CRITIS 2019

The 14th International Conference on Critical Information Infrastructures Security

September 23-25, 2019 - Linköping, Sweden

Sponsors

RICS

MSB Swedish Civil Contingencies Agency

SAAB TECHNOLOGIES SAAB

SVENSKA KRAFTNÄT

SECTRA

li.u LINKÖPING UNIVERSITY

Endorsers

Springer

Lecture Notes in Computer Science LNCS LNAI LNBI

RES ON NETWORK

VRICON

https://critis2019.on.liu.se

CRITIS 2019

14th International Conference on Critical Information Infrastructures Security

Linköping University, Sweden

Program

Committees

Organizing Committee

General & PC chair

Simin Nadjm-Tehrani, Linköping University, Sweden

Honorary chair

Sandro Bologna, AIIC, Italy

Local organization chair

Mikael Asplund, Linköping University, Sweden

Publicity chair

Magnus Almgren, Chalmers University of Technology, Sweden

Session chairs for Industrial/practical experience reports

Sokratis K. Katsikas, NTNU, Norway & Open Unive. of Cyprus, Cyprus
Francesco Flammini, Linnaeus University, Sweden

Technical Program Committee

Cristina Alcaraz, UMA, Spain
Mikael Asplund, Linköping University, Sweden
Alberto Avritzer, eSulabSolutions, US
Fabrizio Baiardi, University of Pisa, Italy
Emiliano Casalicchio, Blekinge Institute of Technology, Sweden
Michal Choras, Univ. of Science and Technology, UTP Bydgoszcz, Poland
Kris Christmann, University of Huddersfield, UK
Gregorio D'Agostino, ENEA, Italy
Geert Deconinck, KU Leuven, Belgium
Mathias Ekstedt, KTH Royal Institute of Technology, Sweden
Francesco Flammini, Linnaeus University, Sweden
Igor Nai Fovino, Joint Research Centre, Belgium
Dimitris Gritzalis, Athens University of Economics and Business, Greece
Stefanos Gritzalis, University of the Aegean, Greece

Bernhard Haemmerli, ACRIS, Switzerland
Chris Hankin, Imperial College London, UK
Grigore M. Havarneanu, International Union of Railways, France
Mikel Iturbe, Mondragon University, Spain
Zbigniew Kalbarczyk, University of Illinois at Urbana-Champaign, USA
Sokratis Katsikas, NTNU, Norway
Marieke Klaver, TNO, Netherlands
Vytis Kopustinskas, European Commission, JRC, Italy
Panayiotis Kotzanikolaou, University of Piraeus, Greece
Ričardas Krikštolaitis, Vytautas Magnus University, Lithuania
Elias Kyriakides, University of Cyprus, Cyprus
Javier Lopez, NICS Lab, Spain
Eric Luiijf, Luiijf Consulting, Netherlands
Jose Marti, The University of British Columbia, Canada
Linas Martišauskas, Lithuanian Energy Institute, Lithuania
Marcelo Masera, Joint Research Centre, Belgium
Aditya Mathur, Purdue University, USA
Kieran McLaughlin, Queen's University Belfast, UK
Max Mühlhäuser, TU Darmstadt, Germany
Gabriele Oliva, Campus Biomedico di Roma, Italy
Evangelos Ouzounis, ENISA, Greece
Stefano Panzieri, Roma TRE University, Italy
Ludovic Pietre-Cambacedes, EDF, France
Anne Remke, Univ. Münster, Germany and Univ. Twente, Netherlands
Henrik Sandberg, KTH, Sweden
Inga Šarūnienė, Lithuanian Energy Institute, Lithuania
Alberto Tofani, ENEA, Italy
Maria Paola Scaparra, Kent Business School, The University of Kent, UK
Roberto Setola, Università Campus Biomedioc, Italy
Nils Ole Tippenhauer, CISPA, Germany
Eugenijus Uspuras, Lithuanean Energy Institute, Lithuanea
Emmanouil Vasilomanolakis, Aalborg University, Denmark
Stephen D. Wolthusen, Royal Holloway Univ., UK, and NTNU, Norway
Jianying Zhou, Singapore University of Technology and Design, Singapore

