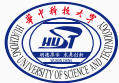


Multi-Model Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems (ICSs)

Zhang Qi

zqmillet@hust.edu.cn

October 6, 2015



Automation School,
Huazhong University of Science and Technology,
Wuhan.

Outlines

Introduction

Architecture

Hazardous Incident Prediction

- The Bayesian Network Based Knowledge Modeling

- Incident Prediction

Dynamic Risk Assessment

- Classification of Incident Consequences

- Quantification of Incident Consequences

- Calculation of Dynamic Risk

Simulation

- Knowledge Modeling and Simulation Platform

- Simulation and Result Analysis

Introduction

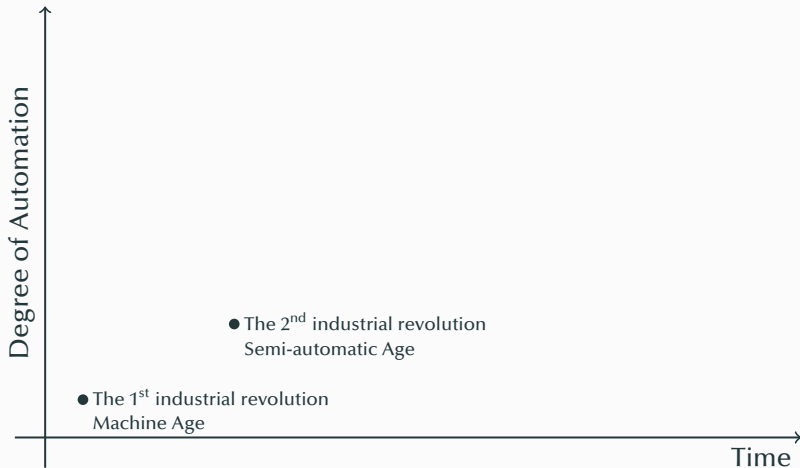
Background

Driven by computer technology, communication technology and intellectual technology, ICSs develop towards the direction of intelligentization and network.



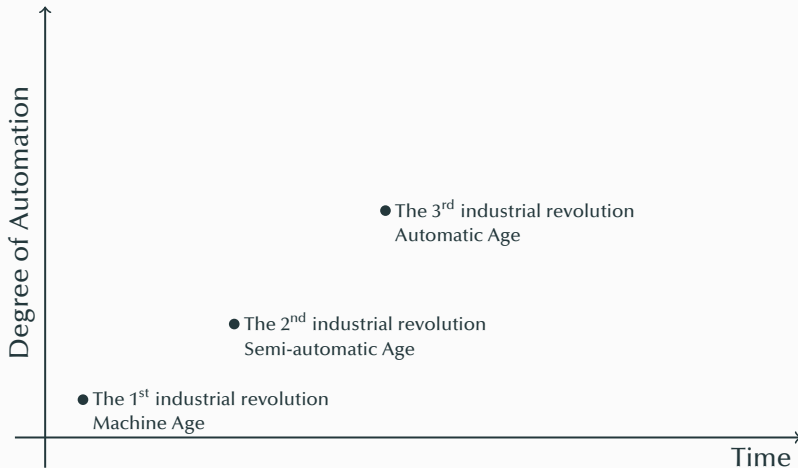
Background

Driven by computer technology, communication technology and intellectual technology, ICSs develop towards the direction of intelligentization and network.



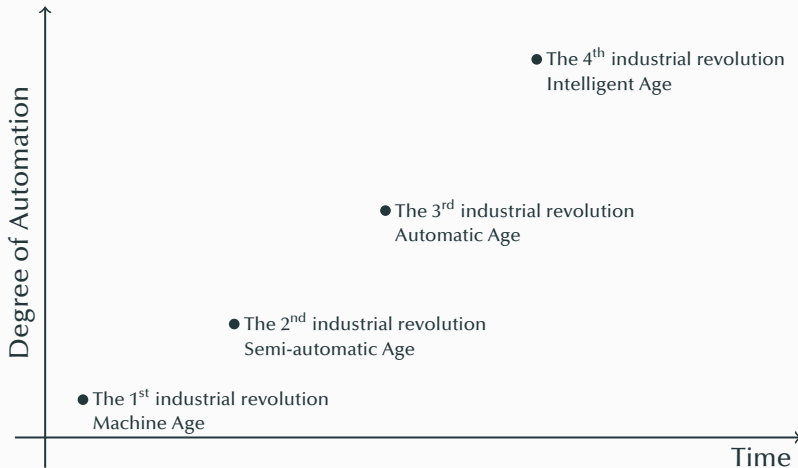
Background

Driven by computer technology, communication technology and intellectual technology, ICSs develop towards the direction of intelligentization and network.



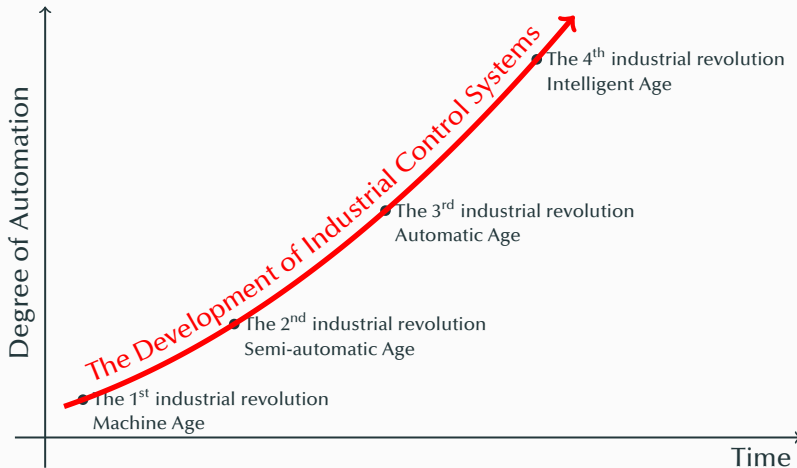
Background

Driven by computer technology, communication technology and intellectual technology, ICSs develop towards the direction of intelligentization and network.



Background

Driven by computer technology, communication technology and intellectual technology, ICSs develop towards the direction of intelligentization and network.



Background

- ICSs have been widely applied in various industry of the national economy and people's livelihood, and gradually become the brain and central nervous of critical infrastructure and all kinds of industrial production.
- Once abnormal situation appears in ICSs, serious accidents may be happen, which may cause damage to property, people or a wide range of environment.



Problems

Architecture

Hazardous Incident Prediction

Function Level

Incident Level

Collection of Evidence

Calculation of Incident Probability

Dynamic Risk Assessment

Harm to Humans

Environmental Pollution

Property Loss

Quantification of Harm to Humans

Quantification of Environmental Pollution

Quantification of Property Loss

Calculation of Dynamic Risk

Simulation

Knowledge Modeling and Simulation Platform

Simulation and Result Analysis

Questions?