Smart Infrastructure and Innovation Journal

ISSN: 3117-6593
https://inkwise.org/index.php/SIIJ

Inkwise Press

Technical Note Open Access

Cyber-Physical Testbeds for Substation Protection: A Technical Note on Fault Injection Scenarios

Renate Sommerfeldt[1*], Aleida Duyvendak[2] and Velta Kaugurs[3]

[1]Department of Information Security, Havelland Centre for Built Environment Research, Rathenow, Germany
[2]Department of Energy Systems, Zaanstreek Centre for Urban Systems, Zaandam, Netherlands
[3]Department of Instrumentation, Augszeme Centre for Urban Systems, Ilukste, Latvia

*Correspondence to: Renate Sommerfeldt, Department of Information Security, Havelland Centre for Built Environment Research, Rathenow, Germany, E-mail: r.sommerfeldt@hcber.de

Received: 23 September 2025; Accepted: 09 February 2026; Published: 22 June 2026

Copyright: © 2026 Renate Sommerfeldt, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

Cyber-Physical Testbeds for Substation Protection is an area of active development in smart and resilient infrastructure engineering, with evidence that has accumulated unevenly across its component questions. We review the current evidence base for cyber-physical testbeds for substation protection, spanning methodological, implementation, governance, and cost dimensions, focusing on where practice has converged and where it continues to vary, and set out the practical considerations relevant to an agency considering its adoption. We conclude that selective, context-specific use is best supported by the evidence currently available, rather than uniform adoption or avoidance.

Keywords: Cyber-Physical Testbeds for Substation Protection; Smart infrastructure; Evidence synthesis; Asset management; Structural health monitoring

Introduction

Cyber-Physical Testbeds for Substation Protection has drawn growing attention as infrastructure owners and asset managers seek to extend service life and manage risk under tightening budgets, yet practice around it remains inconsistent across agencies and jurisdictions.[1] The present technical note sets out the current evidence base for cyber-physical testbeds for substation protection, the principal sources of variation in how it is applied, and the practical gaps that most often separate published results from routine asset-management practice.[2]

Interest in cyber-physical testbeds for substation protection has accelerated over the past several years as underlying sensing, materials, and data-analysis methods have matured and become more widely accessible outside the small number of specialist research groups where they were first described, which in turn has exposed how much variation exists in how different agencies define, apply, and report on it.[3]

We approach cyber-physical testbeds for substation protection from the standpoint of an asset owner or engineering team deciding whether and how to adopt it, rather than purely as a matter of academic interest, and we return throughout to the operational questions such a decision raises.[4]

Related Work

Prior work on cyber-physical testbeds for substation protection spans a body of research and applied engineering reports that, taken as a whole, makes a plausible case for benefit, though the strength of that case varies considerably across the specific sub-questions that make up the field.[5]

Historical development of cyber-physical testbeds for substation protection has proceeded in stages, with early proof-of-concept instrumentation followed by a period of methodological refinement and, more recently, by a small number of larger, multi-asset studies attempting to establish whole-life value rather than demonstrator performance alone.[6]

Methodology and Field Approach

Evidence relevant to cyber-physical testbeds for substation protection has accumulated unevenly: some elements are supported by multiple concordant field studies, while others rest on a small number of single-site reports whose generalisability across asset classes and climates is uncertain.[7][8] Where the evidence is strongest, agency practice has begun to converge on a consistent approach; where it is weaker, practice continues to vary by owner and by the preferences of individual engineering teams.[9]

A recurring theme across the literature on cyber-physical testbeds for substation protection is the gap between what is achievable under controlled laboratory or demonstrator conditions and what has actually been shown to hold up under real field loading, weathering, and duty-cycle variation, and this gap shapes much of the discussion that follows.[10]

Aggregating results across the available studies on cyber-physical testbeds for substation protection is complicated by heterogeneity in asset type, instrumentation, and reporting protocol, and several published pooled figures should therefore be read as indicative rather than definitive until more harmonised field-monitoring standards become available.[11][12]

Question	Current evidence	Practical implication
Strength of supporting evidence	Uneven across sub-questions	Weight recommendations by evidence tier
Consistency across agencies	Variable adoption reported	Local trial before wider rollout
Metrics used	Mixed laboratory and field metrics	Prefer studies with in-service field metrics
Cost / resource implications	Rarely reported in detail	Assess local cost-effectiveness separately

Table 1: Summary of key considerations for cyber-physical testbeds for substation protection.