CRITIS Steering Committee

Chairs

Bernhard M. Hämmerli, Tech. Univ. Lucerne and ACRIS, Switzerland
Javier Lopez, University of Malaga, Spain
Stephen D. Wolthusen, Royal Holloway Univ., UK and NTNU, Norway

Members

Robin Bloomfield, City University London, UK
Sandro Bologna, AIIC, Italy
Gregorio D'Agostino, ENEA, Italy
Grigore Havarneanu, International Union of Railways (UIC), France
Sokratis K. Katsikas, Norwegian University of Science, Norway and Technology and University of Piraeus, Greece
Elias Kyriakides, University of Cyprus, Cyprus
Eric Luiijf, TNO (retired), the Netherlands
Marios M. Polycarpou, University of Cyprus, Cyprus
Reinhard Posch, Technical University Graz, Austria
Erich Rome, Fraunhofer IAIS, Germany
Antonio Scala, IMT – CNR, Italy
Inga Šarūnienė, Lithuanian Energy Institute, Lithuania
Roberto Setola, Università Campus Bio-Medico di Roma, Italy
Nils Kalstad Svendsen, Gjovik University College, Norway
Marianthi Theocharidou, EC Joint Research Centre, Italy

Program

Sessions are held in room Ada Lovelace and Coffe breaks are in room Ljusgården, see the map on page 17.

Monday, September 23

Monday, September 23	
8.00-9.00	**Registration**
9.00-9.15	Welcome (conference Chair: Simin Nadjm-Tehrani)
9.15-10.15	Keynote address: **Awais Rachid, University of Bristol** *Everything is Awesome! Or is it? Cyber Security Risks in Critical Infrastructure*
10.15-10.45	**Coffee break**
10.45-12.15	**Technical session: Risk management** Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security (Zack Ellerby, Josie McCulloch, Melanie Wilson and Christian Wagner) Estimating Cascading Effects in Cyber-Physical Critical Infrastructures (Stefan Schauer, Thomas Grafenauer, Sandra König, Manuel Warum and Stefan Rass) Aggregating Centrality Rankings: A Novel Approach to Detect Critical Infrastructure Vulnerabilities (Gabriele Oliva, Annunziata Esposito Amideo, Stefano Starita, Roberto Setola and Maria Paola Scaparra)
12.15-13.45	**Lunch at Mjellerumsgården**
13.45-14.45	Keynote address: **Marianthi Theocharidou, ENISA** *NIS Directive and the role of ENISA*
14.45-15.15	**Short papers:** On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication (Tomomi Aoyama, Atsushi Sato, Giuseppe Lisi and Kenji Watanabe) SealedGRID: A Secure Interconnection Technologies for Smart Grid Applications (Aristeidis Farao, Juan Enrique Rubio, Cristina Alcaraz, Christoforos Ntantogian, Christos Xenakis and Javier Lopez)

15.15-15.45	**Coffee break**
Monday, September 23, continued	
15.45-17.45	**Industrial & Practical experience reports (Session chair: Dr. Francesco Flammini):** SAFeRA 4STER: Integrated Management of Safety and Security Synergies in Seveso Plants (Gabriele Oliva, Roberto Setola and Giacomo Assenza) Using serious gaming to train operators of critical infrastructure (Tommy Gustafsson and Lars Westerdahl) Industry/Experience report on recent Trends in Cyber Economy and the Impact on OT (Eleni Richter) Experience Report from an Intrusion Attempt on the Power Distribution Grid (Anders Hansson)
17.45	Bus transport to Vricon
18.15 - 20.00	**Reception at Vricon**

