CRITIS 2013

CRITIS 2013
8TH INTERNATIONAL CONFERENCE ON CRITICAL
INFORMATION INFRASTRUCTURES SECURITY
SEPTEMBER 16-18, 2013, AMSTERDAM

Call for Papers

The annually held **CRITIS** conference is devoted to Critical (Information) Infrastructure security, protection and resilience. The 8th edition **will be held from 16-18 September 2013 in Amsterdam, The Netherlands.**
The CRITIS 2013 Call for Papers is addressed to all researchers and critical infrastructure stakeholders who wish to present their papers at the conference. More information can be found at: www.critis2013.nl.

Modern societies increasingly depend on critical infrastructures. Those themselves increasingly depend on and are entangled with Information and Communication Technologies (ICT). Disruption or loss of (ICT-based) critical infrastructures may result in serious consequences for the functioning of the society, the economy, the functioning of governments, the ecology and social well-being of people, and in the most unfortunate cases loss of human lives, livestock and other animals. As a consequence, the security, reliability and resilience of these infrastructures are critical for the society. Critical (Information) Infrastructure Protection (C(I)IP) is therefore a major objective for governments, companies, operators of these infrastructures and the worldwide research community.

CRITIS 2013 is set to continue a well-established tradition of presenting innovative research and exploring new challenges for the protection of critical information-based infrastructures (CIP/CIIP). CRITIS brings together stakeholders from industry, operators and governments as well as researchers and professionals from academia, applied research organisations and industry interested in all different aspects of C(I)IP.
One focus of CRITIS 2013 is on the new challenges of **Resilience of Smart Cities**, a topic that will be highlighted by thought provoking and visionary keynote speeches and by conference papers.

The second day of CRITIS 2013 will be a meeting place between the diverse set of **C(I)IP stakeholders** with their short, medium and long term needs **and** the **academic and applied research communities**. CRITIS2013 intends to foster collaboration, to find common, collaborative approaches towards solutions and to boost R&D to address the identified needs. On the third day, the focus will be on the (academic) **advances in C(I)IP R&D**.
A (virtual) multi-disciplinary community of new talented **PhD students and junior researchers** in the field of C(I)IP will be build: **YOUNG CRITIS**. Young CRITIS appeals to the scientific C(I)IP communities at national, European and global level.

Given the focus areas above, the programme committee will select papers per topic category (or track) mentioned below. Therefore, authors need to state which topic category they address. Researchers are solicited to contribute to the conference by submitting research papers, work-in-progress reports, R&D project results, surveying works and industrial experiences describing significant advances in C(I)IP. Stakeholders from governments, Critical Infrastructure operators, and industry are encouraged to submit papers which describe their current and future challenges to be engaged by researchers and multidisciplinary research teams.

Important Dates

EXTENDED deadline for submission of papers: June 15, 2013 (was May 10, 2013)
Notification to authors: July 15, 2013
Camera-ready papers: August 30, 2013

CRITIS 2013

The CRITIS 2013 Scientific Committee invites papers for the following four topic categories:

Topic category 1: **Resilience of Smart Cities**

Topic category 2: **Requirements for C(I)IP by C(I)I Stakeholders**

Topics of interest for category 2 include:

- C(I)IP requirements for Resilient Smart Cities
- C(I)IP requirements posed as future (near, mid and long term) challenges, e.g. mobility and smart grids
- Requirements for Resilient (Information) Infrastructures
- C(I)I Survivability requirements
- The use of clouds for C(I)I operations
- Economics, Investments and Incentives of C(I)IP
- C(I)I Exercises & Contingency Plans
- Trust Models in Normal Situations and During Escalation
- C(I)IP Polices at National and Cross-border levels
- C(I)IP R&D Agenda at National and International levels

Stakeholders include industry, CI operators, governments and government agencies, EU Directorates and integrated solution providers, e.g. CIP/CIIP-related R&D communities and disciplines. Papers submitted for topic categories 1 and 2 that do not fit the focus of the category, may be reassigned by the Scientific Committee to topic categories 3 or 4.

Topic category 3: **Advances in C(I)IP** and **Topic category 4:** **YOUNG CRITIS**

Topics of interest for categories 3 and 4 include all topics mentioned under topic category 2 as well as topics like:

- Resilient C(I)I and C(I)I Survivability
- Resilience of interacting C(I)I
- Cyber Defence of C(I)I
- Self-healing, Self-protection, and Self-management Architectures
- C(I)I dependency Modeling, Simulation, Analysis and Validation
- Protection of Complex Cyber - Physical Systems
- Cyber security related threats & vulnerabilities, modeling and analysis
- Cyber Security of Smart Grids, Process Control and SCADA
- Advanced Forensic Methodologies for C(I)I
- Public - Private Partnership for C(I)I Resilience

Instructions for Paper Submission

All submissions will be subjected to a thorough blind review by at least three reviewers. Papers should be in English and no longer than 12 pages, including bibliography and well-marked appendices. As in previous years, it is planned that post-proceedings are published by Springer-Verlag in the Lecture Notes in Computer Science series. Pre-proceedings will appear at the time of the conference. At least one author of each accepted paper is required to register with the Workshop and present the paper. Paper submission will be done via EasyChair. The submitted paper (in PDF or PostScript format) should follow the respective template offered by Springer.

The paper must start with a title, a short abstract, and a list of keywords. However, the submission should be anonymised and all author names, affiliations, acknowledgements, and obvious traceable references should be eliminated.

Extended and fully revised versions of the best papers accepted for CRITIS 2013, after a further peer-reviewed process, will be published in a special issue of the International Journal of Critical Infrastructures (Inderscience).