Privacy Analysis and Enhancement for Joint Communication and Sensing Applications

Yevhen Zolotavkin, Prajnamaya Dass, Stefan Köpsell

Barkhausen Institut, Dresden, Germany
{yevhen.zolotavkin|prajnamaya.dass|stefan.koepsell}@barkhauseninstitut.org

***Abstract*—Joint Communication and Sensing (JCAS) technology is envisioned to become a part of many Cyber-Physical Systems (CPSs), further advancing essential capabilities provided to numerous applications in critical infrastructure. Due to the use of human-specific sensing data, JCAS systems are vulnerable to privacy threats, and there is no established method to assess the privacy of such systems efficiently. In this paper, we propose a new privacy assessment approach that quantitatively expresses the overall privacy of the JCAS-based system under consideration, for which privacy enhancements are then proposed. While we apply our approach to a railway JCAS-based CPS in this paper, it also applies to CPSs of other kinds.**

***Index Terms*—Privacy, JCAS, CPS, railway, level crossing.**

I. Introduction

Cyber-Physical Systems (CPSs) constitute a fundamental component of critical infrastructure, seamlessly integrating physical processes with computing and communication capabilities. These systems are composed of both Information Technology (IT) and Operational Technology (OT) components that collect, store, and process human information, making privacy protection a significant concern [1]. Joint Communication and Sensing (JCAS) is expected to be an important part of many CPSs, impacting sectors like transportation, healthcare, and industrial automation.

JCAS utilizes communication signals for simultaneous radar like sensing tasks [2], [3]. For example, a base station (gNB) communicates with cellular users while detecting objects within its range. While these advancements present substantial benefits, they also introduce *new privacy challenges* that must not be overlooked. The inherent complexities of JCAS architectures pose challenges in assessing and mitigating privacy risks [4]. Given the diverse technologies and structural intricacies, a *unified approach* is required to systematically evaluate and address privacy-related concerns [5].

Ensuring privacy in JCAS-based CPSs requires *effective methodologies* to assess and enhance privacy protections. This involves safeguarding Personally Identifiable Information (PII), which includes data that directly or indirectly identifies individuals [6], [7]. Addressing privacy concerns in JCAS-integrated CPSs is particularly challenging in early design stages when implementation details are uncertain. Privacy engineers must make *informed decisions* on risk mitigation while balancing privacy controls with functional efficiency. Overly stringent privacy measures can increase costs and degrade performance, emphasizing the need for a well-optimized approach [8].

A JCAS-based CPS comprises of the sensing environment, JCAS components, and application components, as illustrated in Fig.1. The sensing environment includes targets in the sensing area, transmitted signals, and the reflected signals sent and captured by the base stations or the user equipment. JCAS components consist of base stations and core network entities facilitating communication and sensing. Lastly, applications consume JCAS services (depending on the use case) provided by the network operator. The risk arises not only during PII processing but also from the PII exchanged between different processes and components, potentially revealing sensitive information [4]. As illustrated in Fig. 1, both the PII exchanged between main system blocks and that shared within processes inside each component can expose privacy details.

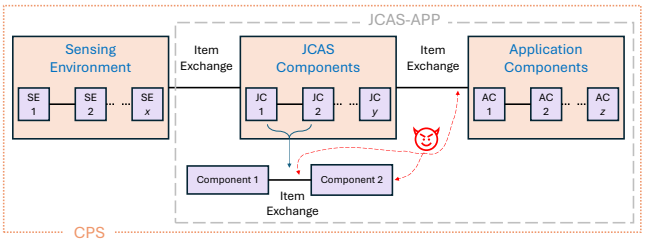

Fig. 1. Typical composition of a JCAS-based CPS.

A. Motivation

Privacy engineers face the challenge of making system-level decisions that balance privacy protection with operational needs in CPSs. Effective decision-making requires systematically aggregating, normalizing, and prioritizing privacy risks [9], [10]. However, existing methods lack quantitative approaches with precise *numeric criteria* for assessing risks and their *system-wide impact*.

