AMI Topology and its Security

Manish Shrestha

Overview of Electricity Grid

- Generation
- Transmission
- Distribution

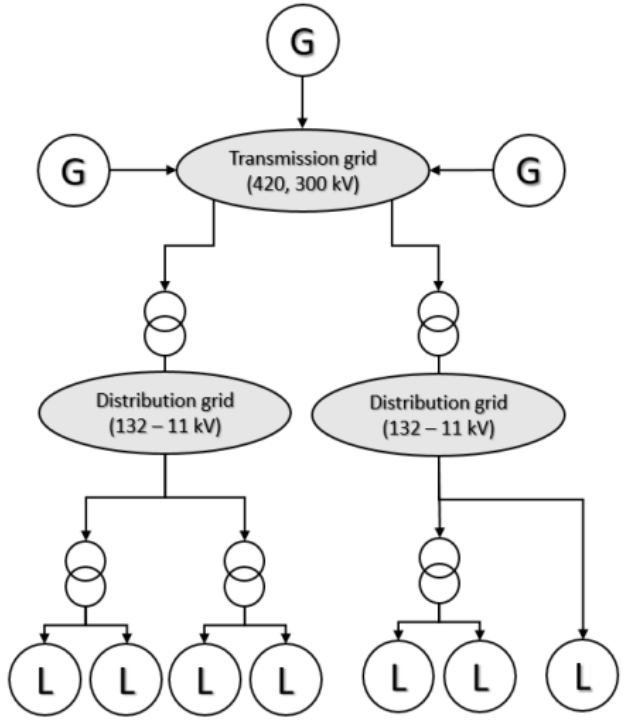
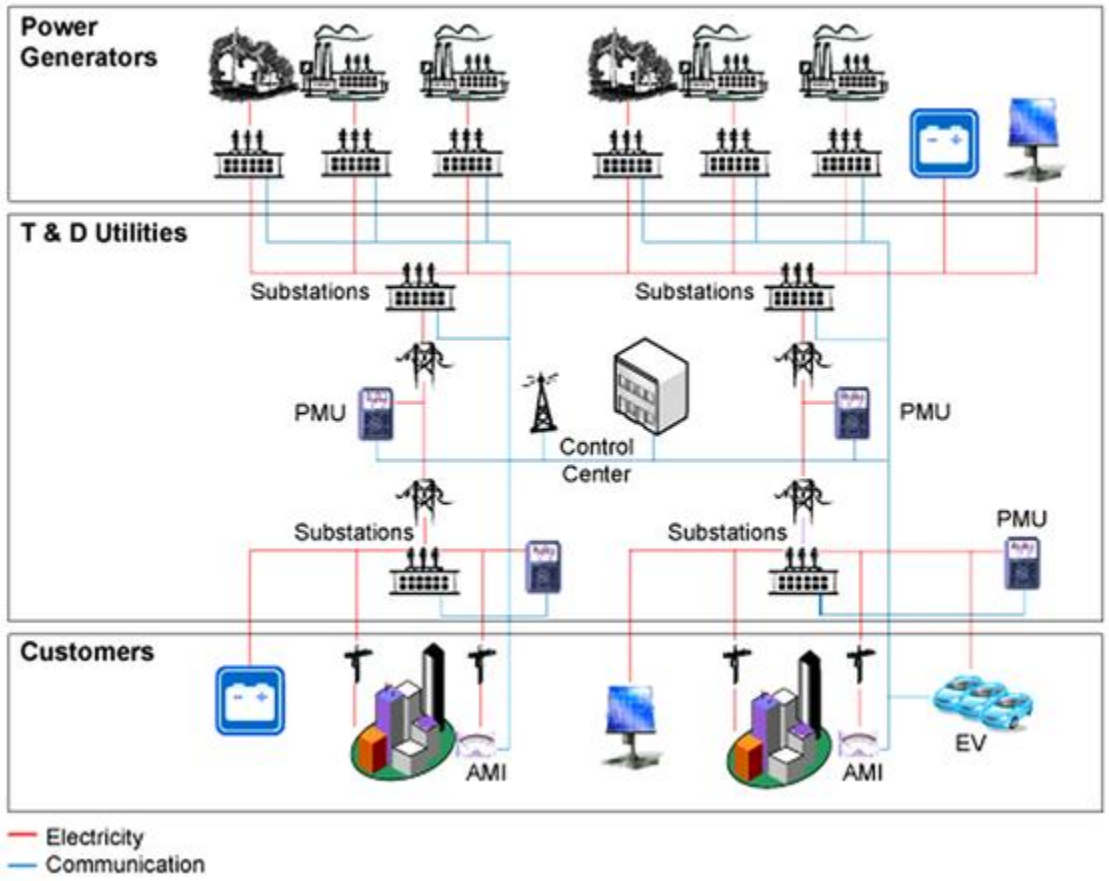


