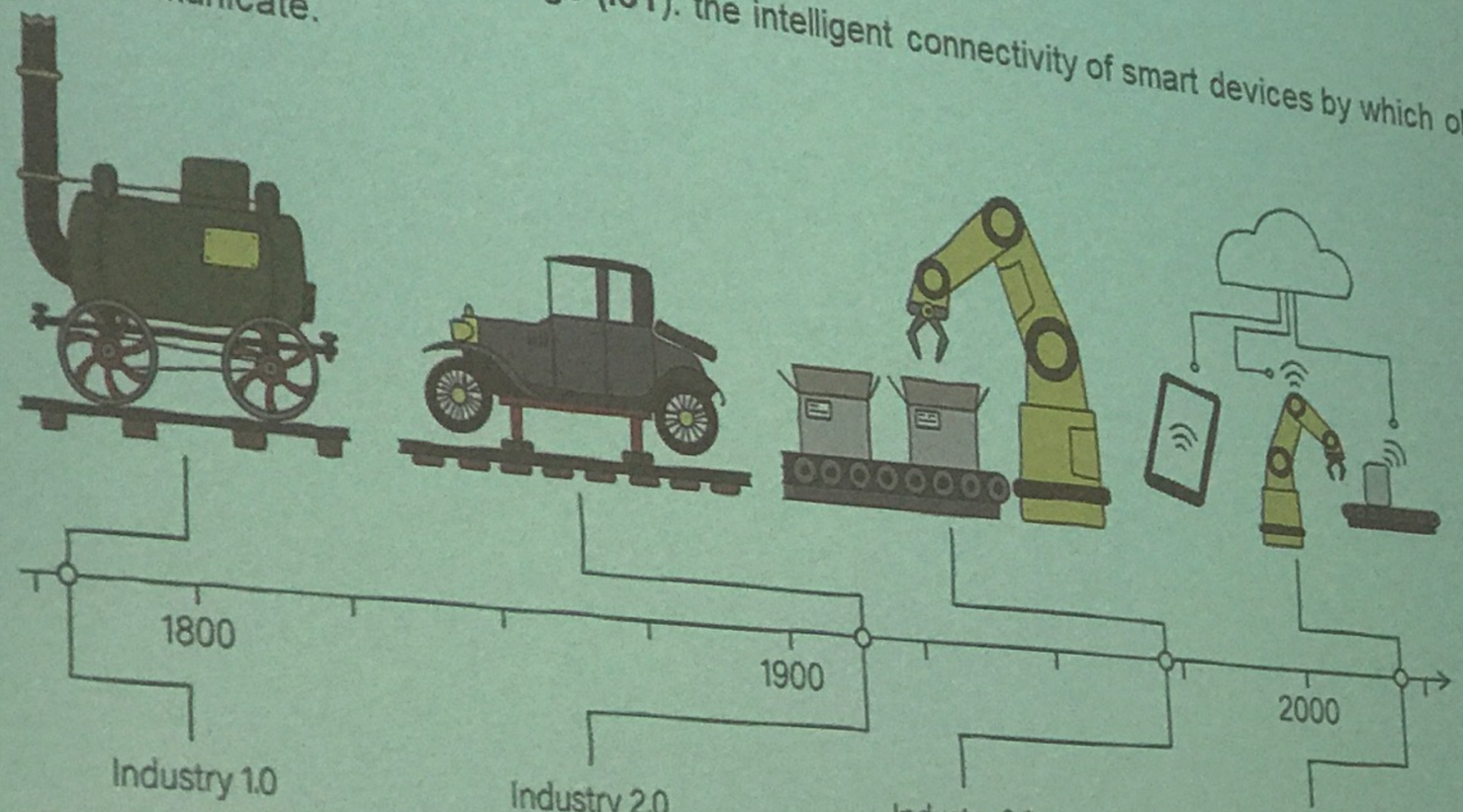
# Towards educational guidelines for the security systems engineer

Suné von Solms & Annlizé Marnewick

UNIVERSITY OF JOHANNESBURG

# Introduction

**Fourth Industrial Revolution / Internet of Things (IoT)**: the intelligent connectivity of smart devices by which objects can sense one another & communicate.