A key limitation of current frameworks like the Privacy Impact Assessment (PIA) is their inability to aggregate risks across components or update evaluations dynamically when new controls are introduced [5], [7]. This underscores the

This research is co-financed based on the budget passed by the Saxonian State Parliament in Germany, and by the Federal Ministry of Education and Research, Germany, project KOMSENS-6G (funding label 16KISK122).

need for a structured, quantifiable privacy assessment tailored to complex JCAS-based CPSs. A potential solution is to limit and standardize risk-influencing parameters across system components. An effective approach involves defining key input parameters, such as the amount of PII collected, processed, stored, or transferred, and the strength of access controls. Using these unified parameters, a structured quantitative assessment can be developed.

B. Contributions

We focus on the JCAS-APP system, illustrated in Fig. 1, emphasizing the privacy implications of JCAS components within the context of the application (APP) consuming the JCAS service. This paper contributes by:

- Developing Operational View (OV) system models for the JCAS-APP;
- Identifying the characteristics of the individual components in Fig. 1 that impact the system privacy;
- Quantitatively expressing the overall privacy of the JCAS-APP system;
- Outlining the steps for systematic privacy improvements.

While our proposed approach supports all CPSs following the framework in Fig. 1, we focus on its *applicability* in a specific *use case*: JCAS-based level crossing monitoring for detecting obstacles on railway tracks [11]. This use case is practically and socially important, yet its novel nature means its privacy aspects remain under-explored in existing literature [3].

II. Existing Works

Numerous literature sources utilize PIA in their attempt to address privacy problems in CPSs. PIA seeks to identify, analyze, evaluate, and plan the treatment of possible impacts on the PII [5], [7]. PIA allows prioritizing risks based on their level, which is needed for a more efficient usage of resources. Nevertheless, conventional PIA approaches neither allow to aggregate risks nor advise how the system's separate components privacy can be enhanced to mitigate those risks.

Several modifications to PIA are documented in academic literature. In the work by [12], the authors categorize the strength of controls designed to mitigate privacy threats, for which impact assessment (IA) scores are calculated. However, their approach has limitations: the likelihoods of the threats are assigned binary values based on subjective judgments. Additionally, more research is needed to determine how individual component upgrades influence the overall IA score.

In [13], the authors utilize the NIST Privacy Risk Assessment Methodology to evaluate the privacy impacts of cyber threats in connected and autonomous vehicle (CAV) networks. They quantify the risks based on the specifics of data flows in CAVs, using parameters such as the frequency of loss, the likelihood of impact, and the magnitude of the risks. However, the study does not address how privacy controls affect these parameters or how to effectively manage the identified risks.

The authors of [14] apply the Pareto principle to balance the conflicting goals of different stakeholders involved in privacy enhancement. Nevertheless, optimizing privacy for the entire system can be computationally complex and may require heuristic methods to ensure scalability. Furthermore, privacy protection objectives need to be better defined to minimize the need for costly and frequent stakeholder surveys. This includes better modeling of the stakeholders' goals based, for example, on the resources available for privacy-related upgrades.

In [15], the authors perform a systematic literature review that examines various Privacy Impact Assessment (PIA) techniques and discusses their validation and evaluation. One of the criteria used in the review is whether PIA modifications cited in the literature are tested as part of the corresponding case studies. However, none of the PIA-related methodologies surveyed take into account the efficiency of threat mitigation under constraints.

The approach proposed in this paper contrasts with the existing body of literature: We analyze a system's privacy posture based on the parameters of separate operational view components. Due to the small number of privacy-related parameters and simple expression for risk, its value can be easily recalculated: this is especially important when new privacy-enhancing controls are introduced.

III. JCAS-Based Railway Level Crossing Use Case

We consider JCAS-assisted level crossing (LX) monitoring, whose primary functionality is to produce early warnings about hazardous situations like obstacles at the crossings, as depicted in the operational view (OV) in fig. 2 [11], [16]. The term JCAS-LX in this paper represents the JCAS-APP system where the application (APP) is the railway level crossing, LX.