Tuesday, September 24

Tuesday September 24	
8.00-9.00	**Registration**
9.00-10.00	Keynote address: **David Nicol, University of Illinois at Urbana-Champaign** *Challenges in Quantifying An Adversary's Cyber Access to Critical Infrastructures*
10.00-10.30	**Coffee break**
10.30-11.30	**Technical session: Vulnerability assessment:** Automatic Vulnerability Analysis for Cyber-Physical System (Yuning Jiang, Yacine Atif and Jianguo Ding) Climate Change Impact and Vulnerability Analysis in the City of Bratislava: Application and Lessons Learned (Daniel Lückerath, Eva Streberová, Manfred Bogen, Erich Rome, Oliver Ullrich and Eva Pauditsová)
11.30-12.00	**Short papers** A Dynamic Risk Assessment (DRA) Methodology for High Impact Low Probability (HILP) Security Risks (Carlo Dambra, Chanan Graf, Jordi Arias and Alex Gralewski) On Actuator Security Indices (Jezdimir Milosevic, Sebin Gracy and Henrik Sandberg)
12.00-13.30	**Lunch at Universitetsklubben**
13.30-15.00	**Technical session: Resilience and Mitigation** Intrusion Resilience for PV Inverters in a Distribution Grid Use-Case Featuring Dynamic Voltage Control (Boojoong Kang, David Umsonst, Mario Faschang, Christian Seitl, Ivo Friedberg, Friederich Kupzog, Henrik Sandberg and Kieran McLaughlin) Mitigating escalation of cascading effects of a payment disruption across other critical infrastructures: lessons learned in 15 simulation-games (Joeri Van Laere, Björn J. E. Johansson, Leif Olsson and Peter Määttä) Using Datasets from Industrial Control Systems for Cyber Security Research and Education (Qin Lin, Sicco Verwer, Robert Kooij and Aditya Mathur)
15.00-15.30	**Coffee break**

Tuesday, September 24, continued	
15.30-16.00	Keynote address: **Ainara Casajus Valles, Joint Research Centre, European Commission** *How science can help in the preparation of National Risk Assessment*
16.00-17.00	**Special session on cyber ranges and testbeds** Short paper: A Virtual Cyber-Security Testbed for Continuously Controlled Systems (Viktor Tuul and Henrik Sandberg) Roundtable discussion: Prof. Anne Remke (univ. Twente/Münster Univ.), Dr. Olaf Manuel Maennel (Center for Digital Forensics and Cyber Security at Tallinn University of Technology, Estonia), Dr. Shahid Raza (RISE), Tommy Gustavsson (FOI, Sweden)
19.00-23.00	**Conference banquet**

Wednesday, September 25

Wednesday, September 25	
8.00-9.00	**Registration**
9.00-10.00	Keynote address: **Yves Rougier, Ministry for the ecological and inclusive transition, France** *Hybrid Threats Impact on Crisis Management*
10.00-10.30	**Technical session: Transport** Securing Software Updates for Trains (Tatiana Galibus)
10.30-11.00	**Coffee break**
11.00-11.30	**Technical session: Finance** A comparison between SWIFT and Blockchain from a cyber resiliency perspective - Addressing the payments infrastructure vulnerabilities to evolving cyber threats (Luisa Franchina and Guido Carlomagno)
11:30-11:45	Young CRITIS award presentation
11:45-12:00	Next CRITIS!
12:00-13:30	**Lunch at Universitetsklubben**
13:30-15:00	Breakout sessions

Keynote talks

Everything is Awesome! Or is it? Cyber Security Risks in Critical Infrastructure

Awais Rashid

Professor of Cyber Security, University of Bristol

Industrial Control Systems play an important role in the monitoring, control, and automation of critical infrastructure such as water, gas, oil, and electricity. Recent years have seen a number of high profile cyber attacks on such infrastructure exemplified by Stuxnet and the Ukrainian Power Grid attacks. This naturally begs the question: how should we manage cyber security risks in such infrastructure on which the day-to-day functioning of our society relies? What are the complexities of managing security in a landscape shaped by the often competing demands of a variety of stakeholders, e.g., managers, control engineers, enterprise IT personnel and field site operators? What are the challenges posed by the convergence of IoT and critical infrastructure through the so-called Industrial Internet of Things? And will frameworks such as the EU NIS directive help mitigate the cyber security risks to critical infrastructure? This talk will discuss insights from a multi-year programme of research investigating these issues and the challenges to addressing them.

