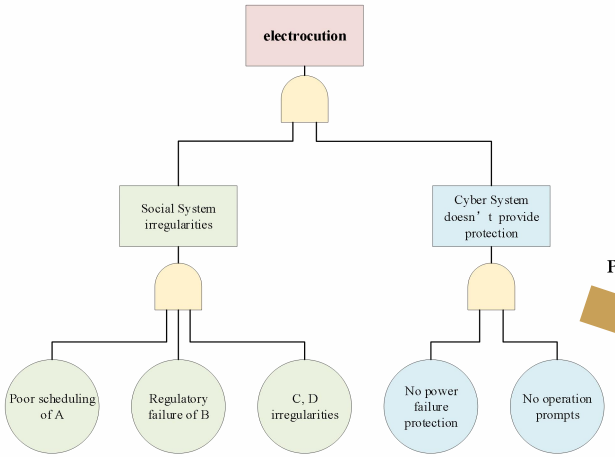
A Double-Direction Cognitive Interaction Security Architecture for CPSS: A Case Study

Mengjin Qu*, Qing Li*, Zhixiong Fang*, Rui Liu*

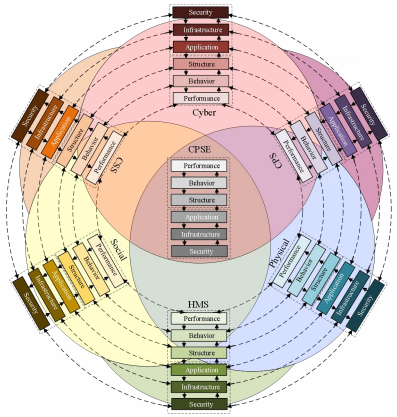
**Department of Automation, Tsinghua University, Beijing 100084 China (Tel: +86-10-62771152; e-mail: liqing@tsinghua.edu.cn).*

1. Introduction

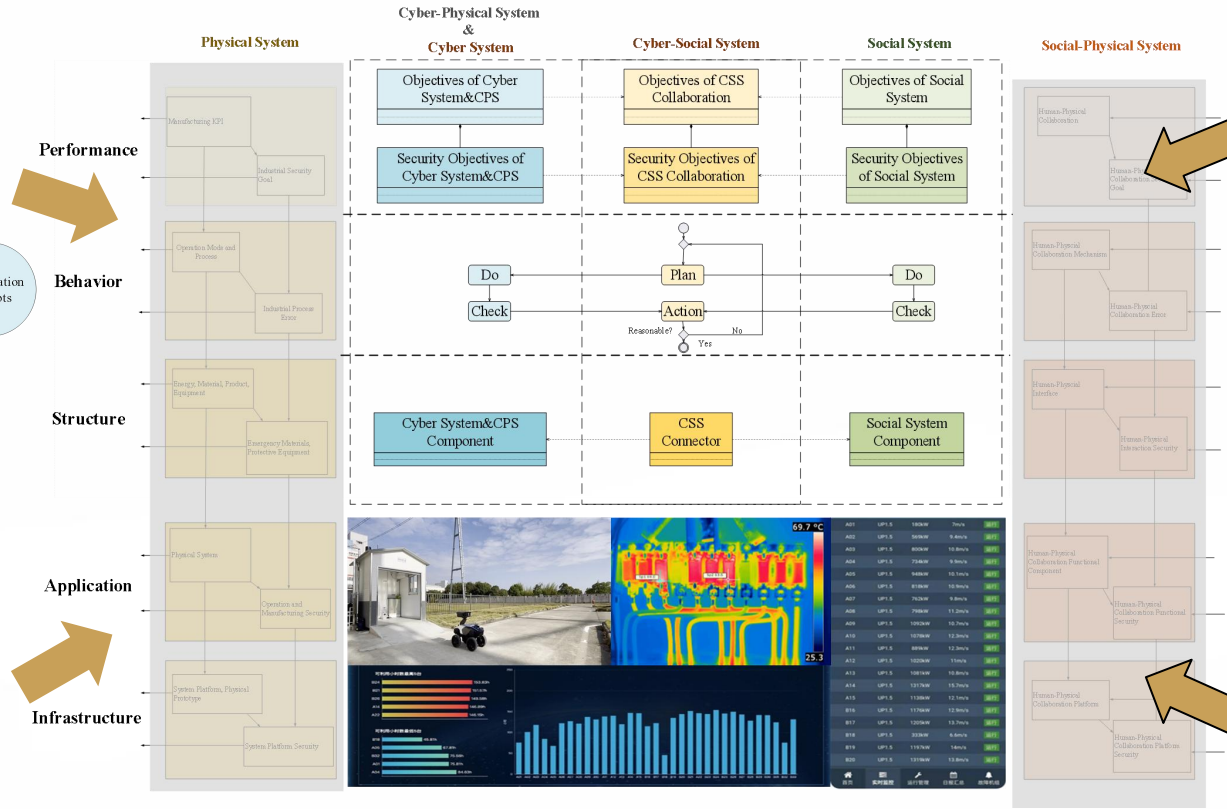
Smart grid security is a complex system that encompasses human, cyber and physical systems