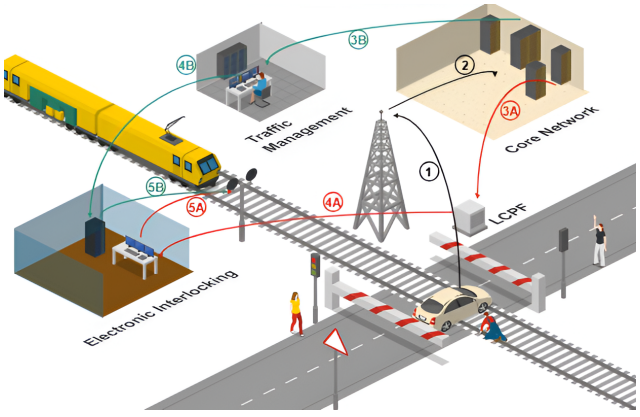

Fig. 2. OV-1 diagram of the level crossing use case.

We describe five main steps and distinguish between two modes (A and B) in implementing Sensing as a Service (SaaS) for LX monitoring. For both modes, the obstacle detection area between the barriers is sensed, ①, and the obtained data is sent for further pre-processing (e.g., clutter removal), ②. The following steps differ for A and B: a short message (e.g., a few Bytes) indicating the presence of the obstacle is sent to the Level Crossing Protection Facility (LCPF) at ③A, while richer sensing data (e.g., point clouds) is sent

to the Traffic Management System (TMS) at (3B). Electronic Interlocking receives different (but short) warning commands from LCPF and TMS at (4A) and (4B), respectively. Based on those commands, corresponding encodings are sent to change the light signal at (5A) and (5B), respectively.

The diagram in Fig 3 is a further detailization of the OV-1 diagram in fig. 2. It reflects interrelations between components of JCAS and railway systems (APP here), demonstrating why PII of natural persons in LX's proximity can be under threat well beyond the typically considered boundaries of JCAS. The diagram consists of Operational Roles (ORs) and Items of Exchange (IEs). ORs are assigned to the Performers on the Operational View (OV) diagram. IEs enable exchange between ORs: IEs may include various elements (e.g., data, signals, energy, etc.) [17].

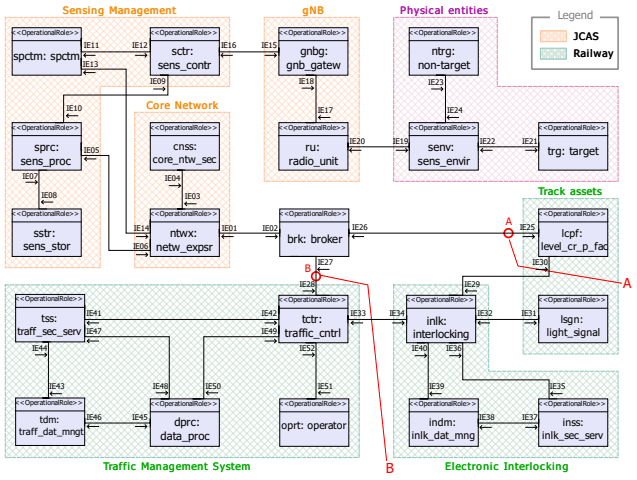

Fig. 3. OV-2 diagram of the level crossing use case.

For further analysis, we specify the boundaries of the considered subsystem: it consists of the JCAS and the Railway components only (excludes physical entities). The broker (`brk`) uses corresponding network exposure functions (`ntwx`) to request SaaS that depends on the mode of operation (`A` or `B`). The request is authorized (based on privacy policies) by SPCTM (`spctm`), after which the sensing control (`sctr`) instructs the gNB gateway (`gnbg`) to use a radio unit (`ru`) for sensing [4]. The gateway pre-processes the received raw sensing data: further processing is decided by sensing control, which typically delegates heavy pattern recognition tasks to sensing processing (`sprc`) and may store (`sstr`) the (intermediate) result. The result is sent through the broker (depending on the mode) to either LCPF (`lcpf`) or TMS (`tctr`). TMS may process rich sensing data in data processing (`dprc`) and/or data management instances (`tdm`), after which the operator (`oprt`) may make a decision to switch a warning (through interlocking, `inlk`) light signal on (`lsgn`). Instead, LCPF can send a short light-switching command and/or message through the interlocking.

