NTNU – Trondheim
Norwegian University of
Science and Technology

Challenges on verifying Neural Network based Safety-Critical Control Software (SCCS)

Jin Zhang

May.07.2019

About me

西南交通大學 Southwest Jiaotong University

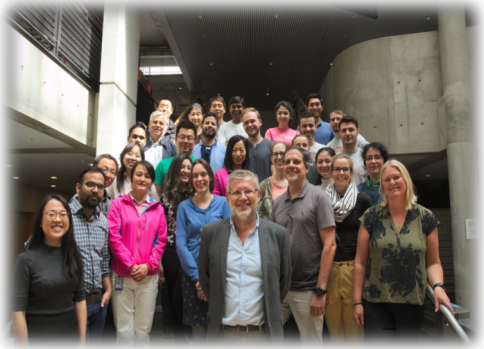
SiChuan Province, CHINA

NTNU

COINS

Safety,
Security, and
Autonomous Vehicle

RAMS group, NTNU



NTNU Norwegian University of Science and Technology

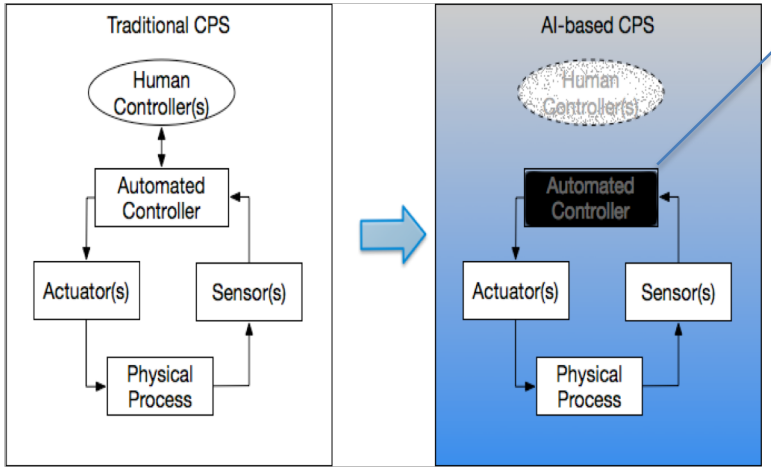
Jin.zhang@ntnu.no

Challenges on verifying Neural Network (NN) based Safety-Critical Control Software (SCCS)

- Presentation based on 1 review paper
  - " Testing and verification of neural network based safety-critical control software: A systematic literature review ", (Submitted to Journal of Information and Software Technology) , Apr., 2019
- And my on-going work about **Safety Verification of Decision algorithm in Autonomous Vehicle**

Motivation

- Artificial Intelligence(AI) Based CPS : a paradigm shift from traditional CPS



Comparison of control structure between traditional CPS with AI-based CPS

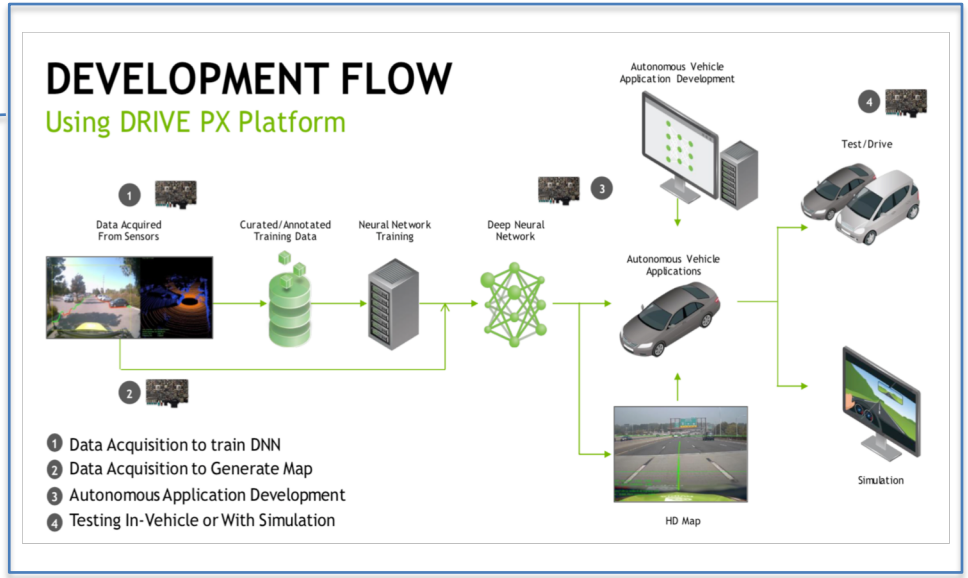
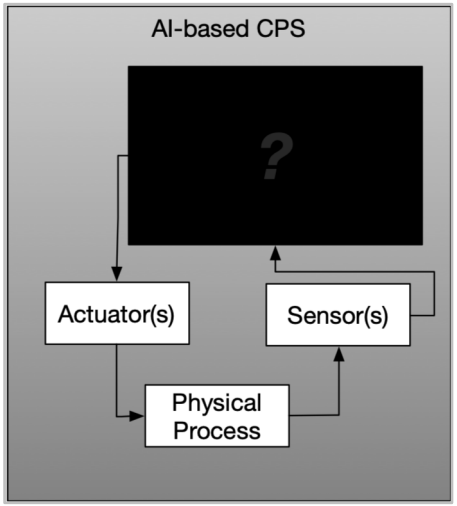