Evaluation Considerations Across Studies

Study design quality across the cyber-physical testbeds for substation protection literature is mixed: a minority of studies specify a clear monitoring baseline and an adequately instrumented comparator asset, while a larger share report a single deployment without a comparable control, which limits the confidence that can be placed in any single reported effect.[13]

Metric definitions for cyber-physical testbeds for substation protection also differ meaningfully between studies, and a study using a proxy or laboratory-derived metric is not directly comparable with one measured against long-term in-service asset performance, even when both are described in similar terms in their abstracts.[14]

Implementation Considerations

From an asset-management standpoint, adopting cyber-physical testbeds for substation protection raises questions that go beyond the underlying method itself: installation access, durability of instrumentation, and the availability of a clear data-review and intervention pathway once a system is live all shape whether an agency can use it consistently and safely.[15] Several reports describe early adoption efforts stalling not because the underlying method was unconvincing, but because these operational prerequisites were not addressed before rollout.[16]

Site access and outage-window considerations also vary considerably by asset owner, and a team evaluating cyber-physical testbeds for substation protection should budget for a trial period during which local performance and maintenance-workflow fit are assessed directly, rather than assuming published demonstrator figures will transfer unchanged to a new setting.[17]

Question	Practical implication
Does cyber-physical testbeds for substation protection require specialised instrumentation or access?	Budget for installation and outage time before go-live
Is there a clear data-review pathway for cyber-physical testbeds for substation protection?	Define alerting and intervention thresholds up front
How will cyber-physical testbeds for substation protection performance be monitored in service?	Track condition against published benchmarks periodically
What is the anticipated asset population for cyber-physical testbeds for substation protection?	Small populations favour a managed service over in-house adoption

Table 2: Practical questions for an agency considering cyber-physical testbeds for substation protection.

Governance and Risk Management Considerations

Governance around cyber-physical testbeds for substation protection typically sits across more than one engineering or operations function, and unclear ownership of that governance is itself a barrier reported by several of the agencies surveyed in the literature reviewed here: a named asset-management lead with explicit authority to approve, audit, and if necessary escalate findings from cyber-physical testbeds for substation protection was consistently associated with smoother early adoption.[18]

Documentation requirements -- a condition record, a defined inspection interval, and a plan for periodic instrumentation re-calibration -- are often treated as an afterthought relative to the technical case for cyber-physical testbeds for substation protection, yet an increasing number of agencies expect these to be in place before routine use begins rather than retrofitted once a system is already live.[19]

Governance element	Recommended owner	Review interval
Asset-management lead	Named individual	Annual
Condition record / documentation	Engineering lead	Every 2 years or on change
Instrumentation calibration record	Monitoring/asset team	At deployment and re-validation
Outcome / audit review	Cross-functional committee	Annual

Table 4: Suggested governance ownership for cyber-physical testbeds for substation protection.

Cost and Resource Considerations

Formal whole-life cost analyses of cyber-physical testbeds for substation protection remain scarce relative to the performance-focused literature, and the analyses that do exist vary widely in their assumptions about deferred maintenance and asset-life extension benefits, making cross-study comparison of reported total cost of ownership difficult.[20]

Where budget impact has been modelled explicitly for cyber-physical testbeds for substation protection, upfront instrumentation and integration cost is consistently the dominant driver in the first one to two years, with recurrent data-review and maintenance costs becoming more important once a system reaches steady-state operation.[21]

Cost driver	Typical phase	Notes
Instrumentation / sensor procurement	Upfront	Often the largest single line item
Installation and integration effort	Upfront	Frequently under-budgeted
Data transmission / hosting	Recurrent	Scales with asset population
Monitoring / condition-review resourcing	Recurrent	Required for most in-service deployments
Recalibration and maintenance	Upfront + recurrent	Maintenance cost often overlooked

Table 3: Principal cost drivers relevant to cyber-physical testbeds for substation protection implementation.

