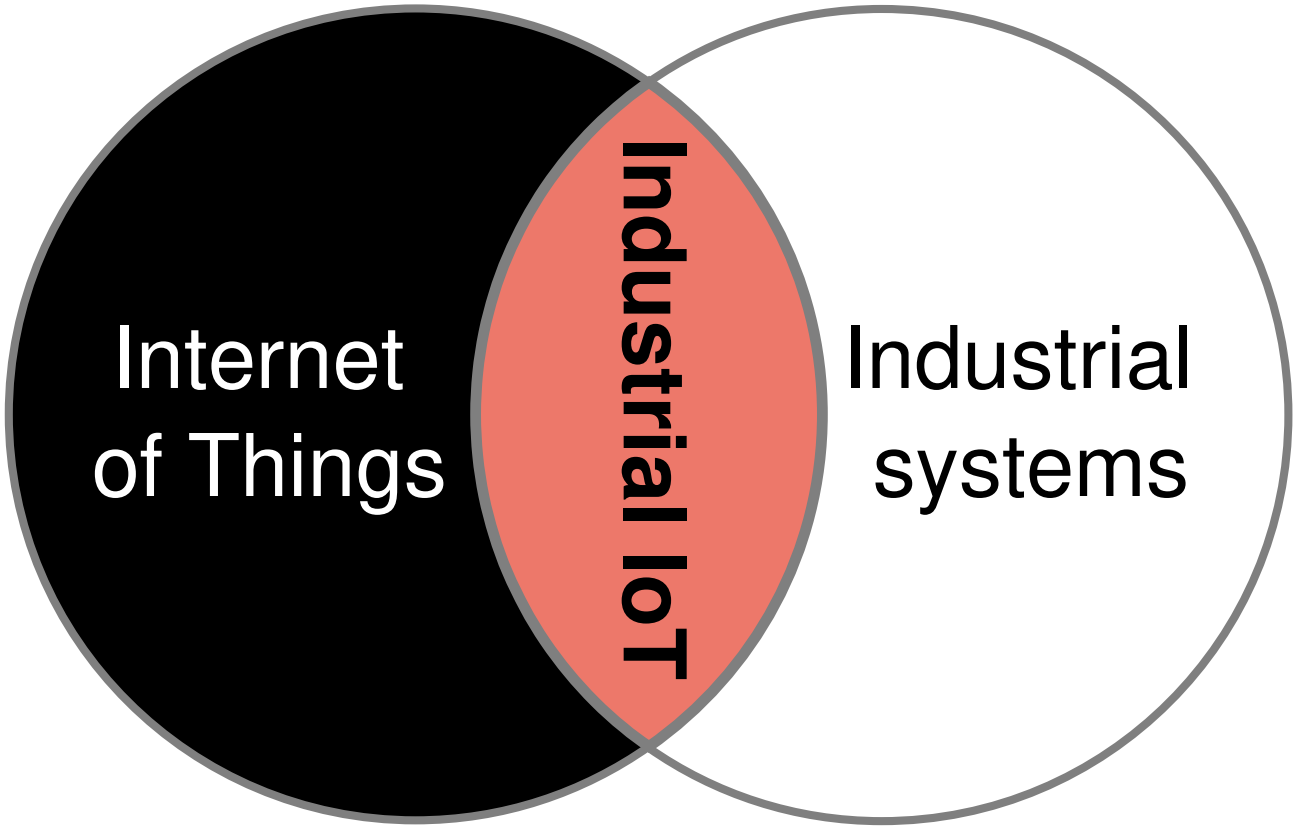
A Distributed Systems Perspective on Industrial IoT

Konrad Iwanicki
University of Warsaw

ICDCS 2018, Vienna, Austria, July 3, 2018

Industrial IoT



Industrial IoT

The adoption of IIoT has lagged compared to the adoption of consumer-oriented IoT gadgets.

IIoT is about distributed systems...

An industrial IoT system is a collection of largely independent interconnected computing elements that monitor or control some physical resources in a way that appears to the users of the system as an operation of a single facility realizing a certain business process.

IIoT is about distributed systems...

An industrial IoT system is a collection of largely independent interconnected computing elements that monitor or control some physical resources in a way that appears to the users of the system as an operation of a single facility realizing a certain business process.

