

GESELLSCHAFT FÜR INFORMATIK E.V.



Automated buildings: Just smart or maybe critical too?

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

**Heinrich Seebauer
GI AK KRITIS**

- Working committee „Critical information and communication infrastructures” of GI’s committee „Management of Information Security“
- Our main objectives are the development
 - of methods and procedures for the identification of critical ICT
 - of principles for design, operation and maintenance of critical ICT
- The committee is directed by a team of five
 - Speaker: Kirsten Messer-Schmidt, excepture and Deputy: Klaus Kirst, PTLV
 - Dr. Heinrich Seebauer, oligo; Dr. Steffen Wendzel, Fraunhofer FKIE; Michael Wiesner, CTNS Security GmbH

Moving ahead

- increasing automation and digitalization
 - nearly all spheres of private and public life affected
- dependability and reliability of ICT is getting more important than ever

Positive effects of technical progress



- traditional processes become more efficient
- complete new services become possible
- communication is getting faster and easier
- economic growth
- ...

It's possibly not as good as it seems ...



- growing complexity due to tightly linked systems
- increasingly non-transparent relations between ICT components
- pressure to be innovative vs. inertia of traditional systems
- implicit pressure to go along with new technical developments
- lack of support for companies and organizations
- overly optimistic estimation of ICT reliability

- **IT risks increase more or less unnoticed ...**

Critical infrastructure



- qualification as such often intuitively
- widely accepted as critical infrastructure are e.g.
 - nuclear power plants
 - telephone networks
 - drinking Water Supply Systems
- example: Germany's „IT Sicherheitsgesetz“ doesn't provide a precise definition of the term „CI“

Gradually degrading systems

- Mergers & acquisitions elevate ICT systems complexity to new levels.
- Outsourcing of internal processes creates new interfaces.
- vanishing know-how of legacy systems
- replacement of outdated hardware components
- improvised interfaces due to missing specifications
- Impact assessments become more intricate.
- Operations are becoming more and more complex and error-prone.

AK KRITIS' definition



A system is called a **critical infrastructure** ...

... if deviations from normal operation impose a threat
to the existence of society.