Figure 1.1. Simplified representation of the physical electric power system

Smart Grid


Power Generators
T & D Utilities
Substations
Substations
PMU
Control Center
PMU
Substations
Substations
PMU
Customers
AMI
AMI
EV
Electricity
Communication

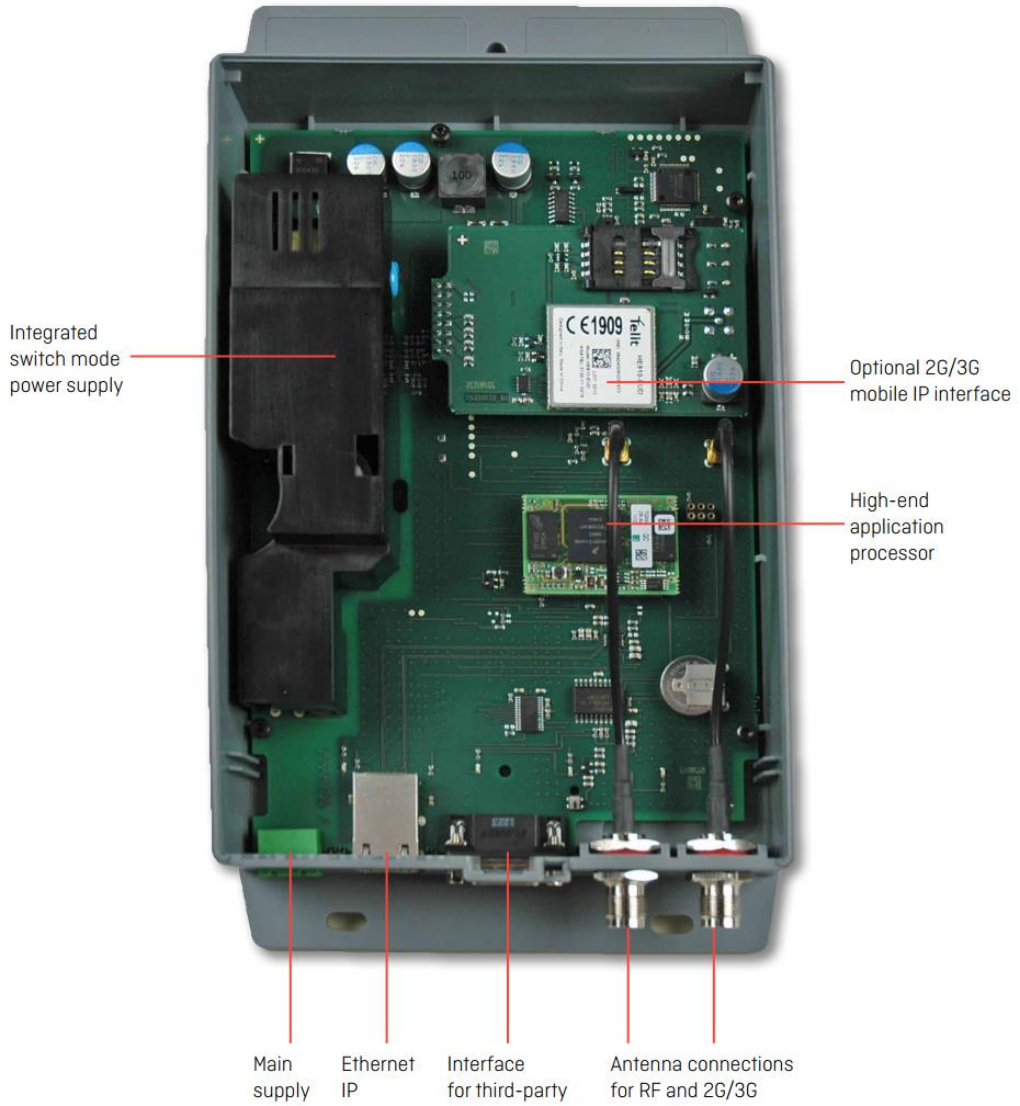
Some Communication technologies in Smart Grid