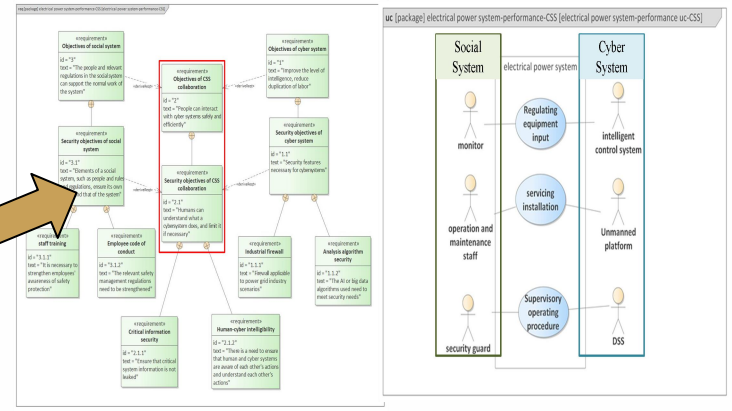
Problem



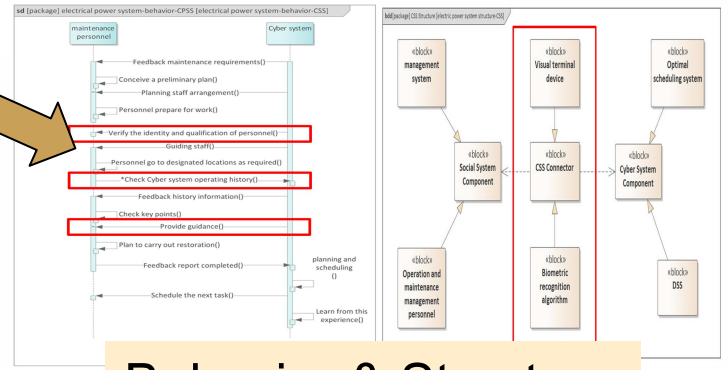
Methodology



Architecture



Performance



Behavior & Structure

1. Introduction

The development AI is constantly reshaping the form of today's society

Yes !

- **Multi-fields:**
  - Aerospace
  - Healthcare
  - Urban Construction
  - Transportation
  - ……
- **Multi-subject:**
  - Cyber-Physical System
  - Cyber-Social System
  - Cyber-Social-Physical System
  - ……

But……

- **Artificial intrusion into physical systems from cyber systems:**
  - Iranian Stuxnet Virus Attack
  - BlackEnergy" attack on Ukraine's power grid
- **People and AI can't understand each other:**
  - Boeing 737 MAX 8 Safety Incident
  - Electricity O&M scenarios with intelligent systems (scenarios in this article)
- **Overpowered Cyber Systems:**
  - A certain brand of car can't go back to the right direction and hits a wall
  - Problems recognizing a white truck by a certain brand of car

The Security of Double-Directional Cognitive Interoperability between Humans and AI is Imminent!

General Enterprise Modelling

CPSS Security is a Complex System Engineering

CPSS Security Requirement

- Big Data
- Cloud Computing
- New Generation AI

→

- Social System
- Cyber System
- CSS Integration and Interoperability

→

- 737 MAX 8 Contest for Control
- Stuxnet Virus

↓

CPSS Security Solution

Architectures and Methodologies:

- FEAF, UAF, DoDAF, GAF, ……
- OSI, IISF, IATF, IEC 62243, ……

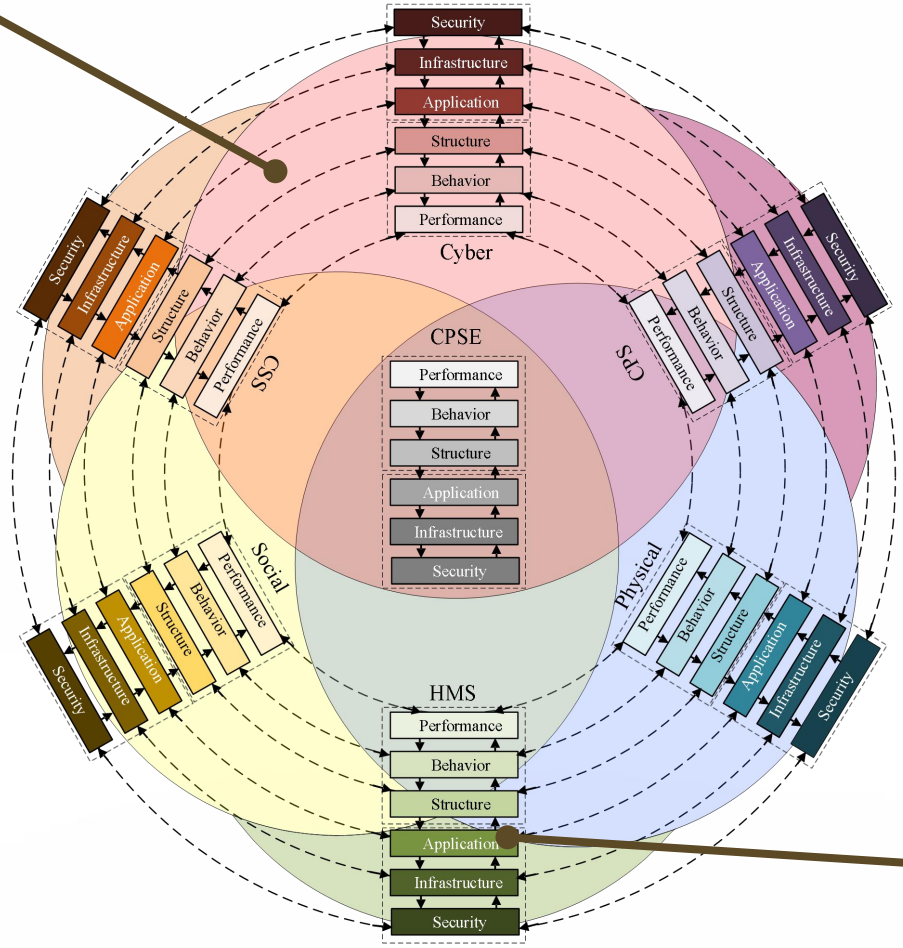
+

Technologies and Algorithms:

- Asset Environmental Protection, ……
- Risk Identification Algorithms, ……

1. Introduction

- The Architecture Framework is like a Venn diagram:
  - Unary System:
    - Social systems
    - Physical systems
    - Cyber systems
  - Binary System:
    - Human-Machine System (HMS)
    - Cyber-physical systems (CPS)
    - Cyber-Social System (CSS)
  - Ternary System:
    - Cyber-Physical-Social System (CPSS)

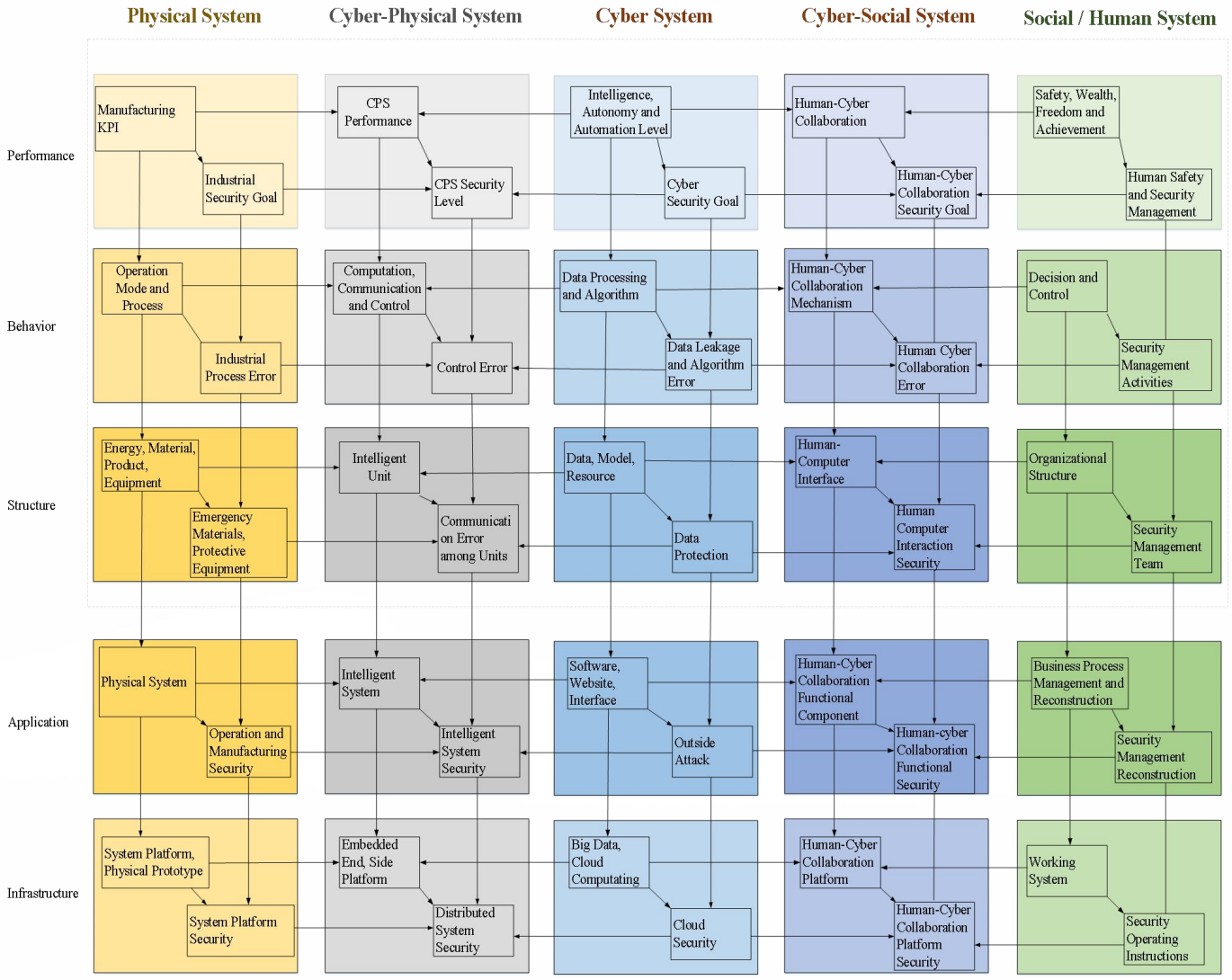


CPSS Architecture

- Each subsystem has 6 key views adapted from the Federal Enterprise Framework version 2.0:
  - Performance: requirements on the business logic.
  - Behavior: the flow of activities to meet requirements.
  - Structural: the organizational, physical, and network structure of people.
  - Application: the implementation of system activities.
  - Infrastructure: the basic support of the system.
  - Security: a core issue in CPSS, closely related to the other models.