NIS Directive and the role of ENISA

Marianthi Theocharidou

Network and Information Security officer, at ENISA, the EU Agency for Cybersecurity

Marianthi Theocharidou works at ENISA, the EU agency for Cybersecurity. Until recently she had been employed in the European Commission's Joint Research Centre. She has experience in critical infrastructure protection and resilience, risk management and dependency modelling. Marianthi will provide an update on the progress of the implementation of the NIS directive. She will explain the role of ENISA to assist Member States in the consistent implementation the NIS Directive (NISD) and to support public and private stakeholders to enhance the security and resilience of their smart infrastructures and services. She will also discuss the new breach reporting under the NIS Directive and discuss some of the opportunities and challenges here.

Challenges in Quantifying An Adversary's Cyber Access to Critical Infrastructures

David M. Nicol

Director, Information Trust Institute Franklin W. Woeltge Professor of Electrical and Computer Engineering University of Illinois at Urbana-Champaign

Critical infrastructures such as the power grid, up and down stream components of oil and gas production, communication network, transportation networks and so on are now all controlled by devices with CPUs and memory that communicate over both wireline and wireless channels. Quantitative assessment of risk to the controlled infrastructure depends both on models and analysis of the infrastructure under attack, and of the adversary's ability to mount those attacks. To quantitatively assess the risk to the critical infrastructure of cyber-mischief we have to be able to quantitatively assess that component of the risk which depends on the adversary's cyber access to devices which measure and manipulate the physical system. There are myriad challenges in this subproblem, which derive from the adversary's learning by moving laterally through the network, on the state of knowledge and lack of knowledge about means by which the adversary can make those movements, on quantifying the difficulty of exploiting vulnerabilities as that lateral movement is made. This talk highlights the challenges as we see them after working on this and related problems for several years.

How science can help in the preparation of National Risk Assessment

Ainara Casajus Valles

Joint Research Centre, European Commission

The Union Civil Protection Mechanism (Decision No 1313/2013/EU) calls Participant States to develop risk assessments periodically and make the summary of those available to the European Commission, with the aim of promoting an effective and coherent approach to prevention of and preparedness for disasters. The different summaries reported have revealed how challenging it can be for Member States to develop National Risk Assessments (NRAs) due to the diversity of disaster risk management governances in place around Europe, the different level of information available about risk and the their past experiences in carrying out that exercise.

The Report *Recommendations for National Risk Assessment for Disaster Risk Management in the EU* (version 0) attempts to answer the questions of "why" and "how" to do a risk assessment, paying special attention to how science can help in that exercise. The Report is the results of a collaborative effort of the Disaster Risk Management Knowledge Centre team (DRMKC) and nine expert groups from the Joint Research Centre (JRC) to cover various hazards and assets.

This first version of the Report proved that science can already provide advice for risk in a single-hazard framework, in most of the cases. As one of the objectives of NRA is to find a common ground of understanding of the risk faced and their relative priority, the first step towards a multi-hazard assessment is actually harmonising and standardising the assessment as well as the risk metrics among different hazards. At the same time, better knowledge base of risk, availability of data and the development of risk analysis methodologies would facilitate the disaster risk managers to recognise the risk drivers that lead to risk and more effectively plan which capacities are needed.

Version 1 of the mentioned Report is under development, trying to include other risk such as forest fires and cyber security risk.