IIoT is about distributed systems...

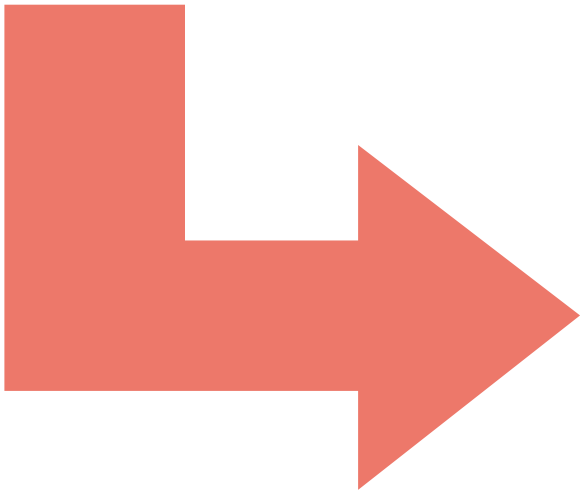
An industrial IoT system is a collection of largely independent interconnected computing elements that monitor or control some physical resources in a way that appears to the users of the system as an operation of a single facility realizing a certain business process.

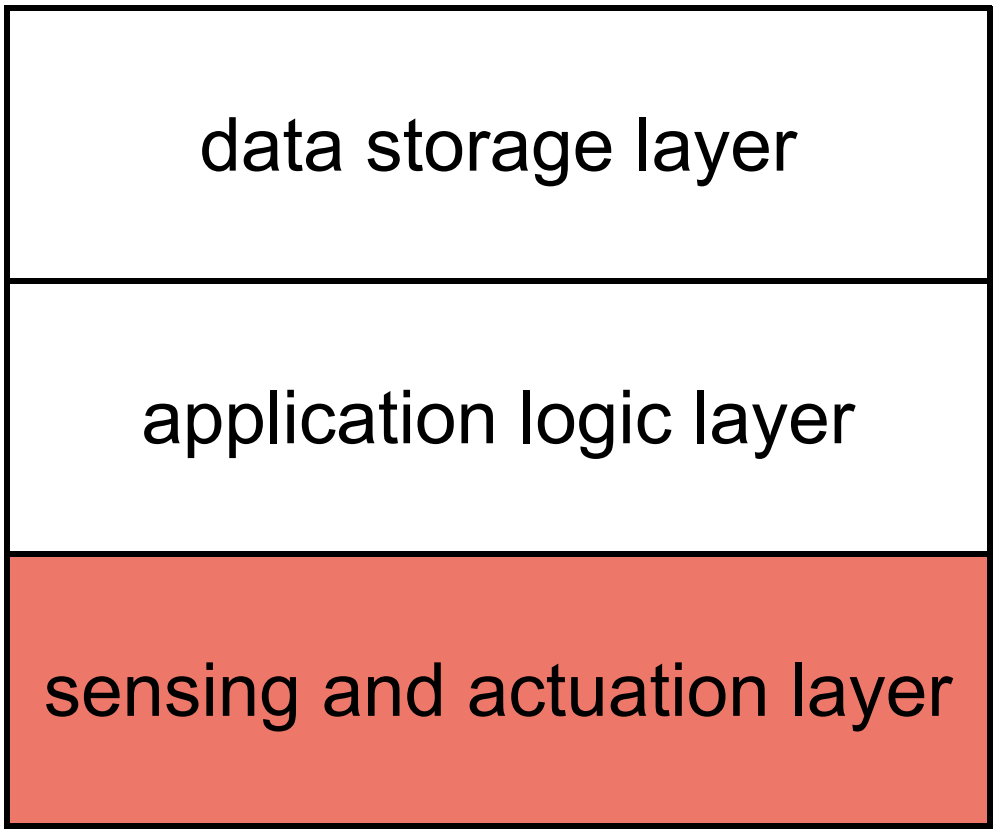
… but peculiar ones

Tight coupling between IIoT systems and the physical objects they monitor and control.

