Ming-rui XIAO, Yun-wei DONG, Qian-wen GOU, Feng XUE, Yong-hua CHEN, 2020. Architecture-level particular risk modeling and analysis for a cyber-physical system with AADL. *Frontiers of Information Technology & Electronic Engineering*, 21(11):1607-1625. https://doi.org/10.1631/FITEE.2000428

Architecture-level particular risk modeling and analysis for a cyber-physical system with AADL

Key words: Human-cyber-physical system (HCPS); Particular risk analysis; Architecture Analysis and Design Language (AADL); Deterministic and stochastic Petri net (DSPN); Particular risk model

Corresponding authors: Ming-rui XIAO, Yun-wei DONG
E-mail: xiaomingrui@mail.nwpu.edu.cn, yunweidong@nwpu.edu.cn
ORCID: https://orcid.org/0000-0002-1926-9590
https://orcid.org/0000-0001-9882-9121

Motivation

1. According to statistics, in the cyber-physical system, there are only a few failures due to software errors, and most of the failures originate from the actors and physical environment.

2. Architecture Analysis and Design Language (AADL) does not support human factors and physical environment modeling.

3. Traditional particular risk analysis does not consider human factors or provide a complete particular risk analysis guidance process.

Main idea

1. AADL is an excellent design language to support the modeling and analysis work in the early phase of safety critical system development.

2. Based on AADL, a particular risk analysis model is designed to describe human factors and physical environment in detail.

3. The mapping rules from the AADL model to DSPN model are formulated.

Contribution

1. We extend an AADL subclause language as an AADL-PRA annex model with a human component and a physical component, and integrate the proposed model with an architecture model and an error model into a PRA model.

2. A new PRA analysis method is proposed based on the particular risk model (PRM) model to obtain a PRA analysis table.

Method

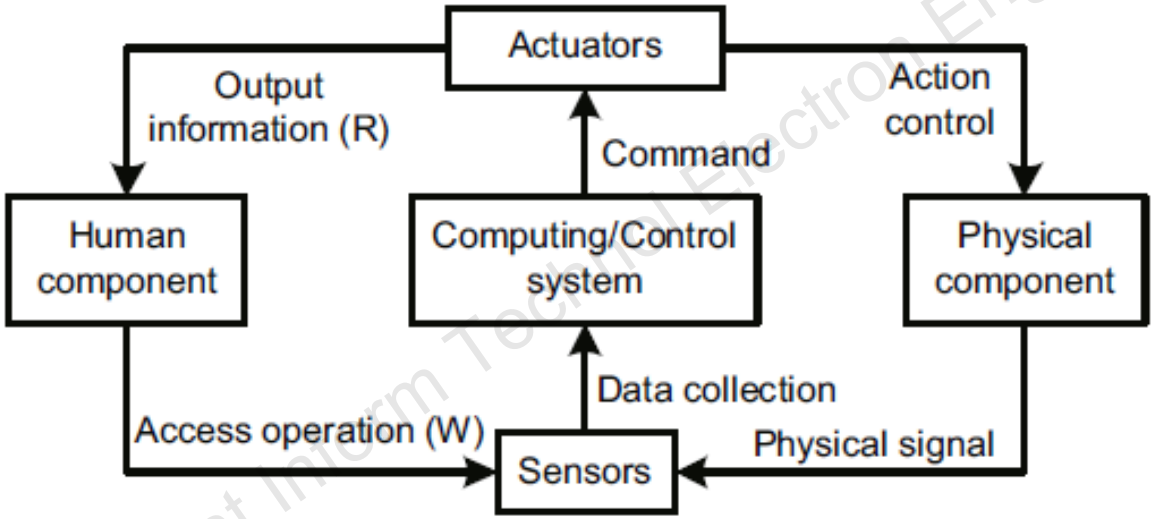

Fig. 1 Framework of the human-cyber-physical system

Major results

1. **human component model** is defined as a tuple $HM = (A, IM, IP, OI, RP, II, ISQ)$, where