IV. Proposed solution

We first propose a privacy assessment approach based on the characteristics of the components in fig. 3: We find the characteristics of individual components impacting JCAS privacy and express the overall privacy of the system. We then describe the specifics of iterative privacy enhancement while considering modes `A` and `B`.

A. Privacy assessment

We assess JCAS-LX privacy based on *1*) the principle of the 'least protected' component, which requires *2*) a coarse categorization of privacy threats and *3*) an estimation of each component's protection level.

First, the privacy of the whole JCAS-LX system relies on the privacy characteristics of its OR and IE components, as per fig. 3. Characteristics of each such component are expressed using numeric vectors $\hat{\pi}$ and $\check{\pi}$ for ORs and IEs, respectively, $\pi \in \mathbf{\Pi}$. The protection level of each component is defined using function $f(\pi) : \mathbf{\Pi} \to \mathbb{R}$. We exercise the principle of the 'least protected' component according to which the entire system's privacy evaluation θ equals $f(\pi_\omega)$:

$$\theta = f(\pi_\omega) = \min \left\{ \min_{i \in \mathbb{O}} f(\hat{\pi}_i), \min_{j \in \mathbb{I}} f(\check{\pi}_j) \right\}, \tag{1}$$

$$\omega = \arg\min \left\{ \min_{i \in \mathbb{O}} f(\hat{\pi}_i), \min_{j \in \mathbb{I}} f(\check{\pi}_j) \right\}, \tag{2}$$

where $\mathbb{O}$ and $\mathbb{I}$ are the sets of indices for ORs and IEs, respectively.

Second, for simplicity and better generalizability, we consider only a limited number of privacy threat categories: dimensionality of space $\mathbf{\Pi}$ equals the number of those selected categories. Threats can be defined based on the weaknesses associated with privacy settings, access management, and PII [4], [5]. For example, settings may lack transparency or proper user consent management. Access management may lack proper policies, or their enforcement may be weak due to insufficiently strong authenticity and/or confidentiality of interactions. The PII amount collected, processed, stored, or transferred by the components may be excessive, which will exacerbate the severity of the potential adversarial actions.

Due to poor generalizability (across different use cases) of the regulatory aspect in privacy settings, we dismiss the corresponding category of threats [4]. As such, we only consider quantities expressing the strength of access enforcement, $a \in \mathbb{N}^+$, and the amount of personal information, $p \in \mathbb{N}^+$. Smaller p is preferable since it reduces the risk of linking or identifying a person. In contrast, larger a is preferable since it reduces the risk of non-consensual information disclosure by illegitimate actors or components. Then, the resulting privacy characteristic is $\pi = (p, a)$.

Third, characteristics p and a can help us to quantify privacy risk: this can be used to define $f(\cdot)$ in eqs. (1) and (2). For example, we posit that the likelihood of a malicious exploit is in inverse relation with a; the impact of such an exploit is in direct relation with p. Because $f(\cdot)$ is in inverse

relation with the risk, it is in direct relation with a, and in inverse relation with p. Various function types can be used for $f(\cdot)$: one of the simplest and most intuitive expressions is $f^*(\pi) = \frac{a}{p}$.

TABLE I
REFERENCE VALUES FOR p

Rate	Fraction of PII*			
	N	*S*	*M*	*L*
Bit/sec	1	2	4	7
Kbit/sec	3	6	12	20
Mbit/sec	5	11	18	25
Gbit/sec	6	14	20	28
Tbit/sec	7	16	22	30

*N - negligible; S - small; M - medium; L - large.

TABLE II
REFERENCE VALUES FOR a

Authentication	Encryption	
	AES 128	AES 256
CB & RA	8	10
Two-Factor	6	8
Certificate-Based	6	8
Token-Based	5	7
Pre-Shared Key	3	6
Password-based	1	2

To ensure adequacy of calculated values $f^*(\cdot)$, for reference we propose tables I and II. In table I, p value increases – while the relation is non-linear – with the data rate in the component and depends on the evaluation of the PII's fraction in that data. In table II, a depends on the strengths of authentication and encryption in the particular component. For instance, certificate-based authentication and remote attestation (CB & RA) provide $a = 10$ if combined with AES 256 encryption.