… but peculiar ones

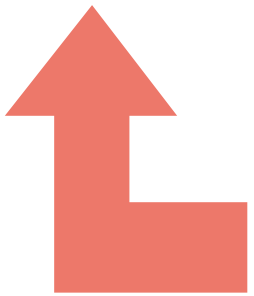
Tight coupling between IIoT systems and the physical objects they monitor and control.

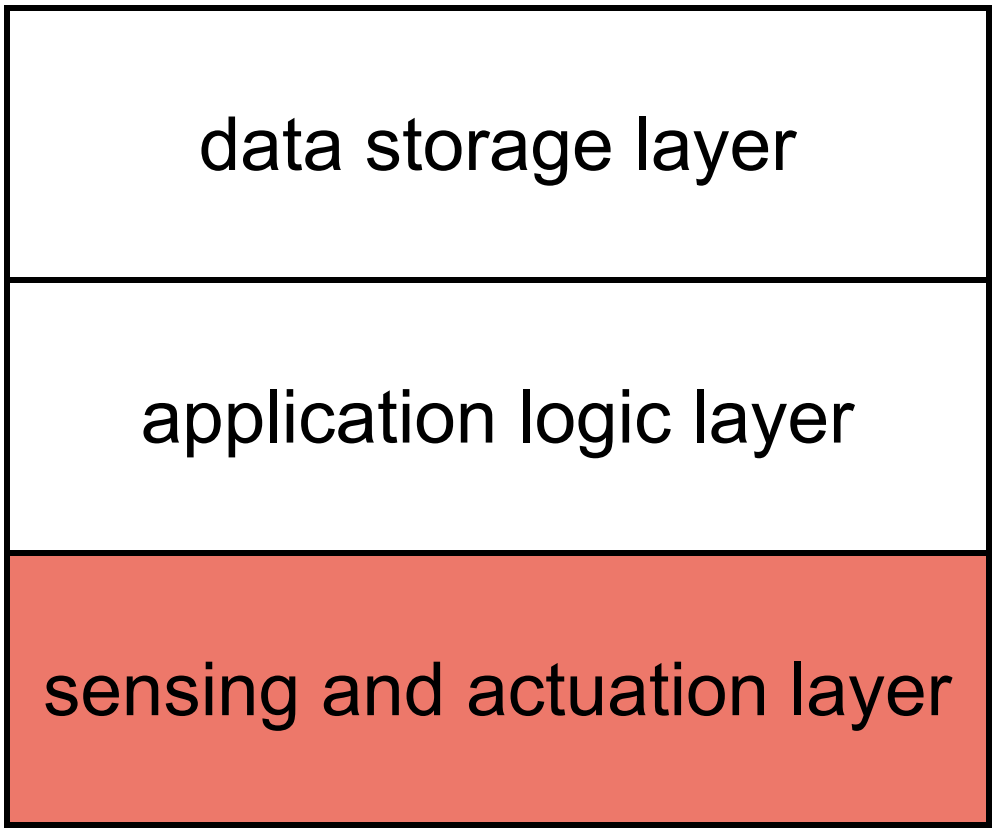




… but peculiar ones

- Highly constrained resources and heterogeneity.
- Fixed physical placement.
- Operating conditions different from “sterile” data centers.





Interoperability

- IIoT systems aim to transform business processes but:
  - Existing infrastructure is hardly ever entirely replaced.
  - Various IIoT solutions are heterogeneous.

Interoperability

with legacy systems

with other IIoT solutions

Interoperability

- Solution: standardization
  - necessary in many cases...
  - ...but does not address all issues (e.g., legacy components).
- Possible complementary solution: middleware
  - leverage the experience from enterprise application integration.

Scalability

- IIoT systems are often deployed incrementally:
  - small tests
  - gradual rollout

