)I-related crisis management (as a threat or a potential benefit)
- Recent trends in cyber economy (clouds, quasi-monopolies, e-currencies etc.) and implications for C(I)I and C(I)IP

Topic 4: Disruptive technologies for C(I)IP, including

- New platforms for financing and data management (e.g. blockchains)
- Infrastructure IoT and emerging standards
- The role of AI and machine learning in autonomous management of infrastructures
- Digital twins and their deployment as augmented reality for training and scenario risk analysis
- Future communication technologies (5G, edge) and their potential impact on other C(I)I

Submission guidelines:

All papers must be original and not simultaneously submitted to another journal or conference. All paper submissions must contain title, a short abstract, and a list of keywords. All submissions will be subjected to a thorough **double-blind** review by at least three reviewers. **Submitted papers shall be anonymised and all author names, affiliations, acknowledgements, and obvious traceable references should be eliminated** to be eligible for the review process.

The following two paper categories are welcome. Any submission needs to be explicitly marked as “full paper” or “short paper”.

- **Full papers** scientific research papers, surveying works and industrial experiences describing significant advances in C(I)IP. Full papers should be no longer than 12 pages, including bibliography and well-marked appendices.
- **Short papers** work-in-progress reports, R&D project and industrial experience reports. Short papers should be 4 to 6 pages long.

Accepted papers are to be included in post-proceedings, published by Springer in their Lecture Notes in Computer Science (LNCS) series. All papers should be submitted in this format.

Important dates:

30 April 2019 -- Full-text submission
18 June 2019 -- Notification of acceptance
9 September 2019 -- Camera-ready papers

Conference website: https://critis2019.on.liu.se/