- A is a set of all actors, and $A = \{a_1, a_2, \dots a_n\}$.
- IM is a set of all interaction modes that may exist in the execution of a task, and $IM = \{im_1, im_2, \dots im_n\}$.
- IP is a set of all interaction interfaces, and $IP = \{ip_1, ip_2, \dots ip_n\}$
- OI is a set of all relations between the IM and IP.
- RP is a set of all role permissions existing in the human component model, and $RP = \{rp_1, rp_2, \dots rp_n\}$.
- II is a set of all relations between interaction subject IS and OI that represents interaction intent of actors. $IS = \{is_1, is_2, \dots is_n\}$, each interaction subject is_i is represented as a set of actors that access the operation interface oi_i.
- ISQ is a set of all interaction sequences existing in the human component model, and $ISQ = \{isq_1, isq_2, \dots isq_n\}$.

Major results (Cont'd)

2. **physical component model** is defined as a tuple $PM = (BS, BS_0, PV, CV, CB, CD, T)$, where

- BS is a finite set of discrete behavioral states in the physical component model, and $BS = \{bs_1, bs_2, \ldots bs_n\}$.
- $BS_0 \subseteq BS$ is the initial states of physical component model, and $BS_0 = \{bs_1, bs_2, \ldots bs_m\}$.
- PV is a set of all physical variables, that is, $PV = \{pv_1, pv_2, \ldots pv_n\}$
- CV is a set of all global clock variables in the physical component model, and $CV = \{cv_1, cv_2, \ldots cv_n\}$
- CB is a set of all continuous behaviors in behavior state bs_i, and describes the change of external physical variables when the physical component is in the state bs_i.
- CD is a set of all trigger conditions, i.e., $CD = \{cd | cd = (tb, cs, cr)\}$
- T is a set of all state transitions included in the physical component model, and $T = \{t_1, t_2, \ldots t_n\}$.

Major results (Cont'd)

3. Particular risk analysis method

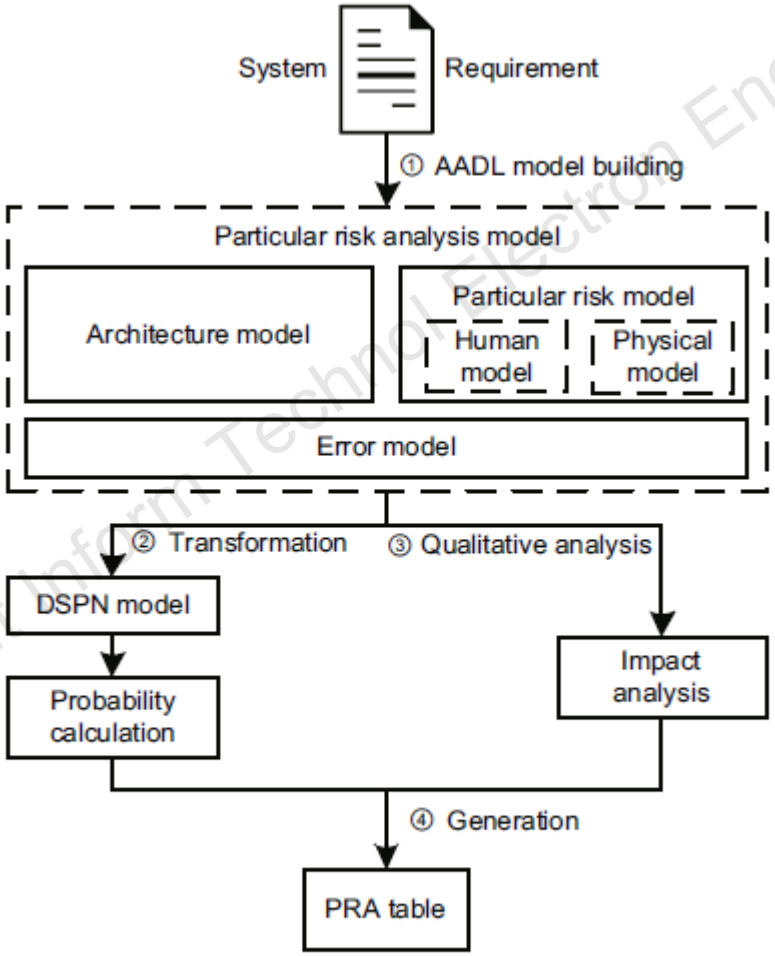

Fig. 5 Framework of the particular risk analysis method

Major results (Cont'd)