Hybrid Threats Impact on Crisis Management

Yves Rougier

Head of planning and crisis management at the ministry for the ecological and inclusive transition, France

Historically the terrorist threats were mainly constituted of physical actions. They took different forms which evolved during the twentieth century in a continuous way with increasing consequences and effects. The eleventh September 2001 attacks were a real strategic surprise but only involving "classical" operational means. Then the cyber threats were considered and they introduced a new dimension of complexity and capacities for the terrorists. Since 2001 everything can be considered as possible, with the cyber threats this means that attacks can be controlled from far away and the systemic dimension of cyber also changes the nature of the threats from a physically limited act to a systemic act which can reach simultaneously every point connected with the system. Recently, a new dimension appeared linked to the social networks and to the flow of news which are not checked before being published by medias, both of them opening the door to the proliferation of fake news. This new dimension has already been used in France by the "Yellow Jackets" in order to win the battle for public opinion. The hybrid threat is in fact nothing more than a cocktail of physical event potentially combined with a cyber-attack and a fake news flow on social networks based on a deformed reality. If the previous situations were handled by security and cyber-security specialists using professional tools, this new type of threat requires a global involvement of the whole company and even of its partners and customers. This means that new skills and a globalizing approach must be developed based on human sciences more than on tools. This is the condition to be able to set up the barriers to prevent, deter, identify, delay, react and recover to and from these new kind of actions.

Maps

The conference is held at the main Campus (Campus Valla) of Linköping University, Sweden. All the conference sessions will be held in room Ada Lovelace, in the B-building. Figure 1 shows an overview of the part of the campus where the conference is held as well as the two lunch places. Figure 2 shows a detailed view of the south end of the B-building.

