The American Journal of Interdisciplinary Innovation and Research
ISSN 2642-7478 | Open Access

Type Original Research
PAGE NO. 43-49
DOI 10.37547/tajiir/Volume07Issue10-05

Reverse-Engineering a Rooftop Solar Station in a Blackout

Oleksandr Gorbachenko
Lead Project Engineer at 60out Escape Rooms Los Angeles, California, USA

OPEN ACCESS

SUBMITTED 15 September 2025
ACCEPTED 28 September 2025
PUBLISHED 11 October 2025
VOLUME Vol.07 Issue 10 2025

CITATION
Oleksandr Gorbachenko. (2025). Reverse-Engineering a Rooftop Solar Station in a Blackout. The American Journal of Interdisciplinary Innovations and Research, 7(10), 43–49.
https://doi.org/10.37547/tajiir/Volume07Issue10-05

Abstract- The article examines the adaptive control as well as the compelled reverse engineering phenomenon of an autonomous solar power station in conditions of infrastructural and geopolitical crises precipitated by large-scale blackouts. The study stresses energy resilience is important, noting a rise in proprietary black boxes and absent documentation about safety-critical parts. Conflict along with disaster zones especially highlight this issue. In Odesa, engineers independently deconstructed an undocumented inverter protocol and developed a monitoring system to minimise life-safety risks. This occurred at a time of wartime outages so the research objective is for a systematic analysis of this case study. This work is novel in that it conceptualizes a Resilience, Vulnerability Nexus model, elucidating a paradox: reverse engineering locally for improvement of resilience inextricably links to globalizing vulnerabilities that were previously hidden within closed technologies. The principal findings show two cardinal engineering trade-offs converge, feasibility opposes rigour, trust opposes accuracy, as well as they also recognize that, under extreme constraints, immediate functionality with solution transparency supersedes technical perfection. Alternative algorithms for estimating battery state-of-charge are also assessed. The article will be of use to researchers in energy and cybersecurity, practicing engineers and policymakers, and system designers when they are developing decentralized and resilient energy systems.

Keywords: reverse engineering, infrastructure resilience, autonomous energy systems, microgrid, cybersecurity, state of charge (SoC), proprietary protocols, crisis governance

Introduction

Contemporary global infrastructure faces increasingly complex and fragile threats. Critical systems failures at a large scale are increasingly precipitated by geopolitical conflicts, extreme weather events, and cyberattacks particularly in energy systems (Qarahasanlou et al., 2025). For one countering high-impact, low-probability (HILP) events, that requires much more than customary reliability design (Panteli & Mancarella, 2017). This caused a shift of the paradigm from reliability to stability - the ability of the system to anticipate, absorb, adapt and quickly recover after destructive influences (Rosales-Asensio et al., 2022).

It was improved upon the resilience in power systems through advanced distributed energy resources (DERs). Distributed energy resources (DERs), such as rooftop photovoltaic (PV) systems, can be integrated into local microgrids. Microgrids are capable of supplying critical loads during grid outages and may operate either in parallel with the main grid or in islanded mode. Such systems particularly augment the functionality of resilience hubs—facilities that sustain essential community services during emergencies.

The path of energy autonomy toward decentralization faces more impediments. The black-box problem is a formidable obstacle along this path. Equipment ships with at least a portion of proprietary closed control. That equipment ships also with monitoring protocols that are undocumented. This is especially true of inverters and charge controllers. This erects barriers that impede interoperability and independently oversee and adapt to context-specific needs, barriers that are especially consequential when resources are constrained and technical support is absent. Details regarding implementation from vendors frequently obfuscate integration and complicate repair while also potentially introducing cybersecurity risks (Dubasi et al., 2021).

The Odesa case study in Ukraine gains relevance. Engineers had reverse-engineered a proprietary inverter to create a life-critical monitoring system during systematic blackouts in armed conflict. This instance empirically depicts that someone surmounted the black-box problem during extreme conditions. Existing academic discourse tends to frame reverse engineering either as a tool for malware analysis and vulnerability discovery or as an unfair commercial practice. The research gap lies in the paucity of studies of pragmatic, compelled reverse engineering—not as a destructive activity, but as a foundational mechanism for building resilience in active crisis zones.

The aims of this article are: (1) to systematically analyse the technical solutions devised within the Odesa case study; (2) to contextualise these solutions within formal engineering approaches and theoretical resilience models; and (3) to assess the broader implications of the approach by proposing a new conceptual model—the Resilience–Vulnerability Nexus. The structure comprises a review of materials and methods, a detailed analysis of results juxtaposed with extant theories and practices, and a conclusion articulating core findings and practical recommendations.

Materials and Methodology

The methodological basis of this work is a qualitative inquiry executed as a single-case study. This approach was selected for its capacity to furnish a deep, holistic, and context-rich understanding of a complex real-world phenomenon: the process of compelled engineering adaptation amidst crisis. Quantitative methods would not adequately capture the decision-making specificities, technical trade-offs, and tacit knowledge mobilised in the project.