B. Privacy enhancement

If resources permit, the privacy of the component with index ω (see eq. (2)) should be enhanced. We are guided by the following principles in enhancing JCAS-LX privacy: *1*) minimal resource usage, and *2*) iterativeness.

First, minimal resource usage refers to the technique satisfying the following conditions. The technique should decrease p_ω, $p_\omega \rightarrow p_\omega^-$, and/or increase a_ω, $a_\omega \rightarrow a_\omega^+$, such that obtained $\pi_\omega^\# = (p_\omega^-, a_\omega^+)$ satisfies

$$f^*(\pi_\omega^\#) \geq f^*(\pi_\zeta), \tag{3}$$

$$\zeta = \arg\min \left\{ \min_{i \in \{\mathbb{O} \setminus \omega\}} f(\hat{\pi}_i), \min_{j \in \{\mathbb{I} \setminus \omega\}} f(\check{\pi}_j) \right\}, \tag{4}$$

meaning that the component with index $\zeta \neq \omega$ becomes the 'least protected' component after the component with index ω is improved. In addition, the resources used to achieve eq. (3) must be minimal. For example, under the assumption that upgrade cost $\mathcal{C}(\cdot, \pi_\omega)$ adequately represents resources used for enhancement, it is required that

$$\begin{aligned} \forall\, \pi_\omega^\$, (\pi_\omega^\$ \neq \pi_\omega^\#) \wedge \left(f^*(\pi_\omega^\$) \geq f^*(\pi_\zeta)\right) \\ \implies \mathcal{C}\left(\pi_\omega^\$, \pi_\omega\right) \geq \mathcal{C}\left(\pi_\omega^\#, \pi_\omega\right). \end{aligned} \tag{5}$$

Second, resources may still be available after the component with index ω is improved, meaning that the enhancement should be repeated for the component with index ζ and so on [5]. The following aspects are important. Dedicated enhancement of one component may affect other components: reducing PII (e.g., parameter p_ω) in component ω may also reduce PII in other components exchanging information items with the component ω. In addition, demonstrating that $\theta(t)$ is monotonic (non-decreasing) simplifies enhancement. We further consider enhancements for modes A and B (see fig. 3).

Example #1 For privacy assessment and enhancement in mode A, we collect information about authentication, confidentiality, and access control mechanisms. In addition, for different components of JCAS-LX and based on the functional needs, we obtain estimates for data rate and an expert judgment about the fraction of PII. We establish that the least protected components are $\mathrm{OR}_{\texttt{gnbg}}$ and IE_{18}: for these components we have $\hat{\pi}_{\texttt{gnbg}} = \check{\pi}_{18} = (15, 6)$, $f^*(\hat{\pi}_{\texttt{gnbg}}) = f^*(\check{\pi}_{18}) = 0.4$. On the one hand, the value a will remain relatively low even after the enhancement. Due to the high data rate in those components, even a small increase in latency may be detrimental to the whole system's performance. To avoid this, it is essential to constrain a: hence, $\hat{a}_{\texttt{gnbg}}$ and $\check{a}_{18}$ can only be increased from 6 to 8 while all other components in the system already have $a \geq 8$. On the other hand, value p will remain relatively high. Initially, characteristics $\hat{p}_{\texttt{gnbg}} = \check{p}_{18} = 15$ are the highest in the system. If additional data minimization controls are applied to $\mathrm{OR}_{\texttt{gnbg}}$ and IE_{18}, corresponding p will decrease (which may reduce p in other components) but it will still remain the highest in the system: irrespective of the enhancement iteration, JCAS-LX privacy engineer should consider those components only.

