### A Joint Venture of TÜV Austria and TU Wien

# Safety and Security in Industry Research Lab "SafeSecLab"

## 

## #SafeSecLab

#### PhD Project 5: Automated Risk Management in Industrial Control Systems (ICS)

Risk management provides an important insight which shapes the safety and security of an organization. The increasing threats in an ever changing industrial environment has made it difficult to meet the required safety and security standards in industrial control systems (ICSs). This PhD topic attempts to achieve automated risk identification, analysis and assessment for information security in ICSs. The project aims to find the state-of-the-art identification of security-relevant data and continuous collection of this data to obtain a useful model. Cost-effective risk reduction techniques are to be implemented and validated.

#### Pushparaj Bhosale

#### **Education:**

Bachelors in Electronics and Telecommunication, Masters in Sensor System Tech., PhD Candidate (Current)



#### **Experience:**

Electronics Development Engineer VAPT Engineer

**Interests:** IIoT, Cyber security, Artificial Intelligence, Machine Learning, Industrial Communication and Control System.

State-of-the-Art			Safety-based methods	Security-based	Integrated methods	
<ul> <li>SECURITY</li> <li>Physical access control</li> <li>Information and resources</li> <li>Identification and Authorization (EC 62443, NIST SP 800, etc.)</li> <li>SAFETY</li> <li>Operational</li> <li>Environmental</li> <li>Employee</li> </ul>		Historical Data	Fault Tree Analysis (FTA) [S, Qn, Ql]	Methods Attack Tree Analysis (ATA) [S, Qn, Ql]	Boolean logic–driven Markov processes (BDMP) [D, Qn, Ql]	
	Data Historian	System Characteristics	Failure modes and effects analysis (FMEA) [S, Qn, Ql] Systematic theoretic process analysis (STPA) [S, Ql]	Cyber Physical Security (CPSec) [D]	Non-functional requirements (NFRs) [S, QI]	
	Operator/	Previous Risk Assessment		Systematic theoretic process analysis Security (STPA-sec) [D, QI]	Systematic theoretic process analysis - safety and security (STPA-SafeSec) [S, QI]	
	Engineer	<b>Process Definition</b>				
<ul> <li>Vulnerability</li> <li>Protection</li> </ul>		Asset Inventory	Hazard and operability methodology (HAZOP) [S, QI]	Bayesian Network approach [S, Qn, Ql]	Bayesian belief network (BBN) [D, Qn, QI]	
<ul> <li>&amp; Threats</li> <li>Safety and Security</li> <li>Risk</li> <li>Measures</li> <li>Assessment</li> <li>Mitigation</li> </ul>	Security Advisor	Safety, Security Requirements	Goal Tree-success tree and master logic diagram (GTST-MLD)	Traditional Security Systems [S, Ql, Qn]	Six-step model (SSM) and information flow diagram (IFD) integration approach	
• Hazard Protocols			[S, Qn] * S->Static. D->Dvn	amic. Ol->Qualit	[S, Qn, QI] ative. On->Ouatitative	
a) Motivation for safety security	b) Inputs	b) Inputs c) Data required		d) Risk assessment techniques		
Methodology						
ProblemObjectiveIdentificationthe Solut	es of ion Development	t Demonstratio	on Evaluati	ion	Communication	
<ul> <li>Manual risk management (RM)</li> <li>Time consuming and error prone</li> <li>(Se au RN RN</li> <li>Int sat se ap</li> </ul>	emi-) tomatic A egrated fety and curity proach • Prototy Model • Theoric • Catalog identific risks ar mitigat	<ul> <li>ype/</li> <li>es</li> <li>g of</li> <li>ied</li> <li>nd</li> <li>tion</li> </ul>	nental se) tion ing F S C	Expert analysis Satisfaction of characteristics of AM Satisfaction of objectives	<ul> <li>Journal/ Conference publications</li> <li>Article publication</li> </ul>	

### **Expected Research Results**

- State-of-the-art identification of data and sources, to extract security relevant information
- Prototype of continuous data collection
- Model of dynamic risk identification and assessment
- Development of automatic risk identification and assessment methods
- Prototype implementation and validation

P. Bhosale, W. Kastner and T. Sauter, "A Centralised or Distributed Risk Assessment using Asset Administration Shell," 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2021, pp. 1-4, doi: 10.1109/ETFA45728.2021.9613152.

Supervisor: Wolfgang Kastner (TU Wien) Co-Supervisor: Thilo Sauter (TU Wien) Contact person: Thomas Doms (TÜV)