# Theme and Problem statement for Apogee 2016

02 Dec 2016

Veerendra Vasamsetty
Innovation Manager

Schneider Electric

THEME 1:

# Cyber Security for Industrial Control Systems

The implications of cyber security and the need for a comprehensive security strategy are now being acknowledged by more sections of the industry. This is because the increased number of cyber attacks and the potential disruption they can cause have made security risks now very much part of operational risk.

However, it is becoming clearer that as cyber threats become more sophisticated, the impact of a cyber attack can be catastrophic for organizations, governments and the public. Potential monetary losses for industry are considerable. In the case of critical infrastructure, non-compliance (with increasingly stringent regulation on security) is unlikely to remain an option. In this context, organizations will be able to make the successful shift toward securing their operations by relying on industrial control solutions providers that treat security as core to their offerings. Of course, it is vital that organizations realize that this is a joint process where vendors and clients need to work together to achieve agreed objectives.

Security is never a one-time project and the process of learning and adapting is ongoing. However, once the need is acknowledged, an actionable plan is required to identify the biggest impact to the organization in terms of a security breach, locating which specific area of plant operations is linked to that impact, and minimizing or eliminating the main vulnerabilities related to that operation. This process can then help kick-start the much wider review of operations towards implementing a holistic Defence-in-Depth approach to cyber security.

Refer the attached whitepaper from Schneider-Electric to understand details in depth

# Problem Statements

Students are expected to study the emerging trends, standards and challenges in these areas.
They can present ideas  (Paper, PoC, Prototypes ) that are related to Cyber Security in Industrial Control Systems.

**Here are a few topics**

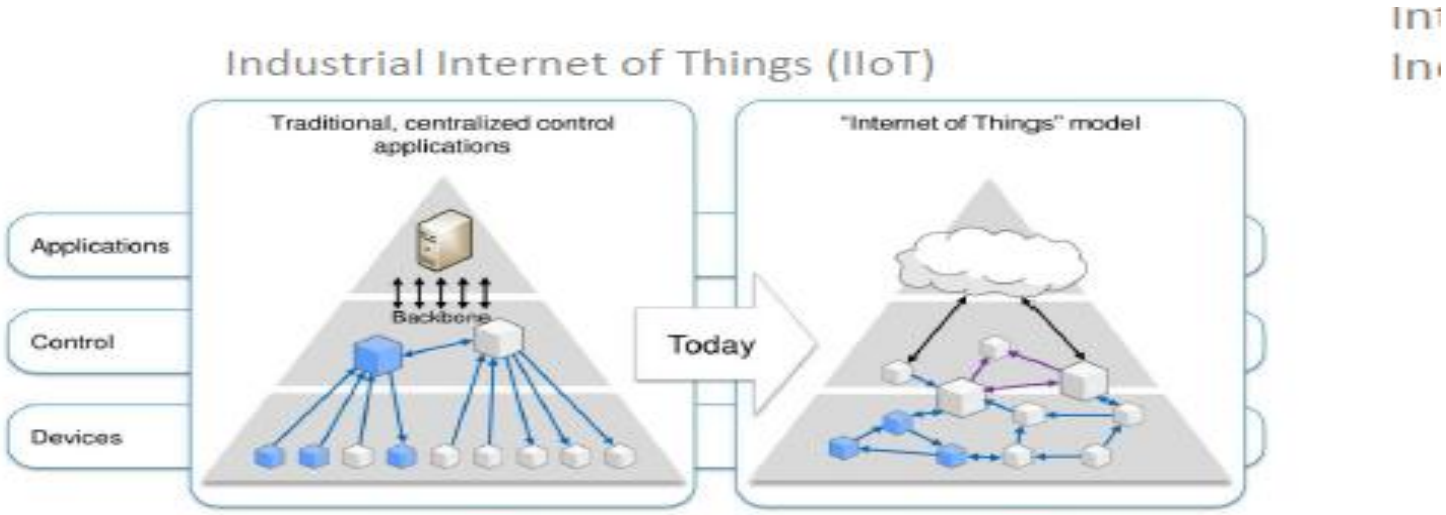
1.What are the Cyber Attack trends happening in Industrial Control Systems
2.How to Detect quickly and at the early stage the Origin of the Cyber Attack in Industrial Control Systems
3. Low Power Light weight Cryptography
4.Innovative ways to prevent Industrial Control Systems from Cyber Attacks
5.Next generation Futuristic Industrial Control Systems (fool proof systems from Cyber Attacks)