Figure from NVIDIA (2016)

Research gap

- Traditional methods for safety analysis are not capable for black-box systems.



Traditional ICSs	CPSs	AI-based CPSs
Component based	System engineering based	? (model, methods, tools)
FMEA\FTA\HAZOP\Bow Tie	Safety cases/STPA	

Methodology

Three Research questions

Search Term

TITLE-ABS-KEY(("Cyber-physical system*" or "Cyber-physical system*" or CPS* or "Smart grid" or "Smart car" or "Automotive cyber-physical system*" or "Self-driving car*" or "Autonomous vehicle*" or "Autonomous driving system*" or "Automotive electronic control system*" or "Automotive embedded system*" or "Unmanned Aerial Vehicles" or "aircraft collision avoidance system*")**AND**("Risk assessment" or "verification" or "test" or "testing" or "analysis" or "Certification" or "assurance")**AND**("Safety" or "Functional safety")**AND**("Autonomous decision" or "Autonomous agent*" or "Deep learning" or "Deep neural networks")

Search process

Step 1 Data Sources: Scopus, IEEE Xplore, Compendex EI, ACM Digital library, SpringerLink, and Web of Science(ISI)	N=950
Step 2 Apply inclusion and exclusion criteria by reading title and keywords	N=254
Step 3 Apply inclusion and exclusion criteria by reading abstract	N=105
Step 4 Apply inclusion and exclusion criteria by reading introduction and conclusion	N=42
Step 5 Snowballing: Read full paper got in 4th step and scan the reference	N=83

Thematic analysis

- Categorization
- Limitation
- Discussion

Systematic Literature Review Process

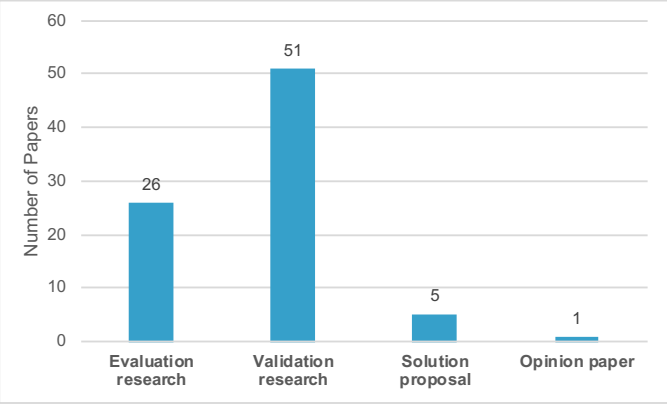
Results:

