



GI-Sicherheit 2016: International Workshop on Security, Privacy and Reliability of Smart Buildings

Speaker: Kirsten Messer-Schmidt M.A., Dr. Heinrich Seebauer AK KRITIS / GI

Keynote Title: Automated buildings: Just smart or maybe critical too?

An attempt of the GI working group KRITIS (AK KRITIS) to apply characteristics of critical ITC infrastructures to building automation

With permanently increasing automation and digitalization of all spheres of private and public life, “dependability and reliability” of ICT infrastructure are getting a complete new meaning.

Systems which had been self-contained as e.g. cars, buildings or industries are linked to other formerly stand-alone systems. System boundaries are newly defined. Data are linked and exchanged beyond system boundaries and a boosting level of process efficiency, velocity of communication and self-determination is becoming possible.

But with shifting system boundaries and new interdependencies between systems, ICT can become a critical infrastructure in entirely unexpected and seemingly trivial contexts.

It is generally agreed that a nuclear power plant is a critical infrastructure and consequently the operating ICT systems need elevated attention. But the classification is not always as easy as in this case, where the consequences of a malfunction are linked in our collective consciousness with similar threats and images. Damage emanates from a distinct entity. It is supposed to be direct and is hence imaginable. The classification as a critical infrastructure is carried out almost intuitively.

To AK KRITIS' understanding an infrastructure is critical if a deviation from normal operation (incident, breakdown) is dangerous to a society's existence. The definition of “danger to a society's existence” is to be provided by a society itself e.g. by means of its political institutions.

But how can we identify a critical ICT infrastructure? Can building automation be a critical ICT? Is it possible to examine the controlled system – “smart building” and the ITC which controls the system – “building automation” separately? And what can we do when having identified a critical ICT infrastructure?

AK KRITIS has developed a set of generic characteristics of critical ICT infrastructures which can help to answer the above mentioned questions. To show the practicability of these characteristics they are applied to the ICT infrastructure of an exemplary automated building scenario in order to find out its criticality.

If criticality of an ICT infrastructure is given and a failure can be dangerous to a society's existence, the responsibility which comes along with the development and operation of such an infrastructure exceeds personal and company boundaries.

AK KRITIS shows which widespread risks can be avoided to significantly enhance dependability and reliability of critical ICT infrastructures.