Criteria for critical ICT infrastructures



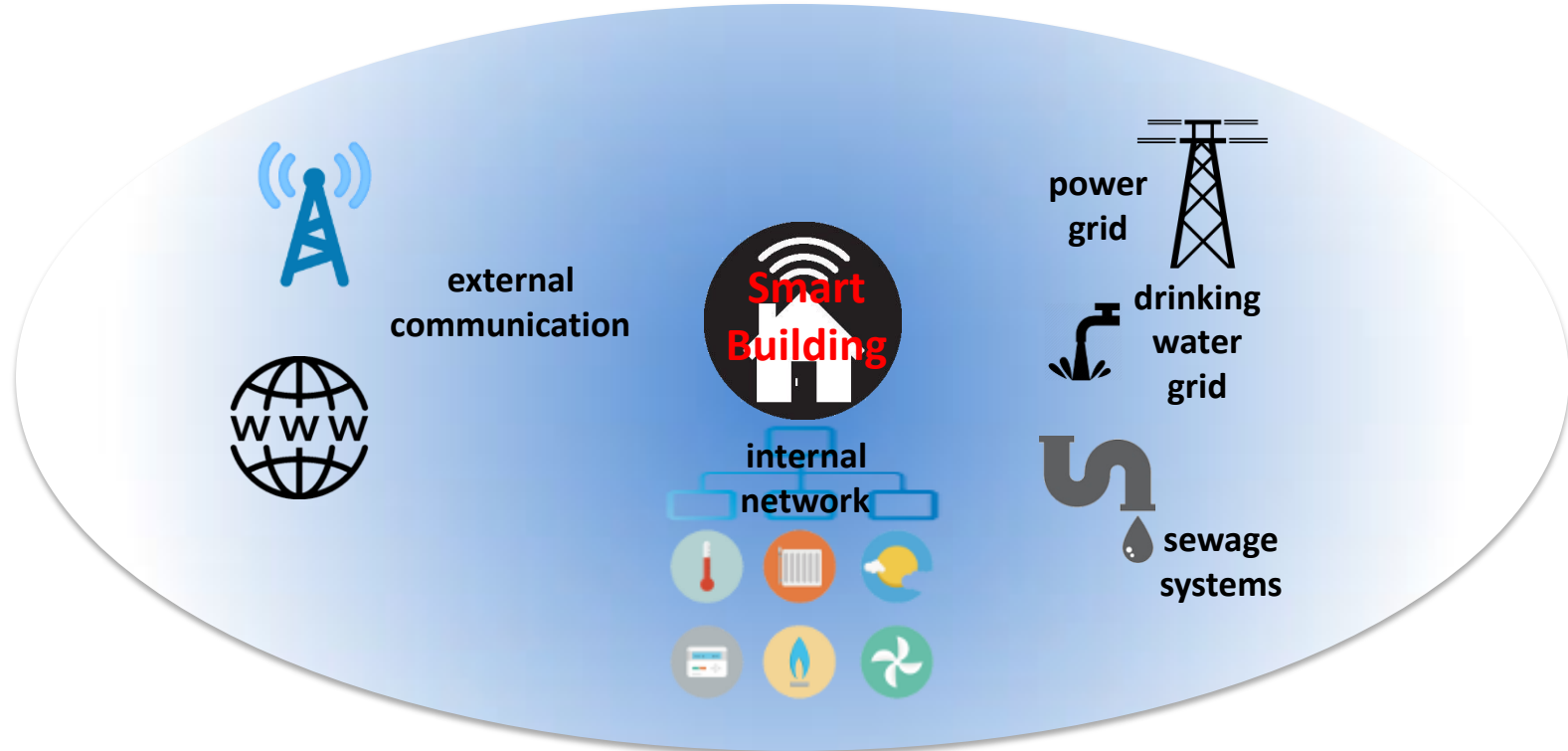
An ICT system X is called a critical ICT infrastructure, if

- it is itself a critical infrastructure

or if it controls some system Y, and

- a disruption of Y affects a significant number of people
- Y delivers essential services for a society
- Y has broad coverage or geographical distribution
- Y cannot be substituted at short notice, or
- Y serves one or more critical downstream systems (single or in combination)

What about buildings?



Example ...