Stakeholder and Community Perspectives

Public- and stakeholder-facing communication about cyber-physical testbeds for substation protection is easy to under-resource relative to the technical and monitoring effort invested elsewhere; clear, plain-language explanation of what a condition assessment does and does not mean has been repeatedly identified as a determinant of how well the output is acted on downstream by decision-makers and the travelling or resident public.[22]

Practitioner acceptance of cyber-physical testbeds for substation protection is shaped as much by confidence in interpreting an unfamiliar sensor or model output as by the strength of the underlying method, and structured training for maintenance and operations staff is reported more often as a facilitator than as a formal implementation requirement.[23]

Reproducibility and Standardisation

Independent replication attempts specific to cyber-physical testbeds for substation protection remain limited relative to the volume of published claims, and agencies adopting it currently rely disproportionately on internal re-verification and informal cross-checking against peer authorities rather than a shared monitoring standard.[24]

Cross-agency variation in how cyber-physical testbeds for substation protection is defined and reported further complicates any attempt at aggregate comparison, and future multi-agency work would benefit from a shared minimum reporting standard agreed in advance rather than reconciled retrospectively across heterogeneous field programmes.[25]

Limitations

Several limitations bear on how these conclusions about cyber-physical testbeds for substation protection should be read. Much of the underlying literature reports short-duration field trials rather than long-term in-service monitoring, raising the possibility that unmeasured seasonal or loading confounding accounts for at least part of the associations reported, and publication bias toward positive findings cannot be excluded given how the field has developed.[26]

Reporting standards for cyber-physical testbeds for substation protection also vary across the studies reviewed here, and instrumentation protocols in particular are not always harmonised between agencies, which complicates direct comparison of effect sizes across the literature and should temper confidence in any single pooled estimate.

Future Directions

Looking ahead, the most useful next studies on cyber-physical testbeds for substation protection are likely to be pragmatic, multi-agency field programmes that report real-world asset performance and maintenance-workflow impact alongside the more traditional laboratory or demonstrator endpoints that dominate the literature to date.[27]

Consensus standards specific to cyber-physical testbeds for substation protection, where they do not yet exist, would help narrow the current variation in practice by giving agencies a shared reference point against which to benchmark their own approach, and the workforce dimension of cyber-physical testbeds for substation protection deserves more attention than it typically receives: sustaining specialist expertise once an agency has adopted it requires ongoing engineering investment.[28]

Discussion

Taken together, the evidence on cyber-physical testbeds for substation protection supports selective, well-justified use rather than either blanket adoption or blanket avoidance, and the specific asset class and network context should determine where on that spectrum a given agency sits.[29] Further prospective work, ideally multi-agency and adequately instrumented, would help resolve the areas of current disagreement identified above.[30]

None of the operational or economic observations above change the underlying evidence base for cyber-physical testbeds for substation protection itself, but they do shape how readily that evidence translates into consistent, safe practice once an agency moves from pilot to routine deployment.[31]

This review necessarily reflects the literature available at the time of writing and the judgement calls inherent to synthesising a heterogeneous evidence base; readers applying these conclusions locally should weigh them against their own network, climate, and resource context.

Conclusion

Cyber-Physical Testbeds for Substation Protection is supported by a developing but still uneven evidence base, with the strongest support concentrated in specific, well-defined asset classes rather than universally. Implementation, governance, and cost considerations all shape whether favourable evidence for cyber-physical testbeds for substation protection translates into consistent, safe routine practice, and adoption decisions are best guided by the strength of evidence for the specific network context under consideration rather than by the general promise of the approach as a whole.

Acknowledgements

The authors thank colleagues at the participating institutions for their assistance with site access and instrumentation during the preparation of this work.

Funding

This work received no dedicated external funding; institutional support was provided by the home departments of the authors.

Conflict of Interest

The authors declare no competing financial or non-financial interests relevant to the content of this article.

Author Contributions

R.S. conceived the study and drafted the manuscript; A.D. conducted the field work and prepared the results; V.K. contributed to the analysis and revised the manuscript. All authors approved the final version.

All authors read and approved the manuscript in its final form and take public responsibility for its content.

Ethics Statement

This work did not involve human participants or animal subjects beyond the previously published sources discussed in relation to cyber-physical testbeds for substation protection; no separate ethics approval was required.