Demographic attributes

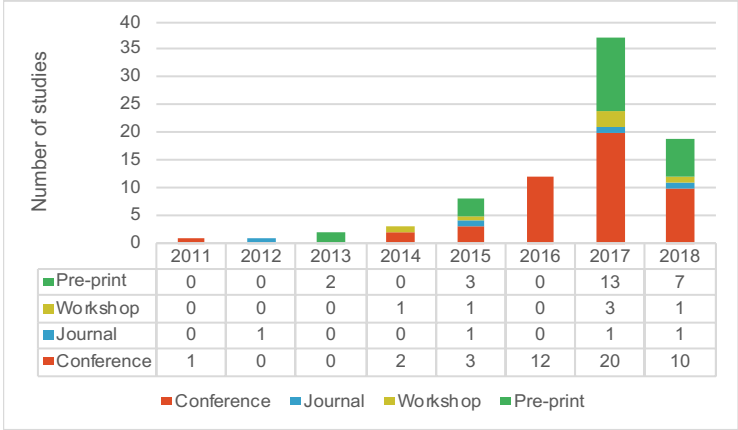
Application domain

Application domain	No. of studies
General SCCPSs	59
Automotive CPSs	13
Autonomous aerial systems	5
Robot system	5
Health care	1

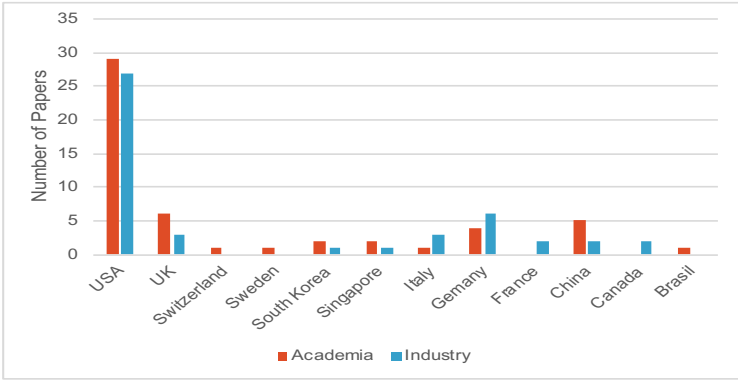
Research type



Publish year and types of work



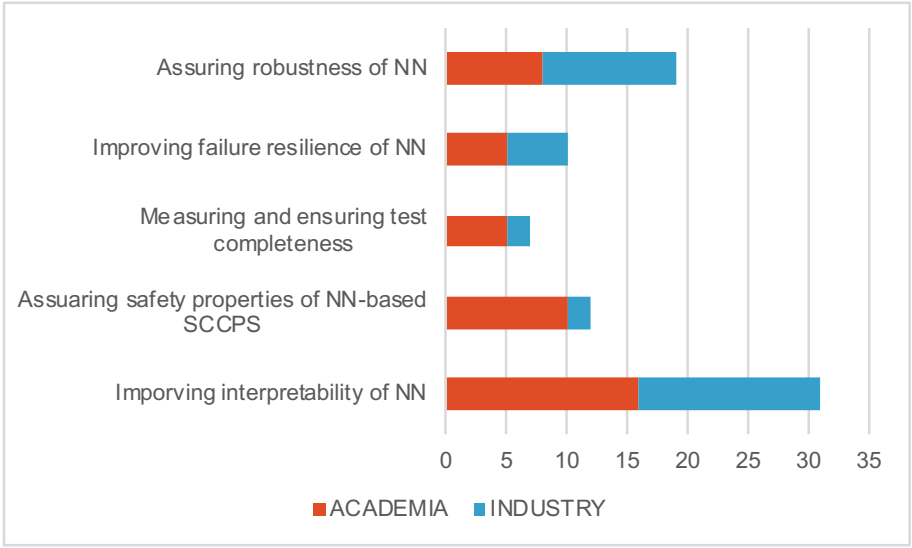
Geographic distribution



Categorization

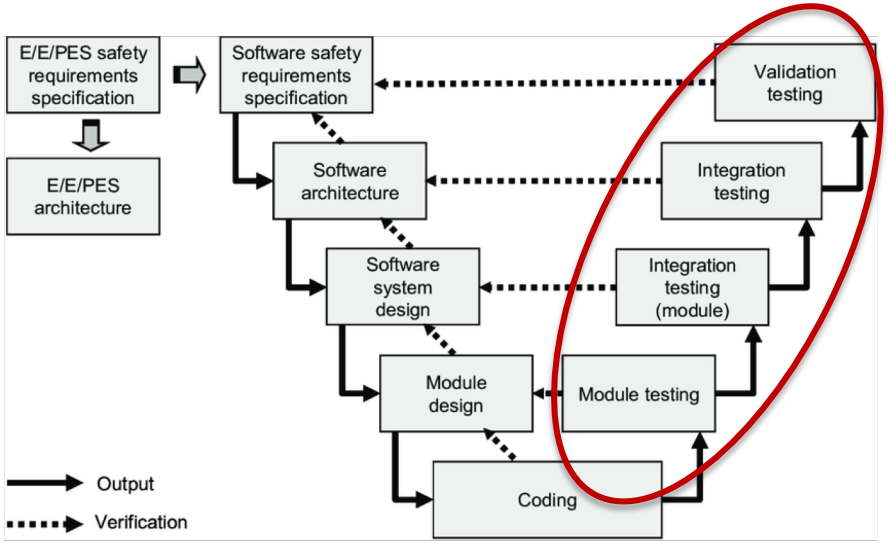
Aims	#	%
CA1: Assuring robustness of NN(Neural network)	17	21.8
CA2: Improving failure resilience of NN	11	14.1
CA3: Measuring and ensuring test completeness	7	8.9
CA4: Assuring safety properties of NN-based SCCPSs	12	15.4
CA5: Improving interpretability of NN	31	39.7

A classification of approaches to test and verify NN-based SCCS