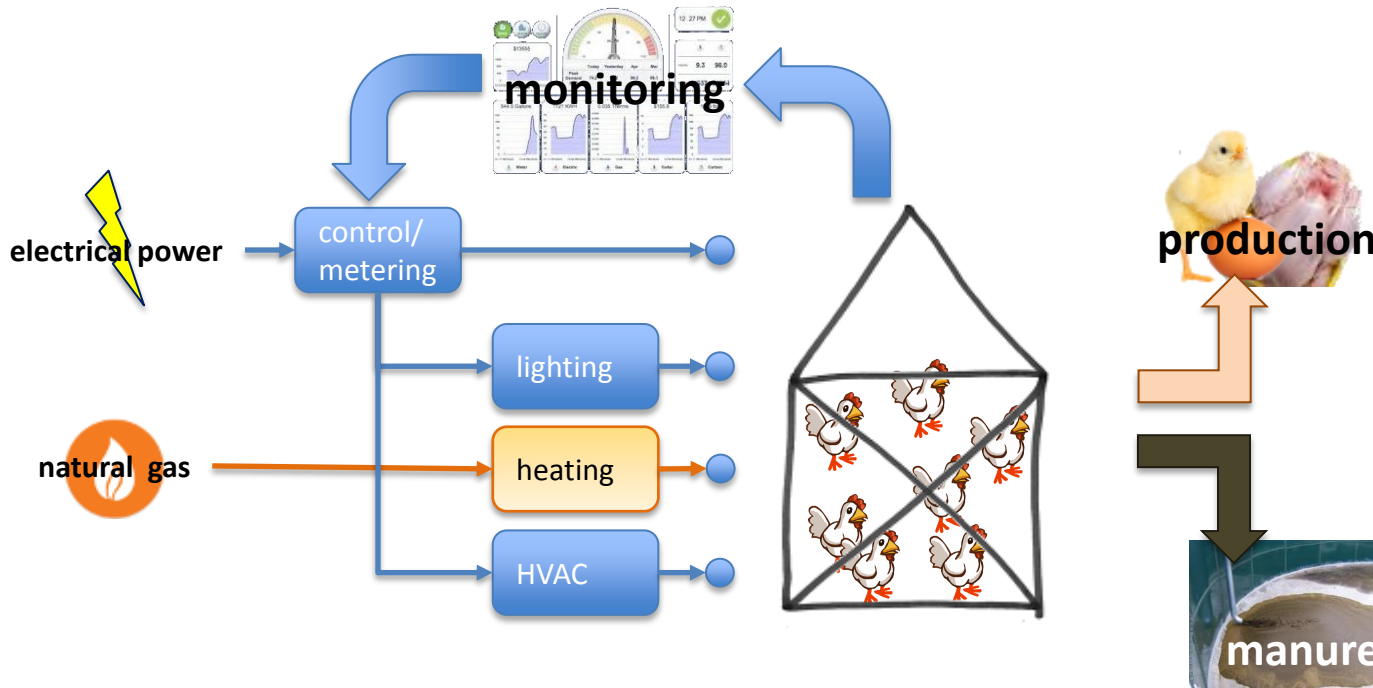
Connect two buildings



Building #1 provides its inhabitants with

- air condition,
- heating,
- nutrition,
- drinking water,
- light.

Building #1: Chicken house



Off the shelf system

- built by professional contractor
- based on industrial SPC
- regularly maintained
- ICT well tried & tested