4. Mapping rules between the PRA and DSPN models

Table 1 Mapping rules between PRA and DSPN models

PRA model	DSPN model
Event (poisson)	Exponential transition
Event (fixed)/Error inPropagation	Immediate transition
Event (latency)	Deterministic transition 
Error state/Error outPropagatio	Place 
Errorfree state/Initial state	Place with token 
State transition	Source place→transition  transition→ destination place

Major results (Cont'd)

5. AADL model of SSC (safety and stability control system)

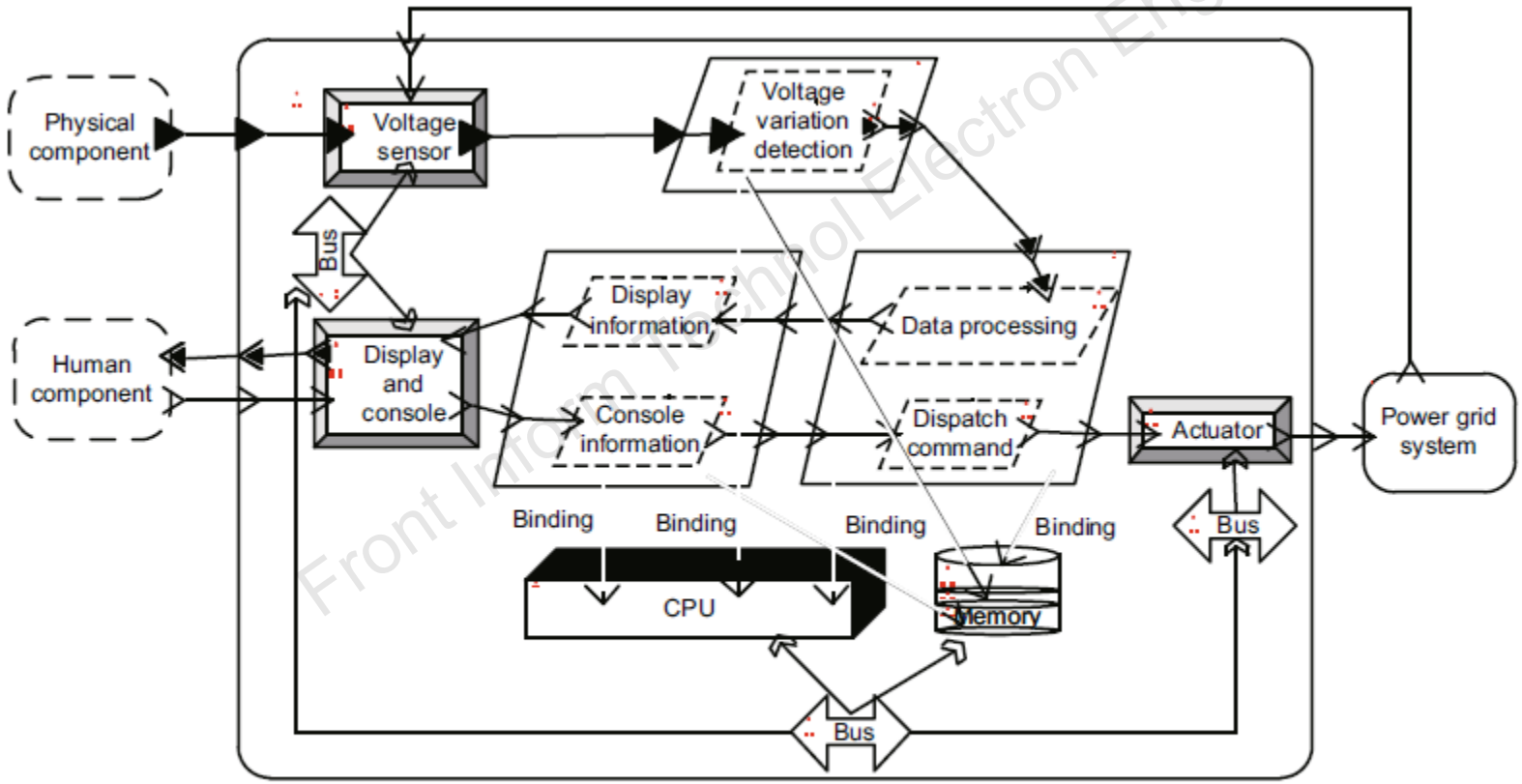

Fig. 10 Architecture model of SSC

Solid triangles on the boundary of the component: in/out data ports; hollow arrows on the boundary of the component: in/out event ports

Major results (Cont'd)