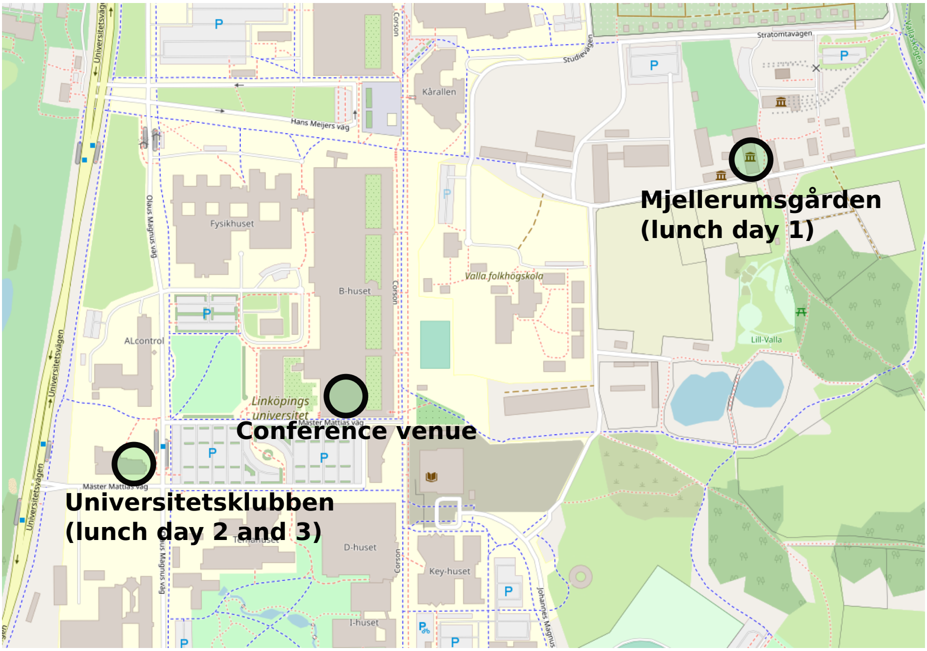


Figure 1: Map of the campus area

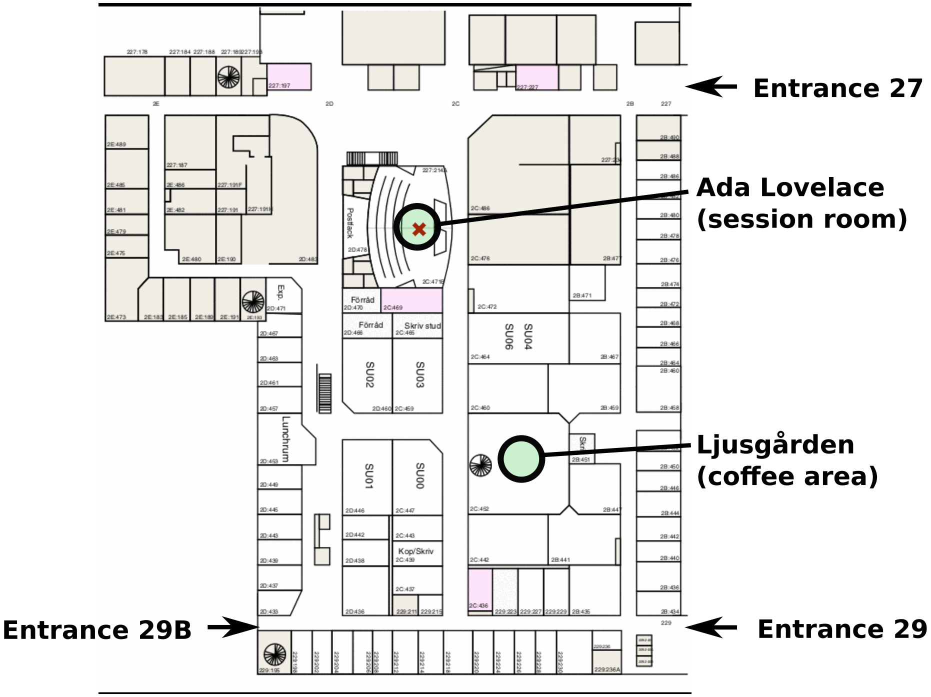


Figure 2: Map of the B-building

CRITIS2019 Bus transport

A free bus transport is organised for all CRITIS attendants to and from the hotels according to the following schedule. **Please be on time!** The bus cannot wait since we do not know who will use the bus and who uses other transport.

Day	**Time**	**Pickup place**	**Dropoff place**	**Comment**
Mon Sept. 23	 08.00 08.15	Downtown: Bus pickup 1 Bus pickup 2	Conference venue	Earlier than other days to allow for registration
Mon Sept. 23	17.45	Conference venue	Reception@ Vricon	After the reception we walk back to downtown
Tue Sept. 24	 08.15 08.30	Downtown: Bus pickup 1 Bus pickup 2	Conference venue	
Tue Sept. 24	17.15	Conference venue	Downtown	
Tue Sept. 24	 18.40 18.50	Downtown: Bus pickup 1 Bus pickup 2	Banquet@Air force museum	
Tue Sept. 24	23.00	Air force museum	Downtown	Approximate time
Wed Sept. 25	 08.15 08.30	Downtown: Bus pickup 1 Bus pickup 2	Conference venue	
Wed Sept. 25	15.15	Conference venue	Downtown	

Downtown the bus pickup and dropoff will be next to Scandic City hotel (Bus pickup 1), and by the St Lars church (Bus pickup 2), which is close to the other two hotels. The places are marked in Figure 3. At the conference venue the bus will stop in the parking lot just outside the B-building where the conference is held.