- Wireline technologies
  - PLC
  - DSL
  - Fibre Optic
- Wireless Technologies
  - IEEE 802.15.4 (Zigbee, ISA 1000.11a,...)
  - Wi-Fi
  - WiMAX
  - GSM (2G, 2.5G, 3G...)
  - EN 13757 (Wireless m-bus)

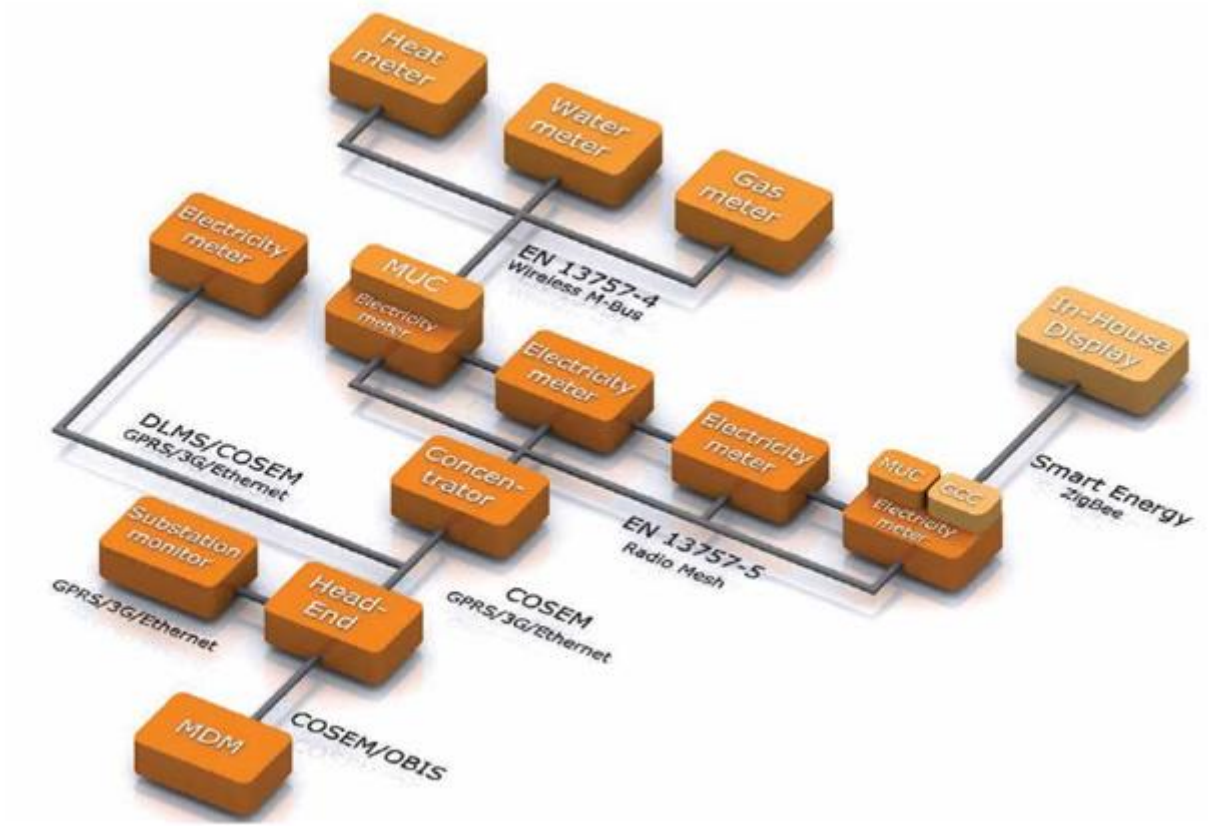
EN13757

EN 13757	Propose
1	Basic data communication between meters and collectors
2	Physical layer requirement for wired M-bus
3	Application Layer
4	Physical and Data Link Layers for wireless M-bus
5	Relaying and routing for range enhancement
6	Local bus for short distance wired links