1. Introduction

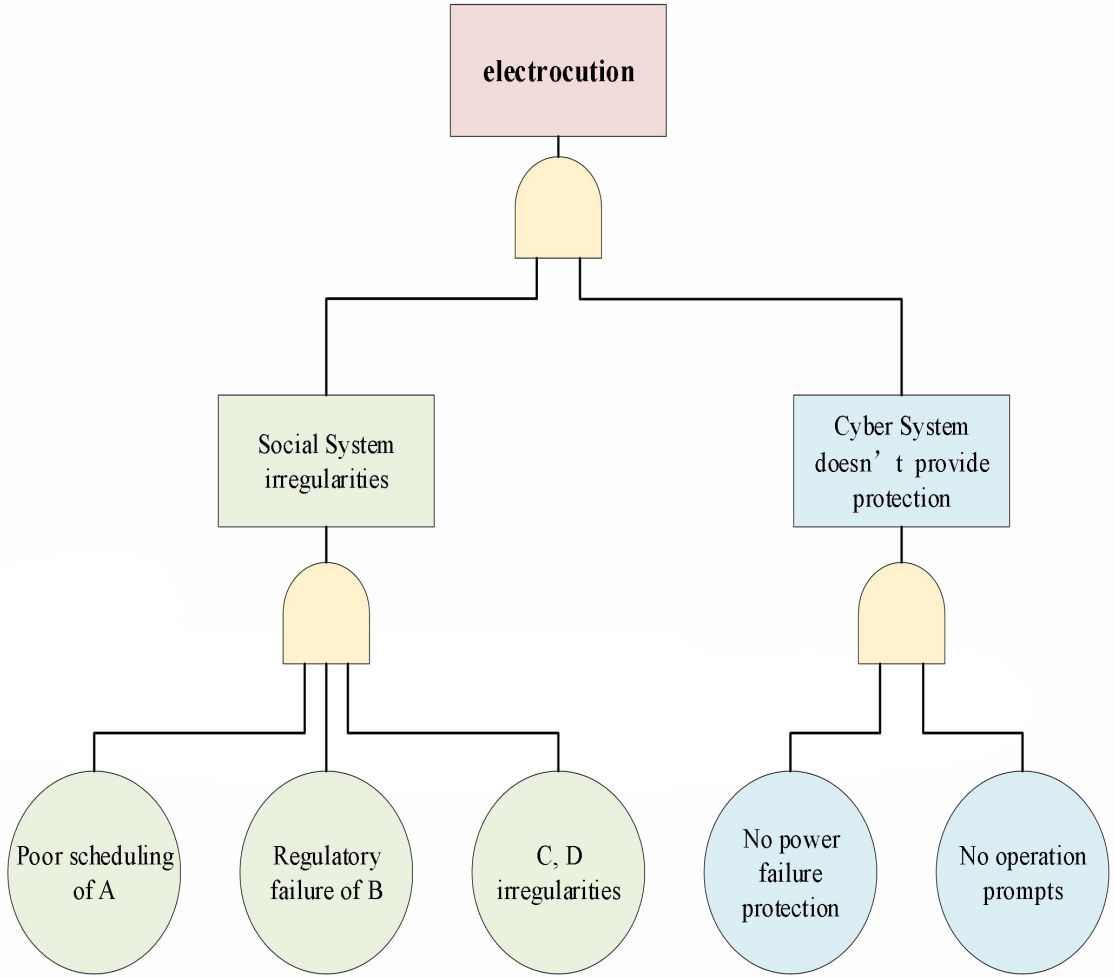
- Consider potential security risks and issues that may exist during CPSS analysis, design, and implementation in conjunction with the layer dimension and the domain dimension.
- There are two smaller blocks within each. The top left represents general matters and the bottom right represents security matters to be considered in system analysis and design.
- The arrows from top to bottom represent the logical sequence of the analysis process.
- The horizontal arrows indicate that the analysis and design of the CPS needs to be based on physical and cyber systems, and the analysis and design of the CSS needs to be based on social and cyber systems.