**Industry 1.0**

The Industrial Revolution begins. Mechanization of manufacturing with the introduction of steam and water power

**Industry 2.0**

Mass production assembly lines using electrical power

**Industry 3.0**

Automated production using electronics, programmable logic controllers (PLC), IT systems and robotics

**Industry 4.0**

The 'Smart Factory'. Autonomous decision making of cyber physical systems using machine learning and Big Data analysis. Interoperability through IoT and cloud technology.

# Introduction

**Internet of Things (IoT): the intelligent connectivity of smart devices by which objects can sense one another & communicate.**


Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

# Introduction

In designed systems:

Aug 20 2018 at 7:00 PM
Updated Aug 20 2018 at 7:00 PM

## 90 per cent of malicious botnets target Internet of Things devices

## Manufacturers facing increased cyberattacks

By **Ian Murphy** - August 9, 2018

## The Internet of (Vulnerable) Things

Millions of devices are at risk of hacking.

Intelligent Machines

## For safety's sake, we must slow innovation in internet-connected things

## Under Threat of Global Cyberattacks, Cybersecurity in Manufacturing Industry Must Keep Pace With Digital Transformation

08/21/2018 - 11:02am  Comments  by Christopher Morales

Hacker

TECHNOLOGY AND IIOT

## Industrial IoT Escalates Risk of Global Cyberattacks

IIoT devices can be the opening cybercriminals need to gain access to your network. This explains where your vulnerabilities are and what to do about it.

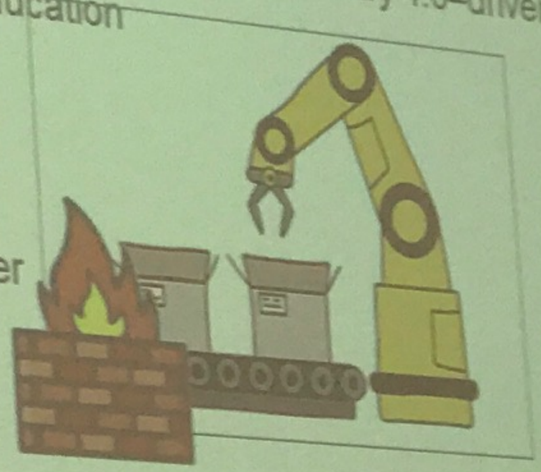
Christopher Morales | Aug 15, 2018

# Introduction

Fear: designers, manufacturers & their supply networks are not prepared for risks of Industry 4.0–driven systems → A big challenge for engineering design & engineering education

Traditional systems engineering processes:

- Isolated environments.
- Security integration limited to the IT industry – security added after system development completed.

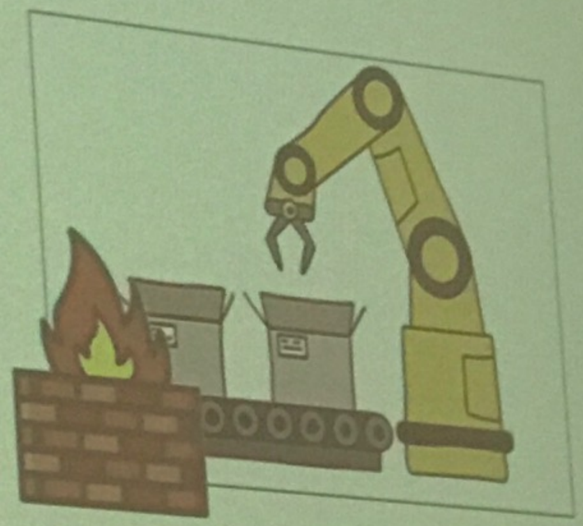


Industry 4.0 (highly integrated) systems:

- Security must be included in software development, risk management, human factors & all other areas (entire lifecycle)
- System security must be accepted & practiced as a fundamental part of SE

# Aim

Limited studies in the field of systems engineering to investigate how the cybersecurity knowledge & skills of the SE in the industrial workforce are changing.