Example #2 Depending on the initial configuration and enhancements, the 'least protected' component may belong to different system parts (e.g., JCAS or Railway) in mode B. As in the previous example, the weakest links of the JCAS part are $\mathrm{OR}_{\texttt{gnbg}}$ and IE_{18}. In addition to that, the Railway part in mode B contains $\mathrm{OR}_{\texttt{oprt}}$ and IE_{51} which might be the 'weakest links' under certain circumstances. We model the iterative enhancement as the process where decreasing of PII at time t (e.g., $p(t) \rightarrow p^-(t)$) depends on the upgrades of access control at time t (e.g., $a(t) \rightarrow a^+(t)$). The latter is governed by the independent Markov processes shown in fig. 4(a) and fig. 4(b) for the weakest components in JCAS and the Railway, respectively. Symbol '*S*' denotes the start of the enhancement process at t_0 while further transitions at time steps $t > t_0$ occur in accordance with the probabilities shown in the diagrams. We combine information about the two processes in fig. 4 to obtain a matrix describing transitions for all the possible combinations of $(\check{a}_{18}, \check{a}_{51})$ (see fig. 5).

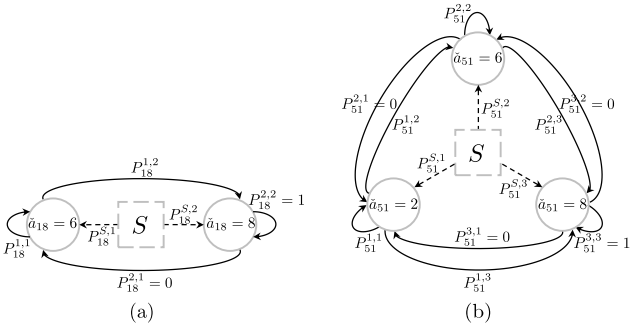

Fig. 4. Markov chain for: (a) $\check{a}_{18}$ in JCAS part, (b) $\check{a}_{51}$ in Railway part.

From: \ To:	S	$(6,2)$	$(8,2)$	$(6,6)$	$(8,6)$	$(6,8)$	$(8,8)$
(S)tart	0	$P_{18}^{S,1}P_{51}^{S,1}$	$P_{18}^{S,2}P_{51}^{S,1}$	$P_{18}^{S,1}P_{51}^{S,2}$	$P_{18}^{S,2}P_{51}^{S,2}$	$P_{18}^{S,1}P_{51}^{S,3}$	$P_{18}^{S,2}P_{51}^{S,3}$
$(\check{a}_{18}=6,\check{a}_{51}=2)$	0	$P_{18}^{1,1}P_{51}^{1,1}$	$P_{18}^{1,2}P_{51}^{1,1}$	$P_{18}^{1,1}P_{51}^{1,2}$	$P_{18}^{1,2}P_{51}^{1,2}$	$P_{18}^{1,1}P_{51}^{1,3}$	$P_{18}^{1,2}P_{51}^{1,3}$
$(\check{a}_{18}=8,\check{a}_{51}=2)$	0	0	$P_{51}^{1,1}$	0	$P_{51}^{1,2}$	0	$P_{51}^{1,3}$
$(\check{a}_{18}=6,\check{a}_{51}=6)$	0	0	0	$P_{18}^{1,1}P_{51}^{2,2}$	$P_{18}^{1,2}P_{51}^{2,2}$	$P_{18}^{1,1}P_{51}^{2,3}$	$P_{18}^{1,2}P_{51}^{2,3}$
$(\check{a}_{18}=8,\check{a}_{51}=6)$	0	0	0	0	$P_{51}^{2,2}$	0	$P_{51}^{2,3}$
$(\check{a}_{18}=6,\check{a}_{51}=8)$	0	0	0	0	0	$P_{18}^{1,1}$	$P_{18}^{1,2}$
$(\check{a}_{18}=8,\check{a}_{51}=8)$	0	0	0	0	0	0	1

Fig. 5. Joint transition probabilities (derived from Markov chains in fig. 4).

Values p of corresponding components in JCAS or Railway should be reduced depending on a at time t. Parity between JCAS and Railway sub-systems occurs when their 'weakest' components are equally protected: parity plots can be defined in the coordinate system $\langle \check{p}_{18}, \check{p}_{51} \rangle$, (see fig. 6). Transitions (switching) between the plots happen according to fig. 5. For instance, if at time t_0 the system starts with $\check{a}_{18} = 6$ and $\check{a}_{51} = 2$, then the parity is achievable for all the points $(\check{p}_{18}, \check{p}_{51})$ belonging to the magenta plot. If point $(\check{p}_{18}, \check{p}_{51})$ is above the corresponding plot, the Railway privacy engineer should reduce $\check{p}_{51}$. If $(\check{p}_{18}, \check{p}_{51})$ is below the corresponding plot, the JCAS privacy engineer should reduce $\check{p}_{18}$. The properties of the transition matrix (see fig. 5) and the fact that p values decrease over t ensure the monotonicity of privacy enhancement.