Works flawlessly
availability: 99,99%

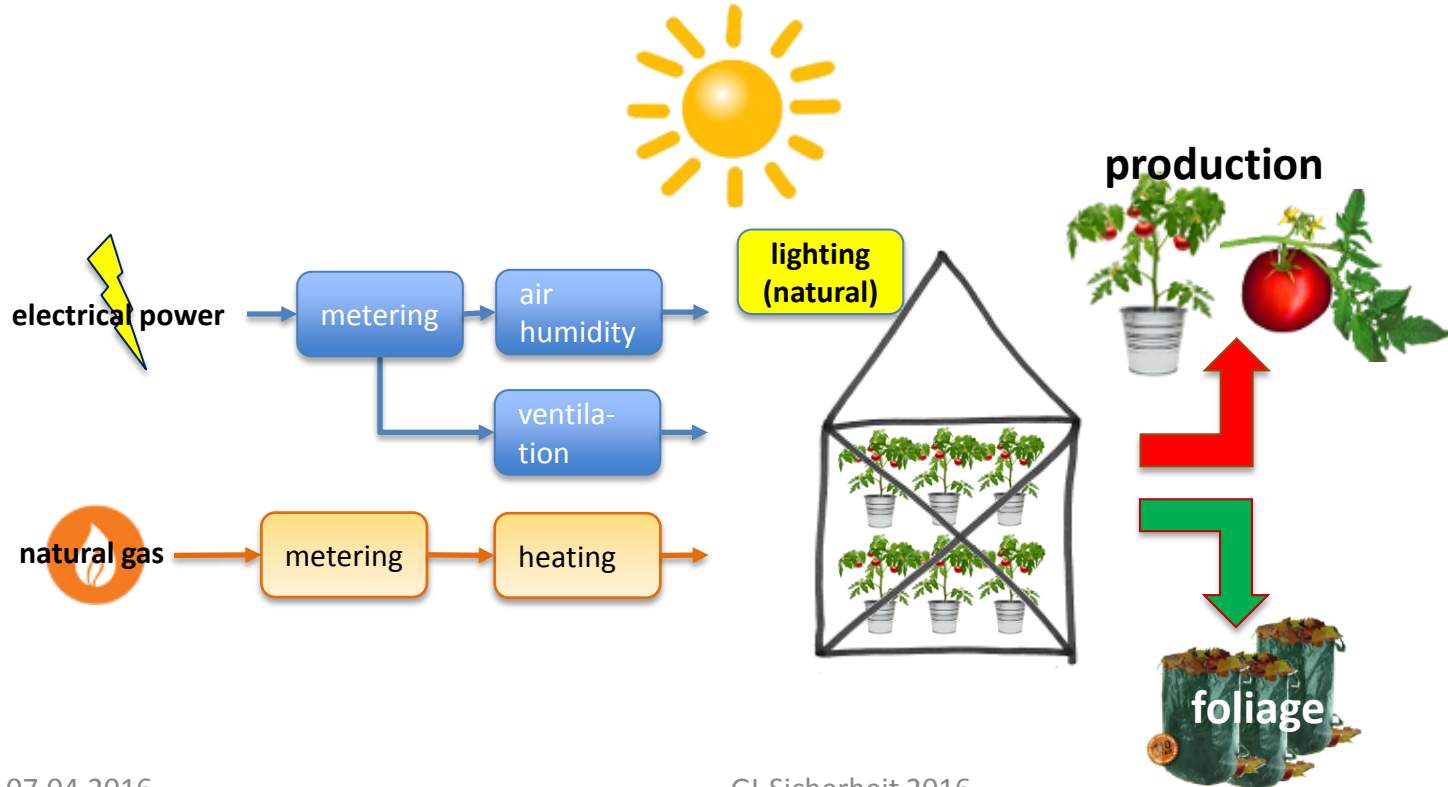
Connect two buildings



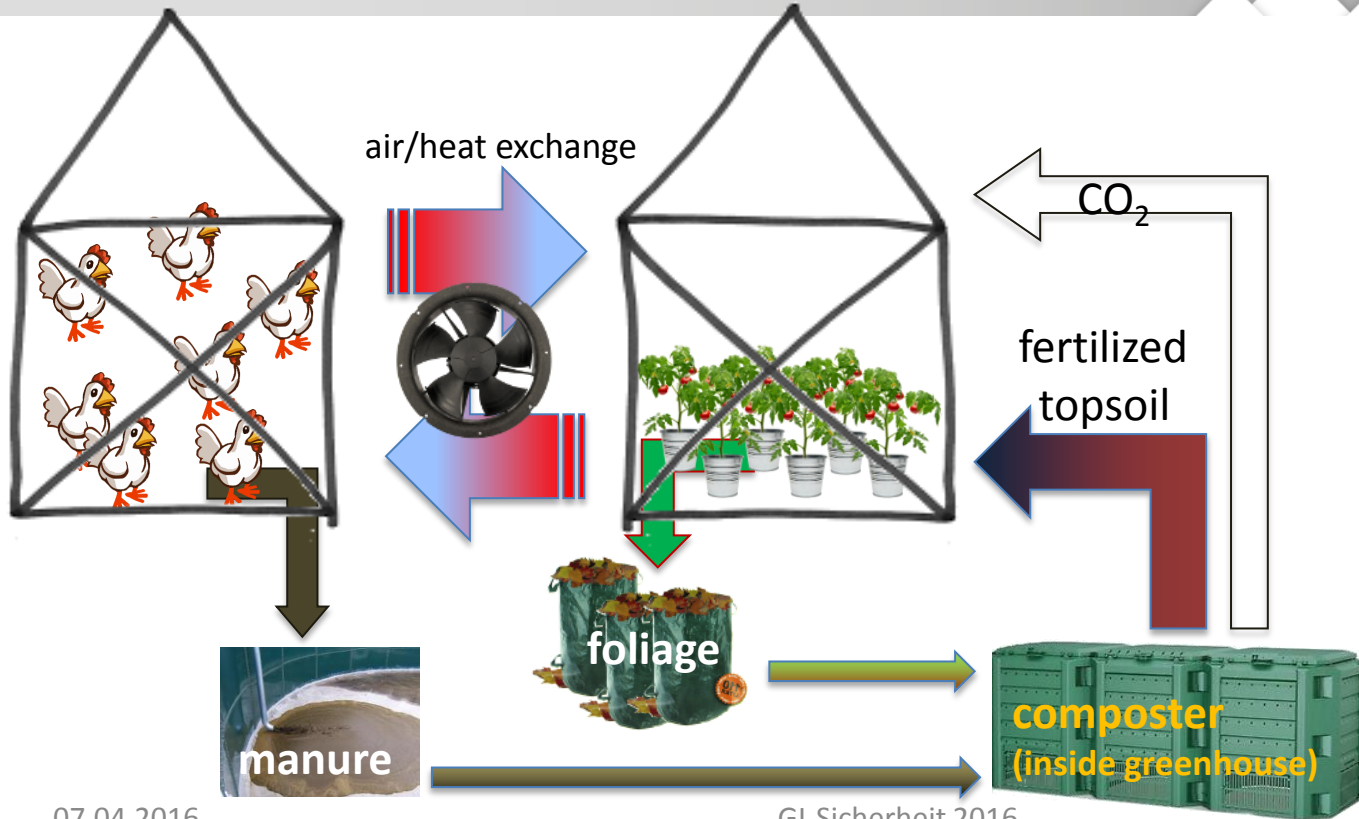
Building #2 provides its inhabitants with