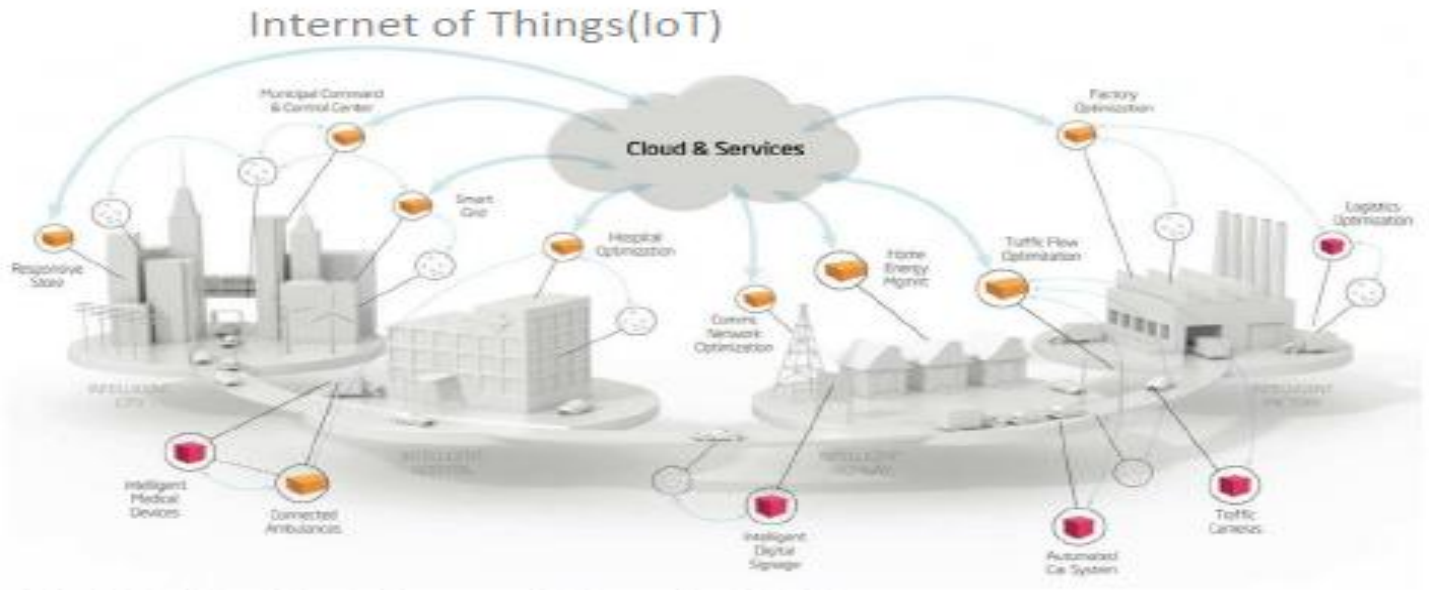
# References & useful information


Cyber Security of
ndustrial Control Sy

THEME 2:

# Internet of Things or Industrial Internet of Things




Schneider Electric - Veerendra Vasamsetty , AOCI\Innovation – Feb 2015

# Possible Topics

Students are expected to study the emerging trends, standards and challenges in these areas.
They can present ideas (Paper, PoC, Prototypes )that are aligned to IoT / IIoT.

**Here are a few topics**

1. On the go discovery of devices (Services, Negotiation, Connectivity etc..)
2. Device interaction governance
3. Integration with heterogeneous devices, diversified protocols / vendors / versions etc..
4. Analytics and Big Data integration with IoT / IIoT
5. Various challenges and advantages to adopt IIoT
6. Cyber security challenges and proposals
7. Trends & Ideas in Silicon Technologies that augment IoT / IIoT
8. Role of Mobility (Mobiles, Tablets, Cloud ) technologies in IoT / IIoT
9. Social / Personnel Impact by the IoT / IIoT
10. Role of IoT / IIoT in Smart Grids
11. Role of IoT / IIoT Smart Cities enabled
12. Application of Iot /IIOT in smart grid
13. Impact of Iot /IIOT in Building management/Hotel management/Hospital management
14. Impact of Iot /IIOT in e-commerce/supply chain/logistics management
15. etc..
16. etc..

Quick References:
http://ewweb.com/marketing/schneider-electric-s-take-internet-things
www.automationworld.com/schneider-electrics-approach-industrial-internet-things
http://software.invensys.com/solutions/internet-of-things/
http://www.zdnet.com/article/schneider-electric-digital-transformation-internet-of-things-sustainability-and-operational/
http://www-db.in.tum.de/teaching/ws1314/industrialIoT/
http://www.mcrockcapital.com/uploads/1/0/9/6/10961847/mcrock_industrial_internet_of_things_report_2014.pdf
http://techcrunch.com/2015/01/25/the-human-impact-of-the-industrial-internet-of-things/
http://blog.schneider-electric.com/tag/internet-of-things/


# Thank you!