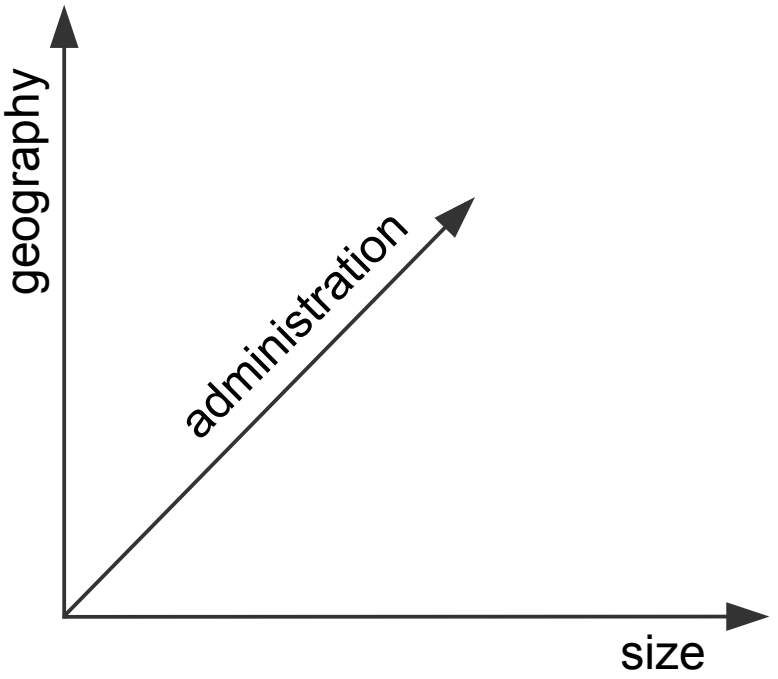
Pros:

- Minimal disruption to business processes
- Smaller risk of calamities

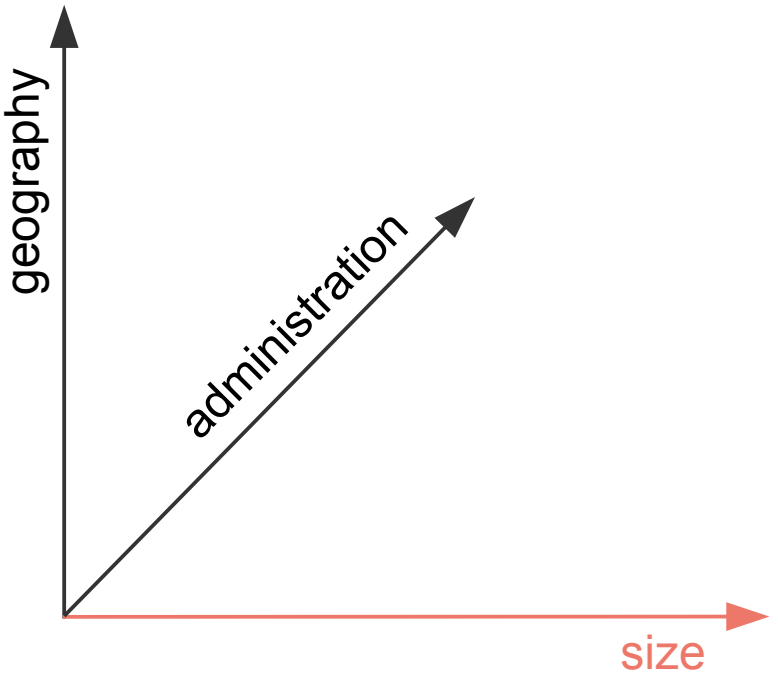
Cons:

- A system has to tolerate a growth of a few orders of magnitude.
- Initial overprovisioning may not be an option.