This paper:

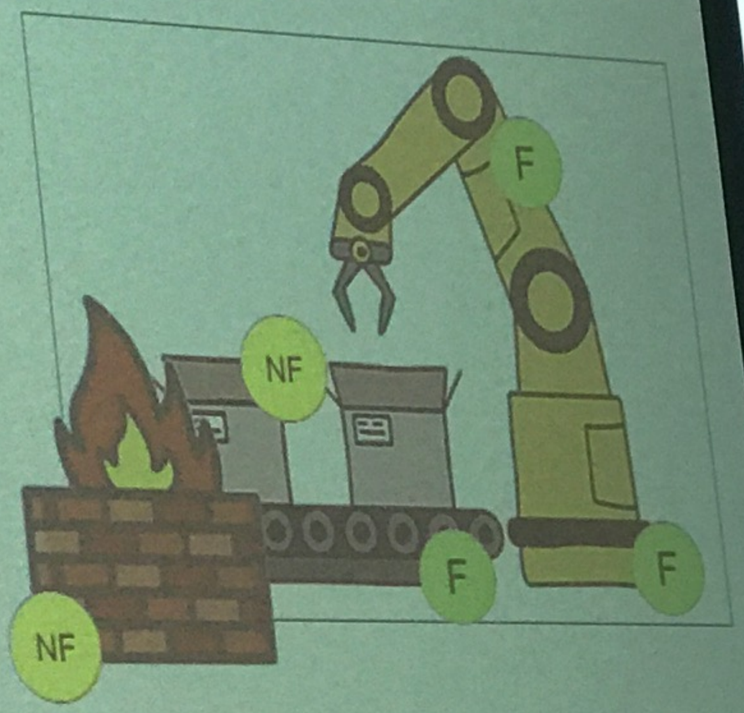
- investigate the additional cybersecurity-related activities the SE will be responsible for in order to design Industry 4.0-ready systems.
- consider the activities in the Requirements and Conceptualization phase of engineering project

Result:

- Input to cybersecurity module for Master's in Systems Engineering
- Cybersecurity strategies should be fully integrated into design strategies from the start.

# Overview of the current systems engineering landscape

- Main systems engineer work role: to derive a complete set of
  - functional requirements (criteria defining specific behavior and functions) → most important
  - non-functional requirements (criteria indicating the operation and constraints) → less important
  - **Security is generally considered a non-functional requirement**




*"As long as systems engineers do not consider security a functional requirement, it will not be likely to rise to the top of the implementation checklist". INCOSE, 2016*

# Overview of the current systems engineering landscape

- Limited exposure of systems engineers to cybersecurity → lack the knowledge, abilities & skills required to address potential Industry 4.0-related security issues → leads to gaps in security architecture of systems