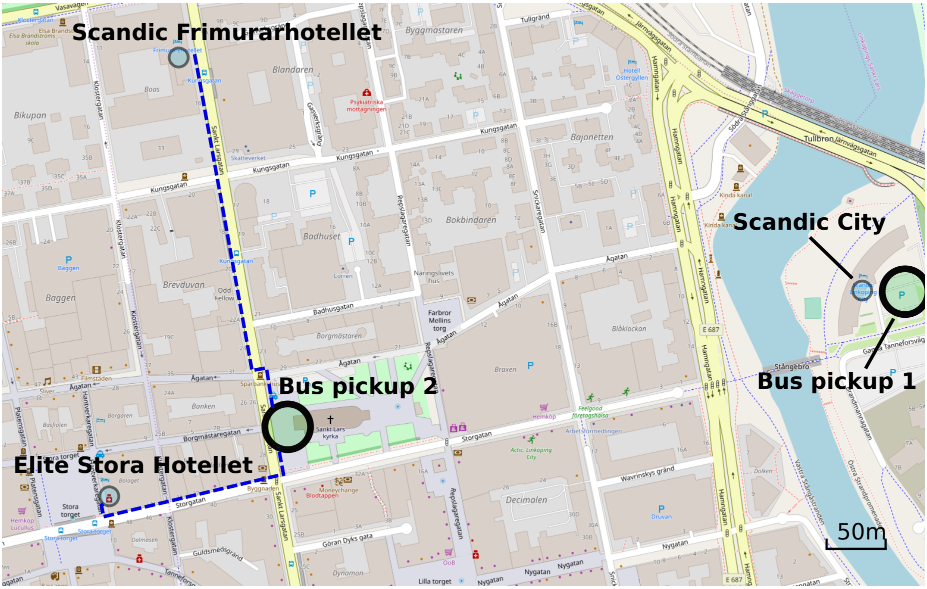
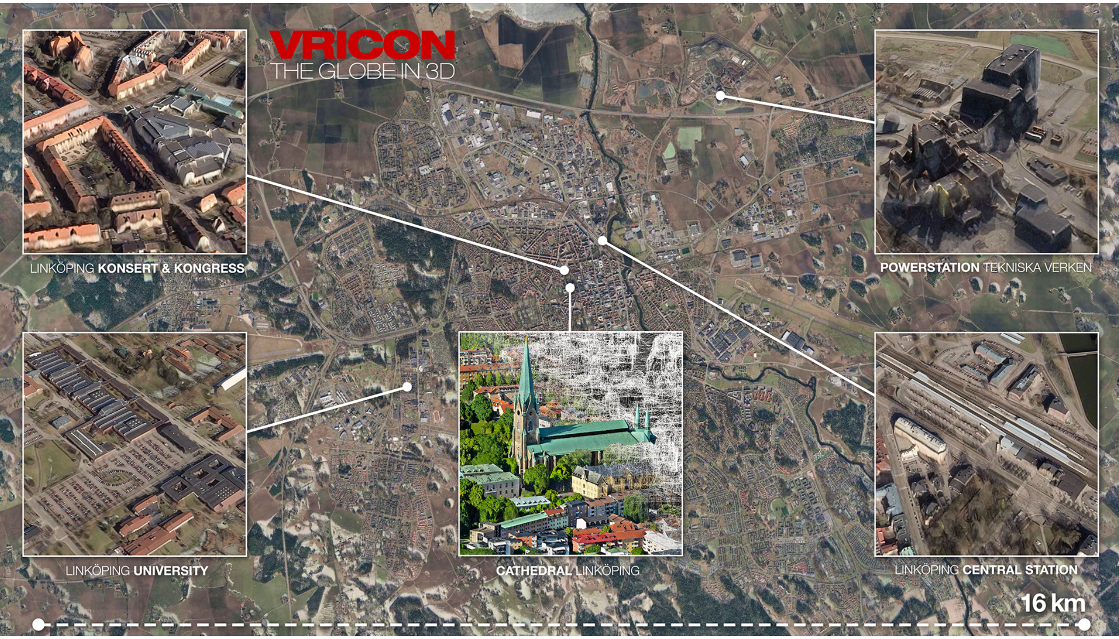


Figure 3: Downtown pickup place

Notes


VRICON
THE GLOBE IN 3D
LINKÖPING KONSERT & KONGRESS
POWERSTATION TEKNISKA VERKEN
LINKÖPING UNIVERSITY
CATHEDRAL LINKÖPING
LINKÖPING CENTRAL STATION
16 km

https://critis2019.on.liu.se