CPSS Security Methodology

The Electric Industry is One of the Lifeblood Industries of Every Country

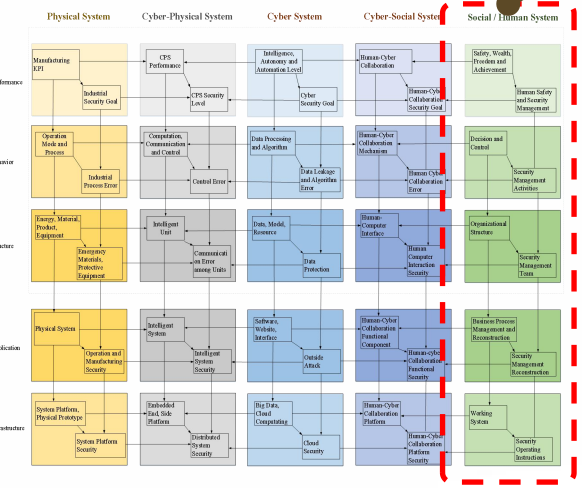
- Currently, the autonomy and intelligence of the electric power system are insufficient to achieve fully automated component replacement and emergency handling.
- It is not challenging to comprehend that this accident occurred precisely because humans placed excessive trust in the protective capabilities of the Cyber System.
- Neither the analysis methods tailored for industrial production nor other individual systems, nor the design concepts grounded on human-computer interface interactions, align with the current case.
- The failure was triggered by double-directional cognition, which was the fundamental premise underlying the proposed analysis architecture.



Typical Accident Case

General Enterprise Modelling

The primary issue remains the interaction between humans and AI



Performance

Behavior

Structure

Application

Infrastructure

Physical System

Cyber-Physical System & Cyber System

Cyber-Social System

Social System

Social-Physical System

Objectives of Cyber System&CPS

Objectives of CSS Collaboration

Objectives of Social System

Security Objectives of Cyber System&CPS

Security Objectives of CSS Collaboration

Security Objectives of Social System

Do

Check

Plan

Action

Reasonable?