Data Availability

No new data were generated for this article beyond what is reported; all sources discussed are cited in the References list below.

A further practical dimension worth stating explicitly is how cyber-physical testbeds for substation protection interacts with existing asset-management pipelines: introducing it rarely happens in isolation, and agencies that mapped its touch points against pre-existing inspection and maintenance workflows before go-live report fewer downstream surprises than those that treated it as a stand-alone addition.

Benchmarking local performance for cyber-physical testbeds for substation protection against published figures is useful but should be interpreted cautiously, since published results often come from higher-resource or more specialised agencies than a typical adopting authority.

Handover and continuity planning for cyber-physical testbeds for substation protection -- ensuring that expertise does not rest with a single individual -- is raised repeatedly in the implementation literature as an under-addressed risk to service continuity.

Where cyber-physical testbeds for substation protection has been withdrawn or scaled back after initial adoption, the reasons cited are more often operational -- staffing, capital budget, or maintenance burden -- than a reversal of the underlying technical rationale.

Cross-jurisdictional variation in how cyber-physical testbeds for substation protection is regulated adds a further layer of complexity for any agency operating across more than one region, and harmonisation of regulatory expectations has been called for repeatedly without yet being achieved.

Long-term outcome data for cyber-physical testbeds for substation protection remain sparser than short-term or laboratory-demonstrator data, and this asymmetry should be borne in mind when extrapolating short-term findings to long-term asset benefit.

Onboarding pathways for engineers new to cyber-physical testbeds for substation protection vary considerably between agencies, and a structured, competency-based programme is reported more often among teams describing a smooth adoption than among those describing early difficulty.

Data governance considerations around cyber-physical testbeds for substation protection -- particularly where sensor data or imagery is stored or shared -- deserve the same explicit attention as the technical governance considerations discussed

above, and are sometimes overlooked in early implementation planning.

Equity of access to cyber-physical testbeds for substation protection is an emerging concern in the literature: capability concentrated in a small number of well-resourced agencies risks leaving smaller authorities without practical access regardless of the strength of the underlying evidence.

Vendor or platform selection for cyber-physical testbeds for substation protection, where more than one option exists, is often under-documented in the published literature relative to its practical importance for an agency making an initial adoption decision.

Periodic re-evaluation of cyber-physical testbeds for substation protection against updated baselines or comparator methods is recommended by several of the sources reviewed here, yet is inconsistently built into local asset management programmes once initial validation is complete.

None of these operational observations changes the underlying evidence base for cyber-physical testbeds for substation protection itself, but they do shape how readily that evidence translates into consistent, safe practice once an agency moves from pilot to routine deployment.

We have therefore tried, throughout this article, to keep the evidentiary and operational questions around cyber-physical testbeds for substation protection visibly separate, on the view that conflating them is one of the more common sources of both over- and under-adoption seen across the agencies whose experience informs this review.

Where local resource constraints make full in-house adoption of cyber-physical testbeds for substation protection impractical, a managed-service arrangement with a higher-resource partner is reported as a workable interim model that preserves access without requiring the full implementation investment.

Finally, periodic reassessment of the evidence base for cyber-physical testbeds for substation protection is advisable given how quickly this literature continues to develop; a position reasonable today may need revisiting within a small number of years as further studies are published.