6. DSPN model of SSC

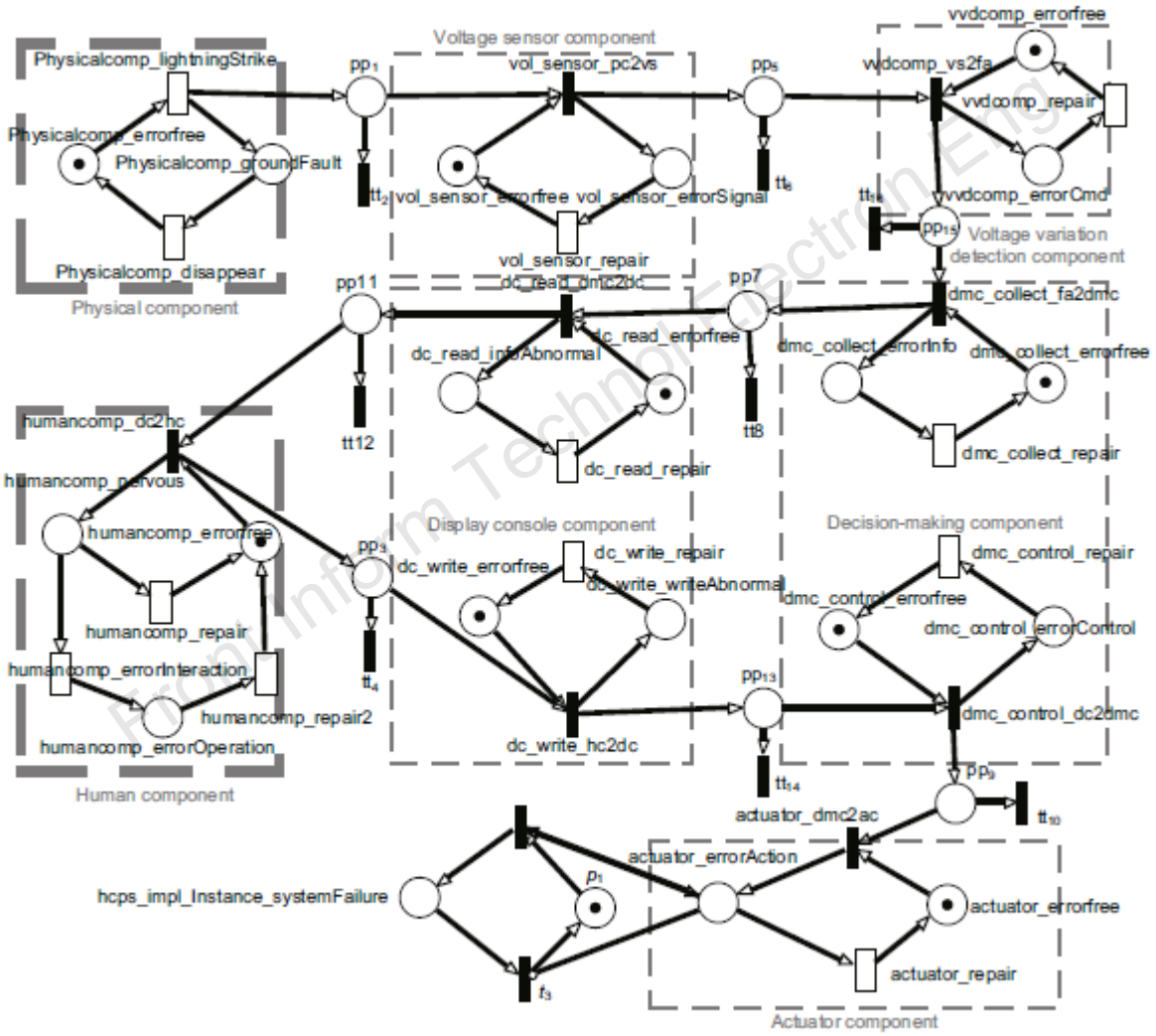

Fig. 12 DSPN model of the PRA model

Major results (Cont'd)

7. Analysis report of the proposed method

Table 2 PRA analysis table

Comp	PR	FS	AC	OR
physicalcomp	lightningStrike	groundFault	voltage_sensor	GB 50343-2019 Clause 5 lightning protection design
humancomp	errorInteraction	errorOperation	dc_write	State professional standard power dispatcher

Comp	PM	Pro	isAccept
physicalcomp	Defending the react lightning and twist lightning	1.11×10^{-4}	Unacceptable
humancomp	Technical training and theoretical examination	7.47×10^{-5}	Unacceptable

Comp: component; PR: particular risk; FS: failure state; AC: affected component; OR: operational requirement; PM: preventive measure; Pro: probability

Major results (Cont'd)

8. Failure probability of components with or without particular risk

Table 3 Comparative analysis

Component	Failure state	Failure probability	
		With PRM	Without PRM
physicalcomp	groundFault	5.26×10^{-5}	
vol_sensor	errorSignal	1.11×10^{-4}	5.59×10^{-6}
vvdcomp	errorCmd	1.93×10^{-5}	9.70×10^{-5}
dmc_collect	errorInfo	6.11×10^{-5}	3.13×10^{-6}
dc_read	infoAbnormal	5.81×10^{-5}	2.87×10^{-6}
humancomp	nervous	5.26×10^{-5}	
	errorOperation	6.60×10^{-8}	
dc_write	writeAbnormal	7.47×10^{-5}	3.05×10^{-6}
actuator	errorAction	6.68×10^{-5}	3.30×10^{-6}
hcps	systemFailure	6.68×10^{-5}	3.30×10^{-6}

With PRM: with human component model and physical component model; Without PRM: without human component model and physical component model

Conclusions

1. A particular risk model has been proposed based on AADL, which is combined with an architecture model and an error model to construct a particular risk analysis model.

2. An architecture-level particular risk analysis framework has been proposed based on the PRM. The method transformed AADL PRM into the DSPN model, and then obtained the analysis results through simulation tool TimeNet. These results showed that it is necessary to carry out PRA in the early design phase of system development.

Ming-rui XIAO received his BS degree in software engineering from Northwestern Polytechnical University. He is currently a master candidate at the Northwestern Polytechnical University. His research interests include safety-critical systems, software architecture, and software safety analysis.

Dr. Yun-wei DONG is a professor of School of Computing Science at Northwestern Polytechnical University, China. He is an excellent member of CCF, and an IEEE senior member. He is also a member of the Administration Committee of IEEE Reliability Society and chairman of the Xi'an Chapter of IEEE Reliability Society. His research interests include embedded system, cyber-physical system, model-driven architecture, and software formal methodology.

Dr. Xue FENG is currently a professor status senior engineer at Nari Group Corporation/State Grid Electric Power Research Institute. His research interests include power system safety and stability control analysis and control.