Comparing the interests difference of academia and industry

Limitations of current research



IEC61508 Software Safety Lifecycle

Major T & V activities in software safety lifecycle	Completeness	Correctness	Repeatability	Precisely defined testing configuration	Freedom from intrinsic faults	Understandability	Verifiable design	Fault tolerance	Defense against common cause failure
Testing for architecture design	0	1	N/A	N/A	10	31	2	5	0
module testing and integration	9	7	1	0	N/A	N/A	N/A	N/A	N/A
Programmable electronics integration (Hardware and software)	0	4	0	0	N/A	N/A	N/A	N/A	N/A
Software verification	2	9	0	0	N/A	N/A	N/A	N/A	N/A

No method contributes to this property

Some methods contribute to this property

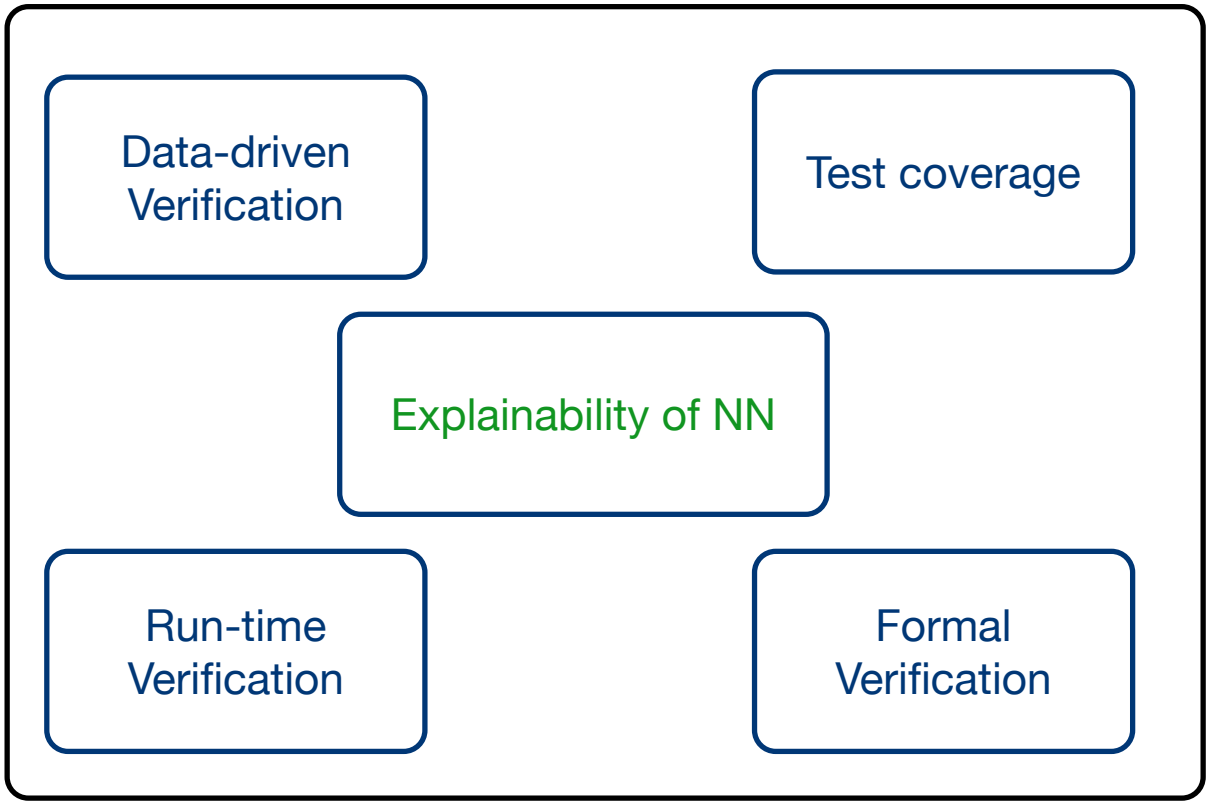
Activity is not relevance to this property