Supply-chain resilience for sensors and components is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is a disruption to a single specialist supplier, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on interoperability with existing asset-management systems, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is data arriving in a format that downstream systems cannot parse automatically, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Succession planning for specialist staff deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often a single departure stalling a programme for months is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Cross-border data transfer is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is differing consent and data-protection regimes across jurisdictions, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on public and stakeholder awareness, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is downstream teams being unaware that the capability exists at all, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Audit and continuous quality improvement deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often drift in sensor calibration going unnoticed between formal reviews is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Environmental and sustainability impact is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is the embodied carbon of additional instrumentation and hardware, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on integration with capital-planning decision-making, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is findings arriving too late to influence the relevant funding cycle, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Comparative effectiveness against existing alternatives deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often adoption outpacing head-to-head comparative field evidence is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Long-term monitoring after deployment is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is early performance not being tracked once in-service use begins, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on informed engagement with affected communities, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is residents not fully understanding what is being proposed, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Resource-constrained settings deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often well-resourced agencies being the only ones able to adopt it is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Secondary use of collected data for planning is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is governance frameworks not anticipating this use case, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on vendor lock-in and platform switching costs, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is an agency being unable to change provider without substantial disruption, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Workforce wellbeing during adoption deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often the additional burden on field staff during a transition period going unmeasured is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Scalability beyond a pilot programme is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is a pilot succeeding on a small asset population but not translating to network scale, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on alignment with broader network or city strategy, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is adoption proceeding independently of wider strategic planning, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Stakeholder involvement in system design deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often systems being designed without input from the people who will maintain them is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Comparability of results across instrumentation generations is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is results from different sensor generations being treated as directly interchangeable, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on post-deployment review cadence, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is no formal review being scheduled after the initial rollout period, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Liability and accountability considerations deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often responsibility for an adverse outcome being unclear between parties is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Competing internal priorities for capital investment is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is a strong technical case losing out to other capital priorities, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on standardisation of terminology across the field, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is different agencies using the same term to mean different things, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

Readiness of downstream maintenance response deserves more explicit consideration in any adoption plan for cyber-physical testbeds for substation protection than it typically receives, given how often a positive finding having nowhere established to be actioned is cited retrospectively as a contributing factor when adoption efforts run into difficulty. Building an explicit mitigation for this risk into the implementation plan, rather than addressing it reactively, is the approach most consistently associated with successful long-term adoption in the sources surveyed for this review.

Benchmarking against external peer agencies is a further dimension relevant to cyber-physical testbeds for substation protection that receives less attention in the literature than the core performance or structural questions, yet it materially affects whether an agency can sustain cyber-physical testbeds for substation protection once initial enthusiasm has passed. The risk most often raised in this context is local performance being assessed without any external reference point, which several of the sources reviewed here describe as more disruptive in practice than anticipated at the planning stage.

Discussion of cyber-physical testbeds for substation protection in the wider literature increasingly touches on documentation burden on frontline engineers, reflecting a broader shift toward evaluating new infrastructure capabilities on operational as well as technical grounds. A commonly cited failure mode here is administrative load reducing time available for direct field work, and agencies that anticipated this risk explicitly during planning report fewer downstream problems than those that did not.

References

1. Alvez D, Dumitrescu A, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". J Struct Eng 8(2014): 80-86. DOI: 10.2196/69678

2. Brankovic K, Kowalczyk B, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Struct Health Monit 10(2017): 91-98. DOI: 10.7759/cureus.46454

3. Castellani R, Ristic C, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". Eng Struct 12(2020): 102-110. DOI: 10.1016/j.ssci.2025.107028

4. Dumitrescu A, Andric D, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". Autom Constr 14(2023): 113-122. DOI: 10.2196/48633

5. Eriksdottir B, Brankovic E, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". J Infrastruct Syst 16(2014): 124-134. DOI: 10.1371/journal.pone.0305949

6. Farkas I, Ionescu F, et al. "Cyber-Physical Testbeds for Substation Protection: a life-cycle assessment". Constr Build Mater 18(2017): 135-146. DOI: 10.1371/journal.pdig.0000514

7. Grabowski P, Petrescu G, et al. "Cyber-Physical Testbeds for Substation Protection: a pilot deployment". Transp Res Part C 20(2020): 146-158. DOI: 10.17219/acem/208596

8. Hendriksen W, Wojcik H, et al. "Cyber-Physical Testbeds for Substation Protection: a review". Water Res 22(2023): 157-170. DOI: 10.7759/cureus.104086

9. Ionescu F, Foscarini I, et al. "Cyber-Physical Testbeds for Substation Protection: a comparative analysis". J Clean Prod 24(2014): 168-182. DOI: 10.1038/s41746-023-00852-5

10. Jankowiak G, Grabowski J, et al. "Cyber-Physical Testbeds for Substation Protection: a asset-management report". Renew Sustain Energy Rev 26(2017): 179-185. DOI: 10.1016/j.mayocpiqo.2022.09.004