Scalability

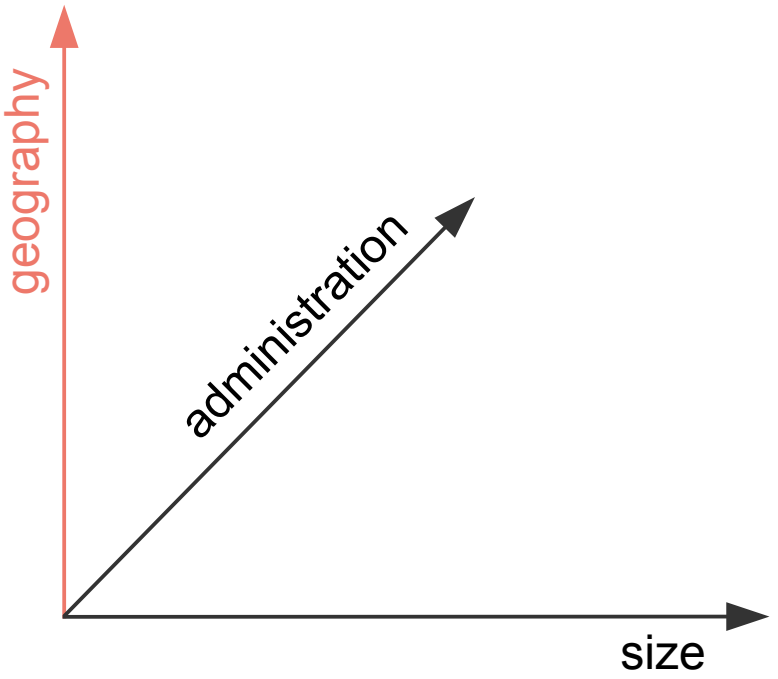


Scalability



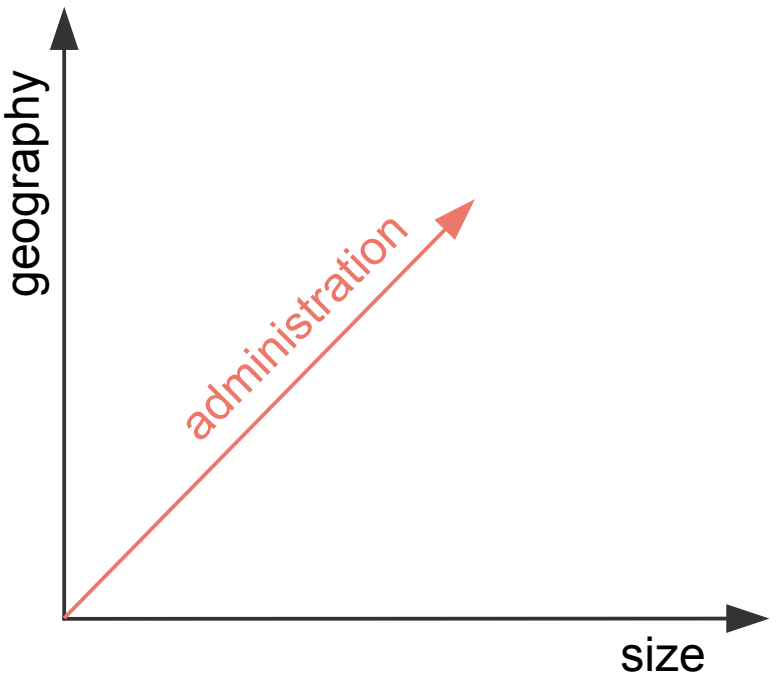
- provisioning more resources often infeasible
- replication and load balancing of limited use
- software architecture usually tightly coupled with system architecture

Scalability



- energy-latency trade-off
- traffic depends on exact placement of sensing and actuation points

Scalability



- sharing physical spaces => conflicts, e.g.:
  - wireless medium
  - sensing and actuation points

Dependability

IIoT must be dependable.

Dependability

- reliability
- safety
- availability
- maintainability
- security

Concluding remarks

- From a distributed systems perspective, IIoT poses a number of challenges, notably in:
  - interoperability,
  - scalability,
  - dependability.
- However, this requires collaboration with industrial partners.

Thank you

Q&A during the panel.

The presented research was supported by the National Center for Research and Development (NCBR) in Poland under grant no. LIDER/434/L-6/14/NCBR/2015.

The National Centre
for Research and Development

LIDER

Dependability

- reliability
- safety
- availability
- maintainability
- security

- Continuity of correct behavior.
- Maximized by:
  - individual components
  - redundancy

Dependability

- reliability
- safety
- availability
- maintainability
- security

- Something wrong does not lead to a catastrophe.
  - Need not be binary!

Dependability

- reliability
- safety
- availability
- maintainability
- security

- Readiness for usage.
  - Relevance of the CAP theorem.

Dependability

- reliability
- safety
- availability
- maintainability
- security

- Ease of changing a system's configuration.
  - Lot of work done
  - There are still some open problems

Dependability

- reliability
- safety
- availability
- maintainability
- security

- Difficult to attack.
  - The “s” in “IoT” stands for security.
  - In IIoT the situation is somewhat better.