Very few methods contribute to this property

Many methods contribute to this property

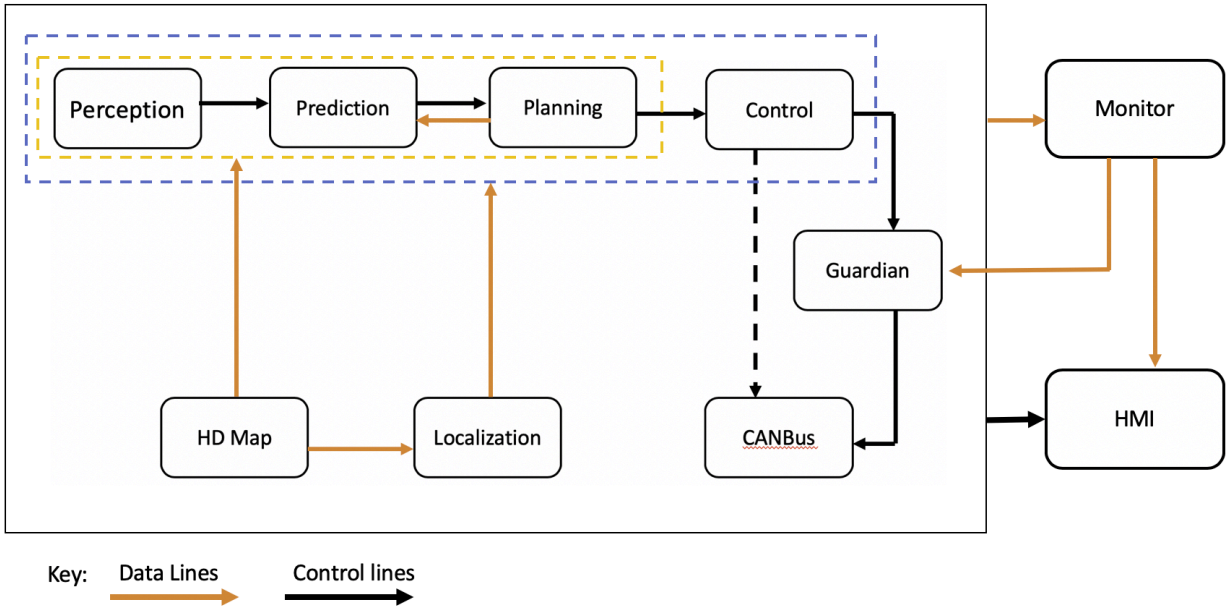
A mapping of reviewed approaches to IEC61508 Software Safety Lifecycle

Research challenges



Future work

- Case study: Safety Verification of Decision algorithm in Autonomous Vehicle



Baidu Apollo 3.5 Software Architecture [1]

[1] Apollo 3.5 Software Architecture, https://github.com/apolloauto/apollo/blob/master/docs/specs/apollo3.5softwarearchitecture.md, Accessed: 2019—04—24

Comments and Suggestions?
Thanks!