No

Yes

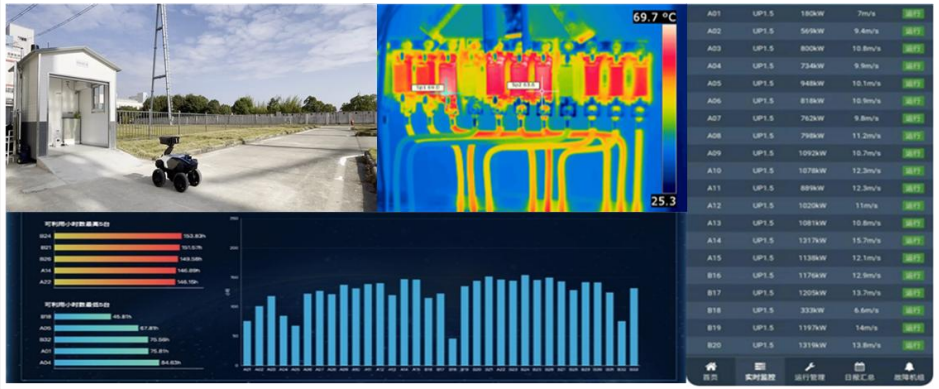
Do

Check

Cyber System&CPS Component

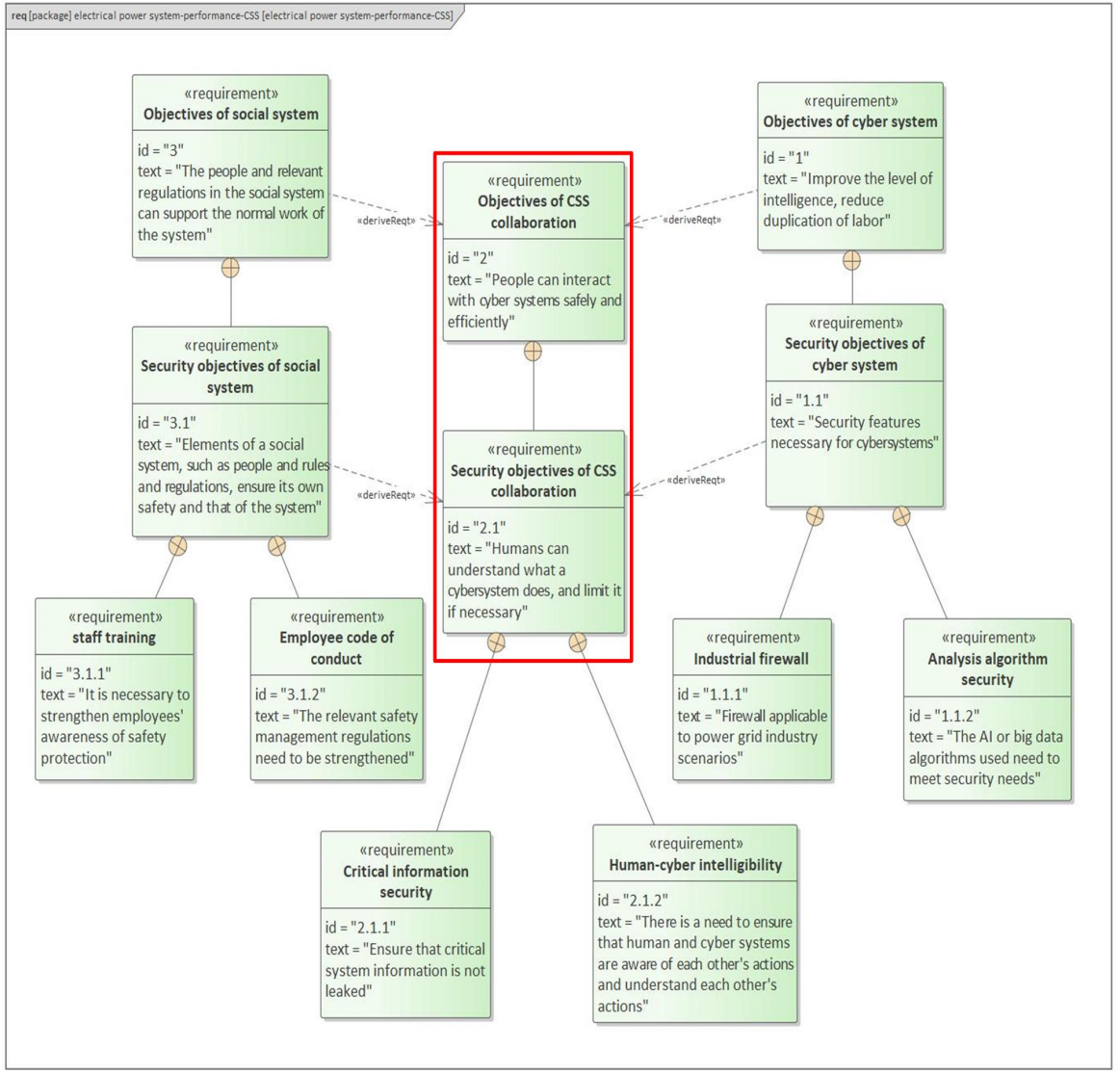
CSS Connector

Social System Component

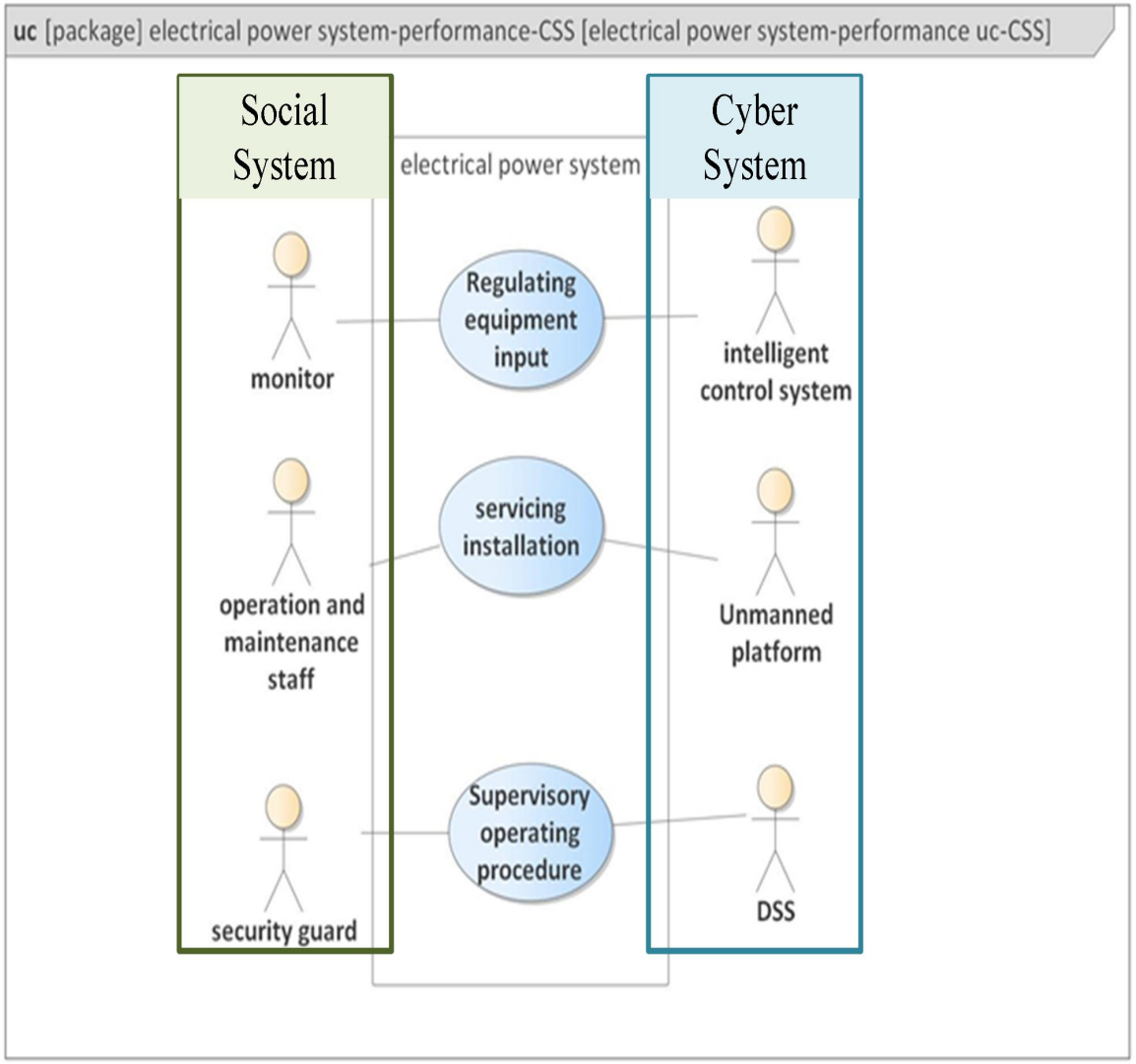


2 The Architecture, Methodology and Performance Analysis of the Case

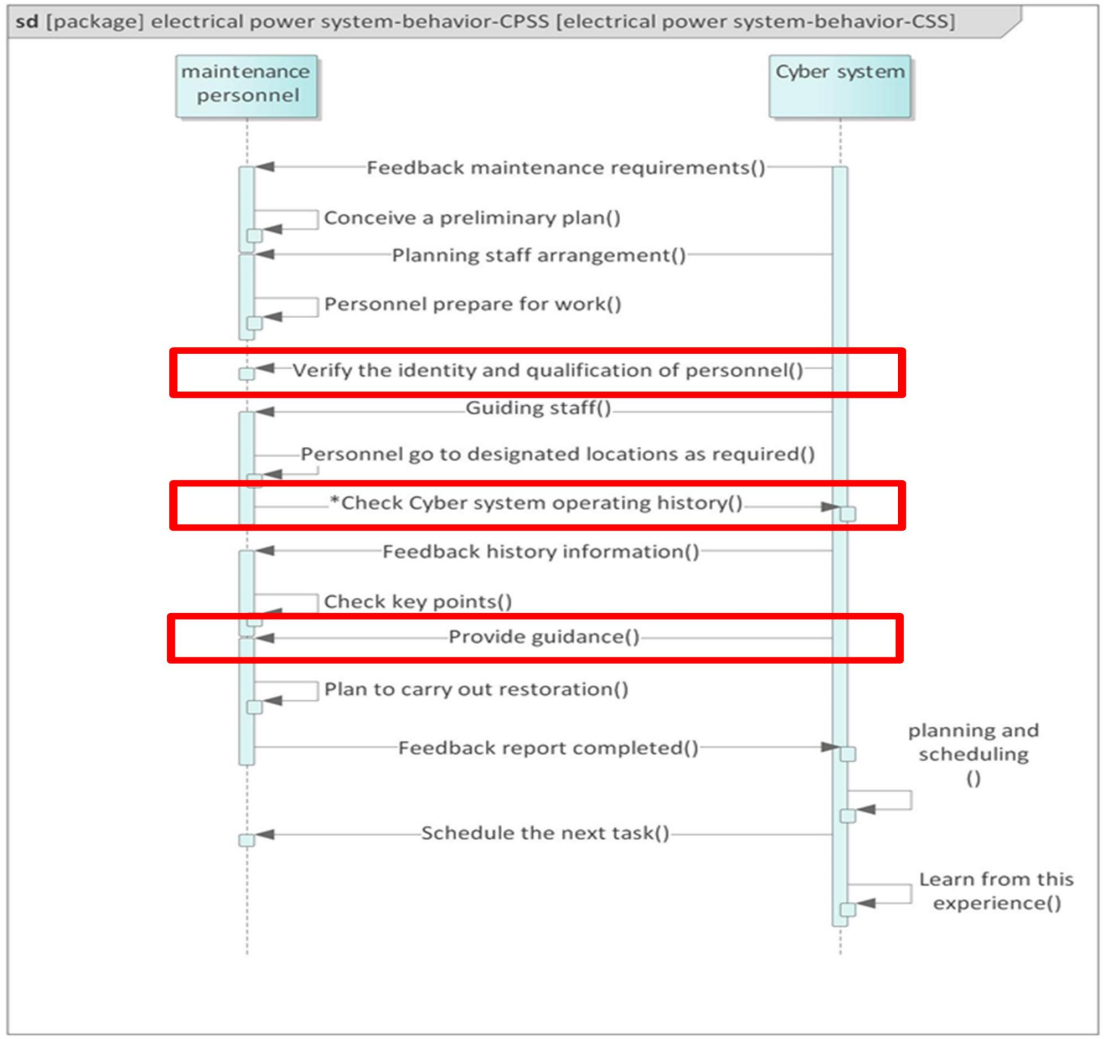
- Based on the constructed system architecture, it is evident that system design must not only consider the performance and objectives of the three individual systems but also account for the interaction performance indices of the binary systems and even the overall ternary integration operation and maintenance (O&M) system in the context of integration. In this case, our analysis focuses on the CSS, a set of double-direction cognitive interaction systems.
- not only contemplate the respective requirements of the Social System and the Cyber System but also take into account the requirement constraints arising from their combined interaction.