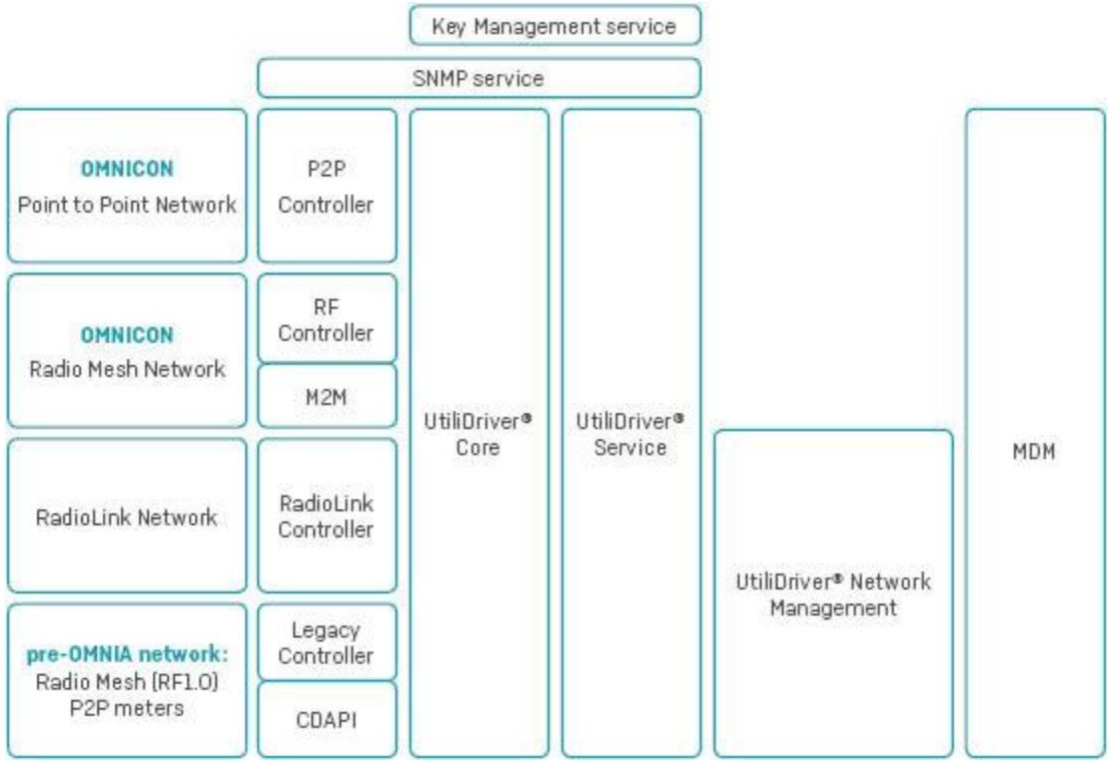
- Smart meter
- Concentrator
- Head-end system
- MDM system
- NAN
- Cellular networks



