

**Long Term Cybersecurity research
Summaries of projects granted in the second NWO call for proposals (2014)**

Project number	CYBSEC.14.001 / 628.001.020	
Main Applicant	Prof. dr. R.J. Wieringa	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica Informatiesystemen
Project title	Learning from Incidents (LINC)	
Scientific summary		
<p>Dutch public telecom providers are required by law to register availability incidents with the Dutch Telecom regulator Agentschap Telecom (AT). Yearly summaries are submitted to ENISA, which compiles annual reports of telecom availability incidents in Europe. The incident database could be a lot more useful if it could be shared among telecom providers to help them improve the resilience of their infrastructure. However, the information in it is often incomplete, and it is extremely confidential. The goal of the LINC project is to develop techniques to extract reusable lessons learned about causes and resolutions of availability incidents from the database, that preserve confidentiality.</p> <p>We will develop an incident analysis method and an incident model that is usable in practice to report on the analysis and recovery of availability incidents. To ensure confidentiality, these lessons learned will be stated in terms of statistical information about the failure mechanisms of incidents without referring to the entire incident, and will be stored in a separate database that is readable by telecom providers. Use of this database must be confidential. Failure mechanisms are diverse, and may include technical as well as organizational mechanisms, as well as natural disasters. Furthermore, we will develop a risk assessment method by which telecom providers will be able to relate these lessons to their own infrastructure in order to identify possible improvements.</p> <p>To ensure usability, we will develop the methods and database iteratively together with AT and with close cooperation with telecom providers and other stakeholders such as ENISA.</p>		
Applicable NCSRA themes		
<ul style="list-style-type: none"> • Forensics and incident management • Risk Management, Economics and Regulation • Secure Design and Engineering 		