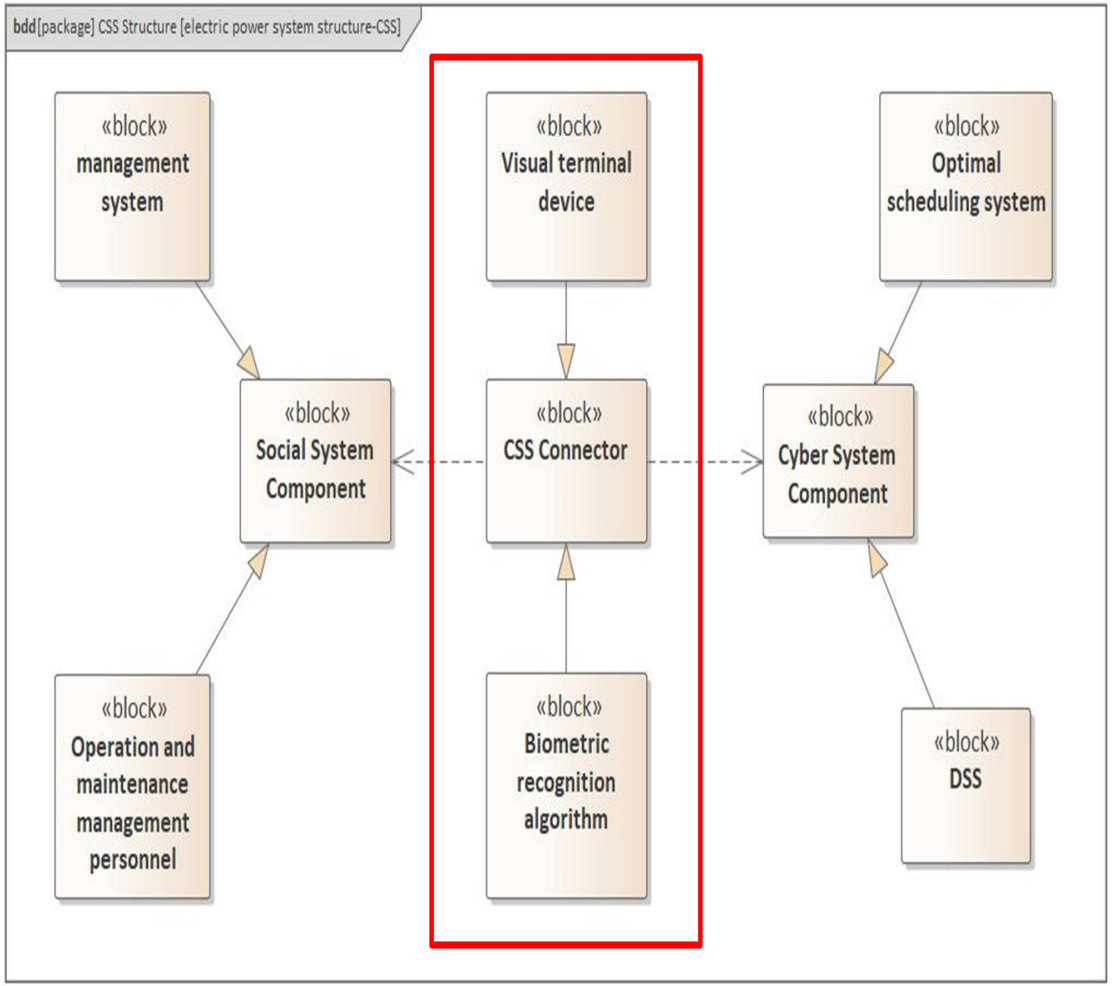
- Due to the current technological limitations and sustainability requirements, not all O&M tasks can be fully automated by the Cyber Systems; instead, corresponding personnel must assume their respective responsibilities and perform the necessary work.
- The electric system O&M use case diagram, which is constructed with a holistic perspective starting from the demand.
- This approach facilitates double-directional interactive cognition and understanding between humans and AI within the complex CPSS of the electric power system, ultimately ensuring the secure and stable operation of the system.



- the absence of interaction channels and an excessive level of trust between the two parties become apparent in the CPS interaction process between humans and the pure electric power system.
- For O&M activities:
  - people can leverage the Cyber System's capabilities in computation, storage
  - Cyber System needs to learn from people's repair methods.
  - Cyber Systems should transparently and openly display every step of its execution and operation, ensuring traceability.



- The implementation of human integration into the traditional CPS, aiming to achieve interactive understanding and support between people and the CPS system, and ultimately realizing effective interaction within the CPSS, necessitates the presence of corresponding structural components.
- A comprehensive CSS should comprise three components: the Cyber System component, the Social System component, and the CSS Connector. Each of these components includes multiple elemental structures, collectively facilitating various functions and business processes within the system.



4. Conclusion

- Contributions:
  - Proposes guidelines for selecting case studies based on the analysis of the security of CPSS, a complex SoS, using the systematic analysis and design methodology developed by Li et al.
  - Provides an overview of the electric power intelligent operation and maintenance system.
  - Focuses on aspects such as demand, operational mode, interaction forms, and structural elements of double-directional cognitive interaction between humans and cyber systems within the framework.
  - Offers valuable insights for designing the electric power intelligent operation and maintenance system, and to validate the proposed theoretical framework's effectiveness.

- Future:
  - Construct corresponding generalized reference models and domain-specific reference models based on the established architecture and methodology.
  - The existing models can be expanded and analyzed comprehensively to thoroughly examine the requirements, functions, and structures associated with intelligent O&M within electric power systems.

Thank You!