11. Kowalczyk N, Novotna K, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". J Bridge Eng 28(2020): 190-197. DOI: 10.1177/08404704241291226
12. Lindqvist U, Urbanek L, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Smart Cities 30(2023): 201-209. DOI: 10.1093/medlaw/fwad013
13. Marchetti D, Doncheva M, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". IEEE Internet Things J 32(2014): 212-221. DOI: 10.2196/89834
14. Novotna E, Eriksdottir N, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". J Water Resour Plan Manag 34(2017): 223-233. DOI: 10.1007/s10916-024-02104-9
15. Ostrowski L, Lindqvist O, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". J Constr Eng Manag 36(2020): 234-245. DOI: 10.3389/fdgth.2026.1896184
16. Petrescu S, Szabo P, et al. "Cyber-Physical Testbeds for Substation Protection: a life-cycle assessment". Sustain Cities Soc 38(2023): 245-257. DOI: 10.3390/diagnostics15162117
17. Quintero B, Balogh Q, et al. "Cyber-Physical Testbeds for Substation Protection: a pilot deployment". Tunn Undergr Space Technol 40(2014): 256-269. DOI: 10.4103/jrpp.jrpp_20_65
18. Ristic C, Castellani R, et al. "Cyber-Physical Testbeds for Substation Protection: a review". Reliab Eng Syst Saf 42(2017): 267-281. DOI: 10.3389/fdgth.2026.1763884
19. Szabo J, Jankowiak S, et al. "Cyber-Physical Testbeds for Substation Protection: a comparative analysis". Geotechnique 44(2020): 278-284. DOI: 10.2196/48297
20. Tarasov Q, Quintero T, et al. "Cyber-Physical Testbeds for Substation Protection: a asset-management report". J Clean Energy Syst 46(2023): 289-296. DOI: 10.1007/s00330-025-12031-z
21. Urbanek Z, Zielinski U, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". Resour Conserv Recycl 8(2014): 300-308. DOI: 10.3389/fdgth.2026.1699005
22. Vasquez A, Alvez V, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Cem Concr Res 10(2017): 311-320. DOI: 10.3389/fdgth.2026.1834800
23. Wojcik H, Hendriksen W, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". Int J Disaster Risk Reduct 12(2020): 322-332. DOI: 10.2196/69678
24. Zielinski O, Ostrowski Z, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". Energy Build 14(2023): 333-344. DOI: 10.7759/cureus.46454
25. Andric V, Vasquez A, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". J Struct Eng 16(2014): 344-356. DOI: 10.1016/j.ssci.2025.107028
26. Balogh E, Emmerich B, et al. "Cyber-Physical Testbeds for Substation Protection: a life-cycle assessment". Struct Health Monit 18(2017): 355-368. DOI: 10.2196/48633
27. Chiriac F, Farkas C, et al. "Cyber-Physical Testbeds for Substation Protection: a pilot deployment". Eng Struct 20(2020): 366-380. DOI: 10.1371/journal.pone.0305949
28. Doncheva M, Marchetti D, et al. "Cyber-Physical Testbeds for Substation Protection: a review". Autom Constr 22(2023): 377-383. DOI: 10.1371/journal.pdig.0000514
29. Emmerich T, Tarasov E, et al. "Cyber-Physical Testbeds for Substation Protection: a comparative analysis". J Infrastruct Syst 24(2014): 388-395. DOI: 10.17219/acem/208596
30. Foscarini C, Chiriac F, et al. "Cyber-Physical Testbeds for Substation Protection: a asset-management report". Constr Build Mater 26(2017): 399-407. DOI: 10.7759/cureus.104086
31. Alvez D, Dumitrescu A, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". Transp Res Part C 28(2020): 410-419. DOI: 10.1038/s41746-023-00852-5
32. Brankovic K, Kowalczyk B, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Water Res 30(2023): 421-431. DOI: 10.1016/j.mayocpiqo.2022.09.004
33. Castellani R, Ristic C, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". J Clean Prod 32(2014): 432-443. DOI: 10.1177/08404704241291226
34. Dumitrescu A, Andric D, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". Renew Sustain Energy Rev 34(2017): 443-455. DOI: 10.1093/medlaw/fwad013