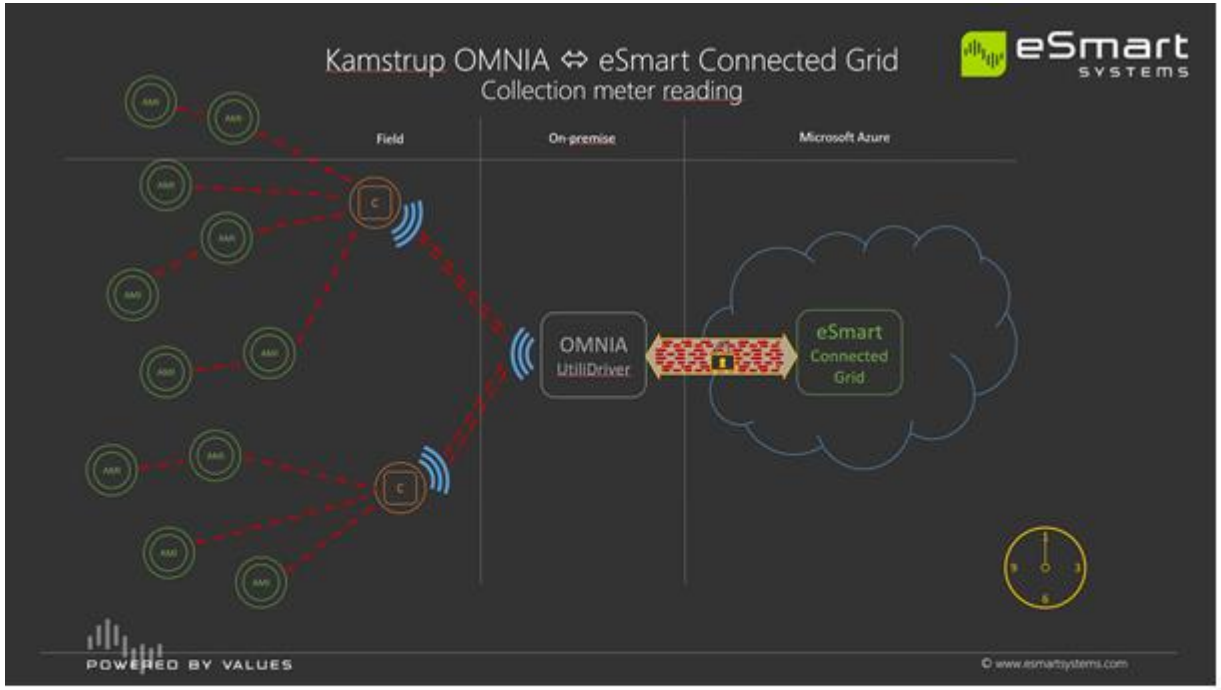
Omnia Nework

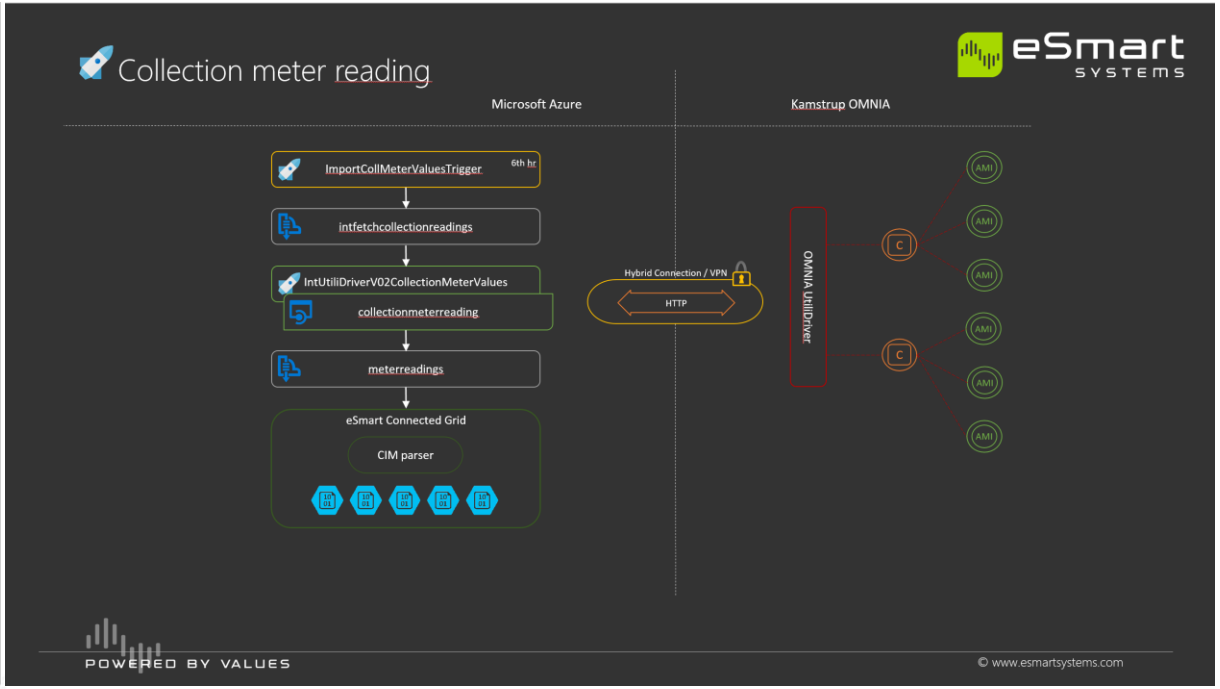


Utilidriver



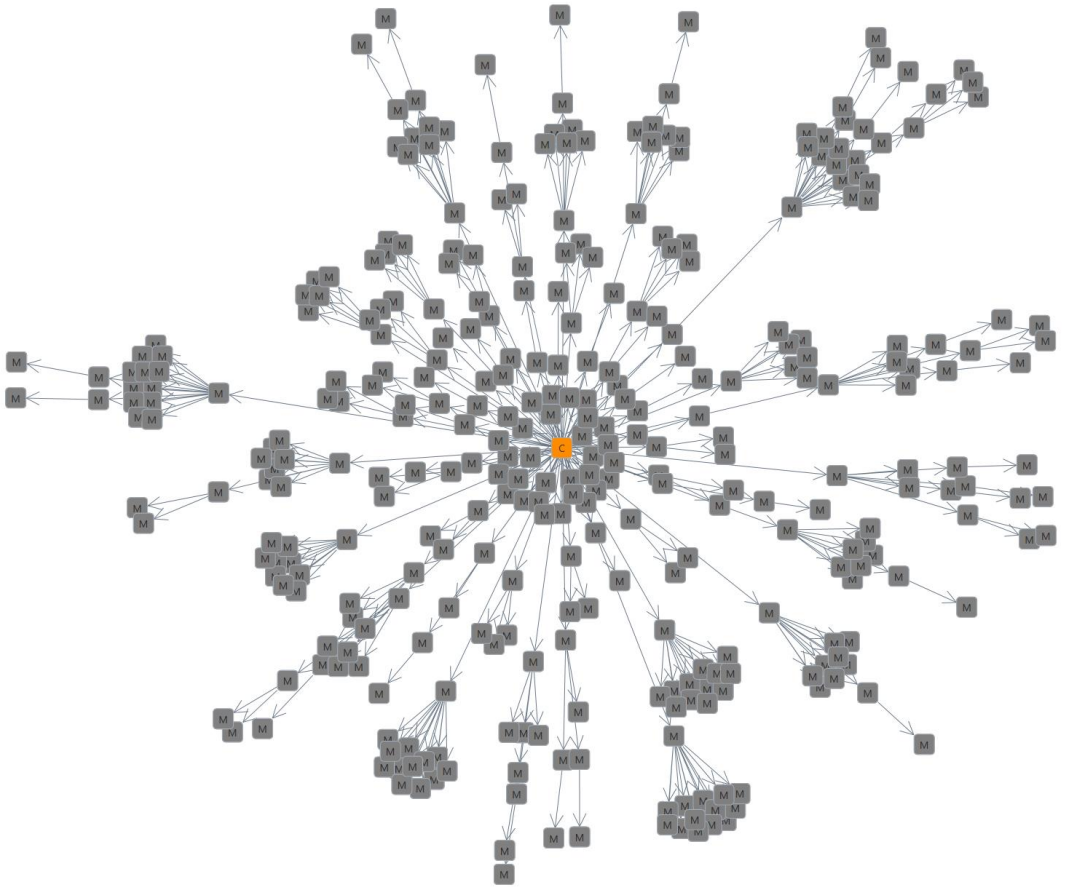
Flow of Information





Attack Interface

- Open Ports
- Default Settings
- Radio Network
- Cellular Network



Assets to protect

- Physical Ports
- Stored metering data (consumption, logs, alarms)
- Encryption keys
- Communication channel
- Firmware/updates
- API
- Physical location

What can we do?

- Proper key management
- Incident response, user training and awareness
- Use of private APN
- Physical Security and tamper detection
- Update/patch management
- Follow guidelines and best practices from designated organizations.
- Proper configuration
- Defence in Depth

Conclusion

- Several security risks exist
- Need of certification or minimum concrete standards requirements before choosing the vendors
- DSO collaboration with research institutions

References

- Brunschwiler, Cyrill. "Wireless M-Bus Security Whitepaper Black Hat USA 2013 June 30th, 2013.
- Kamstrup Documents http://www.products.kamstrup.com
- Zhou, Jiazhen, Rose Qingyang Hu, and Yi Qian. "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid." IEEE Transactions on Parallel and Distributed Systems 23.9 (2012): 1632-1642.
- Line, Maria Bartnes, Inger Anne Tøndel, and Martin G. Jaatun. "Current practices and challenges in industrial control organizations regarding information security incident management–Does size matter? Information security incident management in large and small industrial control organizations." International Journal of Critical Infrastructure Protection 12 (2016): 12-26.
- http://pages.silabs.com/rs/634-SLU-379/images/introduction-to-wireless-mbus.pdf