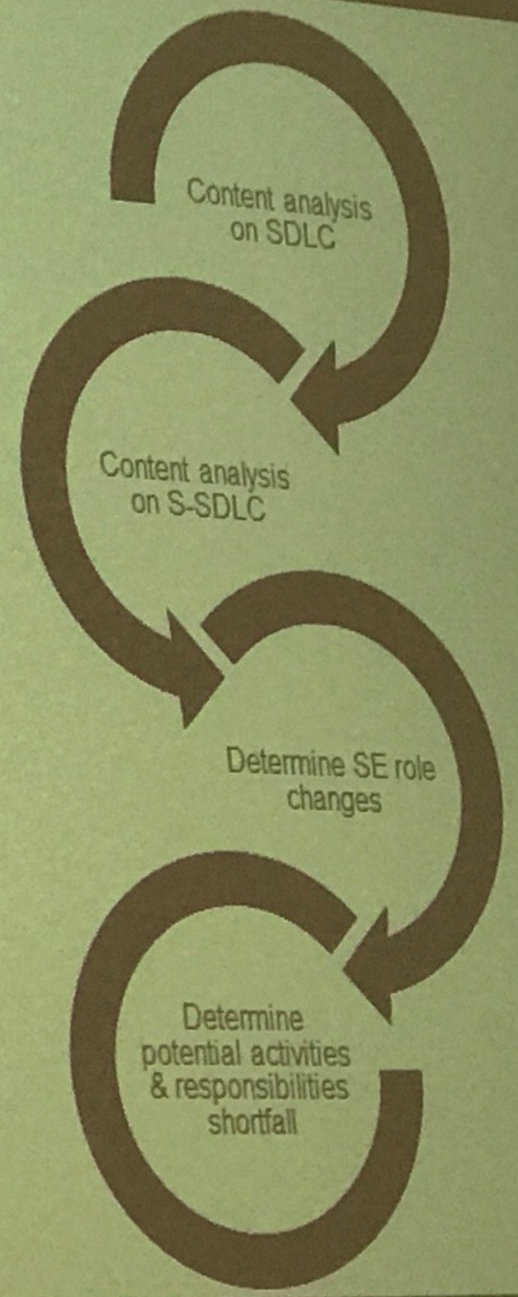
- **International Council of Systems Engineering** (INCOSE): chartered a working group in 2016
  → start the processes required for fostering security within systems engineering (no progress further)
- **National Institute of Standards and Technology** (NIST) produced National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in 2017:
  → highlights interdisciplinary nature of cybersecurity work & provides guidance on workforce development, training & education of cybersecurity professionals
  → details knowledge, abilities & skills required by a professional in order to successfully execute the applicable tasks and activities

- (NICE) Cybersecurity Workforce Framework = currently used to evaluate the inclusion of cybersecurity considerations in the system development life cycle (SDLC) of systems engineering.

# Methodology & Research Process

**Objective: determine the new activities that a systems engineer will be exposed to when developing systems for the Industry 4.0 environment.**

1. Conduct content analysis on traditional SDLC processes (ISO/ICE/IEEE 15288:2015 standard)
   - → identify security activities included in the SDLC
   - → where the responsibility lies.
2. Conduct content analysis on the NIST NICE Cybersecurity Workforce Framework
   - → identify security activities included in the S-SDLC
   - → where the responsibility lies.
3. Comment on activities, knowledge, abilities and skills differences between the two processes
   - → determine the how SE role in the industrial workforce might change
   - → comments on the potential activities and responsibilities shortfall



# Analysis of security activities in the SDLC

Main work roles of SE:

- Conduct risk analysis & threat assessments of system
- Derive complete set of functional & non-functional requirements of system
- Architecture and systems design

| System concept development stage | | | Design and development stage | | | Production stage | Development stage | Retirement stage |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | System operations | |
| Requirements and conceptualization phase | | | Implementation period | | | Operations period | | |
| User requirement phase | Concept definition | System specification | Acquisition preparation phase | Selection phase | Development phase | Verification phase | Deployment phase | Operations & maintenance | Deactivation phase |

Typical SDLC for commercial systems integrator environments

- Risk analysis: "*identify, assess & take action to reduce risks of system technical performance, cost and schedule estimates*" - does not include cybersecurity (must be done by expert risk analyst)

# Conclusion

- Industry 4.0 - a need for the creation of systems with a greater level of connectivity
- Current SE processes do not consider all required security activities needed
- There exist a need in engineering education for the creation of cybersecurity course or modules within SE

- Future Research:
  - Consider other phases in the SDLC
  - Determine knowledge areas, abilities & skills required to successfully implement cybersecurity in engineering systems
  - Work to serve as driver towards creation of cybersecurity-related content into engineering education