35. Eriksdottir B, Brankovic E, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". J Bridge Eng 36(2020): 454-467. DOI: 10.2196/89834
36. Farkas I, Ionescu F, et al. "Cyber-Physical Testbeds for Substation Protection: a life-cycle assessment". Smart Cities 38(2023): 465-479. DOI: 10.1007/s10916-024-02104-9
37. Grabowski P, Petrescu G, et al. "Cyber-Physical Testbeds for Substation Protection: a pilot deployment". IEEE Internet Things J 40(2014): 476-482. DOI: 10.3389/fdgth.2026.1896184
38. Hendriksen W, Wojcik H, et al. "Cyber-Physical Testbeds for Substation Protection: a review". J Water Resour Plan Manag 42(2017): 487-494. DOI: 10.3390/diagnostics15162117
39. Ionescu F, Foscarini I, et al. "Cyber-Physical Testbeds for Substation Protection: a comparative analysis". J Constr Eng Manag 44(2020): 498-506. DOI: 10.4103/jrpp.jrpp_20_65
40. Jankowiak G, Grabowski J, et al. "Cyber-Physical Testbeds for Substation Protection: a asset-management report". Sustain Cities Soc 46(2023): 509-518. DOI: 10.3389/fdgth.2026.1763884
41. Kowalczyk N, Novotna K, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". Tunn Undergr Space Technol 8(2014): 520-530. DOI: 10.2196/48297
42. Lindqvist U, Urbanek L, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Reliab Eng Syst Saf 10(2017): 531-542. DOI: 10.1007/s00330-025-12031-z
43. Marchetti D, Doncheva M, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". Geotechnique 12(2020): 542-554. DOI: 10.3389/fdgth.2026.1699005
44. Novotna E, Eriksdottir N, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". J Clean Energy Syst 14(2023): 553-566. DOI: 10.3389/fdgth.2026.1834800
45. Ostrowski L, Lindqvist O, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". Resour Conserv Recycl 16(2014): 564-578. DOI: 10.2196/69678
46. Petrescu S, Szabo P, et al. "Cyber-Physical Testbeds for Substation Protection: a life-cycle assessment". Cem Concr Res 18(2017): 575-581. DOI: 10.7759/cureus.46454
47. Quintero B, Balogh Q, et al. "Cyber-Physical Testbeds for Substation Protection: a pilot deployment". Int J Disaster Risk Reduct 20(2020): 586-593. DOI: 10.1016/j.ssci.2025.107028
48. Ristic C, Castellani R, et al. "Cyber-Physical Testbeds for Substation Protection: a review". Energy Build 22(2023): 597-605. DOI: 10.2196/48633
49. Szabo J, Jankowiak S, et al. "Cyber-Physical Testbeds for Substation Protection: a comparative analysis". J Struct Eng 24(2014): 608-617. DOI: 10.1371/journal.pone.0305949
50. Tarasov Q, Quintero T, et al. "Cyber-Physical Testbeds for Substation Protection: a asset-management report". Struct Health Monit 26(2017): 619-629. DOI: 10.1371/journal.pdig.0000514
51. Urbanek Z, Zielinski U, et al. "Cyber-Physical Testbeds for Substation Protection: a field monitoring study". Eng Struct 28(2020): 630-641. DOI: 10.17219/acem/208596
52. Vasquez A, Alvez V, et al. "Cyber-Physical Testbeds for Substation Protection: a systematic evaluation". Autom Constr 30(2023): 641-653. DOI: 10.7759/cureus.104086

53. Wojcik H, Hendriksen W, et al. "Cyber-Physical Testbeds for Substation Protection: a laboratory study". J Infrastruct Syst 32(2014): 652-665. DOI: 10.1038/s41746-023-00852-5

54. Zielinski O, Ostrowski Z, et al. "Cyber-Physical Testbeds for Substation Protection: a case study". Constr Build Mater 34(2017): 663-677. DOI: 10.1016/j.mayocpiqo.2022.09.004

55. Andric V, Vasquez A, et al. "Cyber-Physical Testbeds for Substation Protection: a reliability analysis". Transp Res Part C 36(2020): 674-680. DOI: 10.1177/08404704241291226

Citation: Renate Sommerfeldt, Aleida Duyvendak, Velta Kaugurs. "Cyber-Physical Testbeds for Substation Protection: A Technical Note on Fault Injection Scenarios." Smart Infrastruct Innov J (2026):5; 046-054. DOI: 10.5281/zenodo.22662546