- air condition, heating,
- nutrition, drinking water,
- light, shadowing

Building #2: Greenhouse



Connected buildings



More or less impromptu system

- built by farmer's son
- maintained in case of necessity
- ICT components off the shelf

availability not monitored

Competitors don't sleep



- Competitors' objective: interrupt production
 - reconnaissance gives hints to vulnerable system
 - hires some black hat
 - hacker attacks greenhouse

The attack

- The greenhouse's ICT capitulates after short time.
- approach:
 - heat greenhouse to $>35^{\circ}$ by night
 - raise relative humidity to min. 85%
 - cool down before dawn
- effects: water condenses on plant's leaves



Murphy's law is still valid



- Composters are placed **inside** the greenhouse.
- Composters at $>35^{\circ}\text{C}$ produce **A LOT OF CO_2** .
- Tomatoes cannot lower **CO_2** during the night.
- Cooling down the greenhouse involves exchange of air between the two buildings.

Critical or not?



LOKAL AFFAIRS

Mysterious Death of Over 3.000 Chickens

State attorney: Owner probably neglected security measures

Growham/hse – A shattering sight awaited the owner of a chicken farm in Growham, DCF in the morning. The owner found more than 3000 chickens dead on the spot.

The state attorney general has announced that the owner of a chicken farm in Growham, DCF, is likely to face criminal charges for the mysterious death of over 3,000 chickens. The attorney general stated that the owner had neglected security measures, which led to the deaths of the chickens. The owner is currently under investigation and is expected to be charged with negligence. The state attorney general is currently reviewing the case and is expected to announce the charges in the coming weeks.

The state attorney general has announced that the owner of a chicken farm in Growham, DCF, is likely to face criminal charges for the mysterious death of over 3,000 chickens. The attorney general stated that the owner had neglected security measures, which led to the deaths of the chickens. The owner is currently under investigation and is expected to be charged with negligence. The state attorney general is currently reviewing the case and is expected to announce the charges in the coming weeks.

What is your opinion?

Is this chicken shack a critical infrastructure?

Let's apply the KRITIS-criteria ...



An ICT system X is called a critical ICT infrastructure, if

- it is itself a critical infrastructure

or if it controls some system Y, and

- a disruption of Y affects a significant number of people
- Y delivers essential services for a society
- Y has broad coverage or geographical distribution
- Y cannot be substituted at short notice, or
- Y serves one or more critical downstream systems (single or in combination)

true?



Conclusion



Fortunately this smart building is NOT a critical infrastructure.

But ...

- if it were an airport?
- or a data center?
- or a nuclear power plant?

Any questions?

Feel free to contact AK KRITIS:
info-ak-kritis@secmgt.de

Thank you very much for your attention!