

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

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

Problems

Architecture

Hazardous Incident Prediction

Attack Level

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?