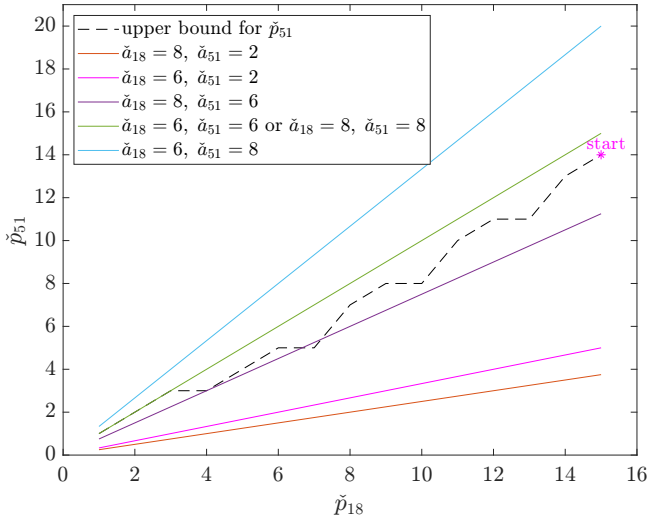

Fig. 6. Parity plots for mode B.

V. Discussion

The new privacy assessment approach developed in this paper can assist privacy engineers in making *informed decisions* about enhancing privacy controls in large and complex CPSs. By applying this approach, privacy engineers can identify the system components that require the most attention and take steps to mitigate potential privacy risks.

The approach's *applicability* is demonstrated through the JCAS-enabled LX obstacle detection *use case* for railways (see Figures 2 and 3). This use case permits different scenarios (A and B) of JCAS-based service utilization, allowing us to understand how different stakeholders may use our approach to upgrade corresponding parts of JCAS-based CPS competitively. For instance, **Example #2** (see section IV-B) helps us better comprehend the true stakeholders' behavior (and consequences) in realistic settings when new technologies and services are being deployed. The latter knowledge can be leveraged by privacy regulators overseeing JCAS adoption in the future [5], [18].

The *underlying principle* of our privacy assessment and enhancement is *simple*: the risk value (and the priority for enhancing) of a system's component depends on the amount of PII and the access strength. This principle is based on the most comprehensive definitions of privacy (e.g., privacy is the protection of PII) and risk, making our approach adequate and generalizable to different CPSs. Our approach *contrasts* with existing approaches, such as various PIA modifications, by aggregating, normalizing, and prioritizing privacy risks. This covers the *gap* currently existing in the literature (see section II). In addition, it allows for quick recalculation of the risk value after privacy-enhancing controls are applied to the corresponding components [19]. To infer the value of privacy risk, we only use $\min - \max$ operations, which makes our approach scalable and efficient (see eqs. (1), (2) and (4)). This is particularly important in the context of *large CPSs*, where integrating communication and sensing capabilities brings additional structural complications on a system level [4].

Our approach follows these *major steps*: first, a JCAS-based CPS is represented in the form of connected components with an appropriate level of granularity (suitable to judge the amount of PII and access strength in those components). For this, we utilize system engineering principles (e.g., DoDAF) to create OV-1 and OV-2 diagrams [17], [20]. Second, expert judgment is made about the amount of PII and the access control strength for every component and every link on the OV-2 diagram. For instance, the amount of PII in a component depends on the corresponding rate, but the strength of access control depends on authentication and encryption technologies (see tables I and II). Third, unsolicited PII disclosure risk value is calculated for every component based on the function whose arguments are the amount of PII and the strength of access control (see $f^*(\cdot)$ in section IV-A). Fourth, the component with the highest risk value (e.g., the lowest $f^*(\cdot)$) constitutes the "weakest link" of

the system: the privacy engineer is advised to enhance privacy controls for this component to improve the privacy posture of the whole system (see eq. (2)).

While our approach is advantageous, it also has certain limitations we *plan to address*. For instance, expert judgment may be subjective, and one way to overcome this is to introduce means for a group of experts to come to a *consensus*. Additionally, the decision to enhance a system's component should be supported by the tools allowing the selection of appropriate privacy controls under the *constraint on resources* (e.g., time, budget) available to the privacy engineer [8]. The development of these tools is yet another challenging task.

References

[1] A. Akbarzadeh and S. Katsikas, "Unified IT&OT modeling for cybersecurity analysis of cyber-physical systems," *IEEE Open Journal of the Industrial Electronics Society*, vol. 3, pp. 318–328, 2022.

[2] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, 2021.

[3] 3GPP, "Feasibility Study on Integrated Sensing and Communication (Release 19)," 3GPP, Tech. Rep. TR 22.837 V19.4.0, 2024.

[4] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing Privacy Concerns in Joint Communication and Sensing for 6G Networks: Challenges and Prospects," in *Privacy Technologies and Policy*, 2024, pp. 87–111.

[5] "ISO/IEC International Standard -Information security, cybersecurity and privacy protection – Privacy operationalisation model and method for engineering (POMME)," *ISO/IEC 27561:2024(en)*, pp. 1–36, 2024.

[6] C. Kumar, S. Marston, and R. Sen, "Cyber-physical systems (CPS) security: State of the art and research opportunities for information systems academics," *Communications of the Association for Information Systems*, vol. 47, no. 1, p. 36, 2020.

[7] "ISO/IEC International Standard – Information technology – Security techniques – Guidelines for privacy impact assessment," pp. 1–43, 2023, ISO/IEC 29134:2023(E).

[8] F. Smeraldi and P. Malacaria, "How to spend it: Optimal investment for cyber security," in *Proceedings of the 1st International Workshop on Agents and Cyber-Security*, 2014.

[9] K. Stine, S. Quinn, G. Witte, and R. Gardner, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," National Institute of Standards and Technology, Tech. Rep. NIST Internal or Interagency Report (NISTIR) 8286, 2020.

[10] R. He, Z. Jin, and J. S.-H. Li, "Modeling and management of cyber risk: A cross-disciplinary review," *Annals of Actuarial Science*, vol. 18, no. 2, pp. 270–309, 2024.

[11] R. Mollenhauer, "Level Crossing Obstacle Detection System," in *2007 IET Seminar on Reducing Risk at the Road Rail Interface*, 2007, pp. 71–80.

[12] A. S. Ahmadian, D. Strüber, V. Riediger, and J. Jürjens, "Supporting privacy impact assessment by model-based privacy analysis," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 9, 2018, pp. 1467–1474.

[13] S. Panda, E. Panaousis, G. Loukas, and K. Kentrotis, "Privacy Impact Assessment of Cyber Attacks on Connected and Autonomous Vehicles," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023.

[14] M. Mollaeefar and S. Ranise, "Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR," *Computers & Security*, vol. 129, p. 103 206, 2023.

[15] S. Wairimu, L. H. Iwaya, L. Fritsch, and S. Lindskog, "On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review," *IEEE Access*, vol. 12, pp. 19 625–19 650, 2024.

[16] G. Theeg and S. Vlasenko, *Railway Signalling and Interlocking International Compendium*, 3rd edition. Edition Eurailpress, 2019.

[17] "IEEE/ISO/IEC International Standard for Software, systems and enterprise–Architecture description," *ISO/IEC/IEEE 42010:2022(E)*, pp. 1–74, 2022.

[18] K. Boeckl, M. Fagan, W. Fisher, *et al.*, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8228, 25, 2019.

[19] T. Bisztray and N. Gruschka, "Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality," in *Secure IT Systems*, 2019, pp. 3–19.

[20] A. G. Romero, K. Schneider, and M. G. V. Ferreira, "Semantics in Space Systems Architectures," *Innovations in Systems and Software Engineering*, vol. 12, no. 1, pp. 27–40, 1, 2016.