The primary data source consisted of field notes and a technical project description. This document contains authentic information on motivation, challenges, system architecture, and concrete software implementations, enabling a detailed inside-out analysis of the engineering process.

To ensure theoretical depth and comparative context, a systematic review of secondary sources was conducted, selected from peer-reviewed scholarly databases (Scopus, Web of Science) and publications of leading professional organisations (IEEE, ACM, Springer). Sources were grouped into three focal strands:

1. Reverse-engineering of protocols: literature on automated and manual techniques for analysing undocumented protocols, with particular emphasis on embedded systems and industrial control systems (ICS). This corpus includes methods grounded in network-trace analysis, dynamic analysis, and heuristic approaches.

2. Battery state-of-charge (SoC) estimation: research describing established algorithms for monitoring lithium-ion batteries, including equivalent circuit models (ECMs), coulomb counting, Kalman filtering, and data-driven methods (Tao et al., 2024).

3.Critical-infrastructure resilience: theoretical frameworks defining and assessing resilience through notions such as robustness, resourcefulness, and rapid recovery, particularly as applied to energy systems and blackouts (Qarahasanlou et al., 2025).

The analytical strategy proceeded in two stages. First, a descriptive analysis was conducted to deconstruct the technical architecture, algorithms, and code fragments of the presented case. Second, an interpretive analysis juxtaposed the case's pragmatic, situational solutions with canonical principles and methodologies from the academic literature. The system's development and operation were interpreted through the theoretical lens of infrastructure resilience, wherein engineering practice itself is construed as an expression of resourcefulness and adaptation (Panteli & Mancarella, 2017).

Results and Discussion

The Odesa system epitomises engineering adaptation under conditions of extreme crisis. Its architecture was dictated not by optimisation imperatives but by existential necessity. The available components consisted of rooftop PV modules with an aggregate capacity of ≈4 kW, a lithium-ion battery pack of ~26 kWh, and an unbranded Chinese inverter. The operational context defined radical instability, characterizing it by persistent electricity and internet outages, fractured supply chains, also engaging no contractors. The key objective was for the team to create a simple monitoring system that has near-zero standby power draw, and it was able to dispatch critical alerts that included grid restoration, overload, overheating, or the presence of low battery charge.

This system must be construed as no more than just a DIY project. It must be considered a small unplanned resilience center within one large complex building. Whereas formal community microgrids are often the outcome of planned projects that power libraries, schools, or shelters (Coffey, 2025), the Odesa system exemplifies a grassroots, community-driven initiative. It provided information enabling residents to adapt their behaviour—for example, to know when elevators were operational or to rationally schedule consumption of stored energy. This directly links the case to broader discourse on the role of microgrids in post-disaster recovery (Abbey et al., 2014).

The example highlights an important distinction regarding designed resilience, which planners embed into infrastructure at the planning stage, and emergent resilience, which arises organically when people respond to a crisis. That one shows the Odesa system. It shows resilience is a dynamic process of adaptive engineering as well as not solely a static system attribute manifested at moments of greatest need.

The core technical project task involved proprietary protocol reverse engineering for data exchange through the inverter UART serial port. Lacking documentation and internet access, the engineers used a heuristic hardware and software strategy. They physically connected to the inverter's UART an ESP8266 microcontroller (MCU) salvaged from a smart light bulb, and they programmed the microcontroller as a bridge that forwards data over the local network via UDP packets. A laptop was used. A subsequent analysis of the data was done later. It included packet capture with pattern discovery and iterative hypothesis testing to decode the data-request command. The data-request command was but a variant of QPIGS and it also decoded what was the response format.

Formal methodologies rich with instruments contrast greatly with this applied method. Approaches that involve protocol analysis are of today's reverse engineering. They fall into two main categories. Network-trace analysis comes first utilizing statistical methods, clustering, and sequence-alignment algorithms for inferring field boundaries plus semantics automatically within high-volume traffic. The heuristic builder PREE is an exemplar also eases knowledge transfer from one protocol to another (Qasim et al., 2023). Dynamic analysis is the second (for example, taint analysis) and it traces firmware executable data processing, so high-fidelity reconstruction of the protocol parser's logic is enabled.

A foundational feasibility-rigour trade-off within crisis engineering is revealed through a comparison of these approaches. Formal methods do require stable environments plus substantial data volumes in addition to specialised tooling yet are undeniably more powerful as well as complete resources unavailable during any blackout. The Odesa method was less rigorous and may not have exposed every protocol nuance; nevertheless, it was realisable with on-hand means and sufficient for the critical task. This demonstrates that, in crisis conditions, the optimal solution is not necessarily the most technically elegant, but rather the one that can be deployed here and now to satisfy an immediate need. A

comparative analysis of protocol reverse-engineering methodologies is given in Table 1.

Table 1. Comparative Analysis of Protocol Reverse-Engineering Methodologies

Criterion	Heuristic Method (Case Study)	Network Trace Analysis (e.g., PREE)	Dynamic Analysis (Taint Analysis)
Required Tools	Oscilloscope/logic analyzer (optional), microcontroller, laptop	Traffic capture software, specialized analysis tools (Netzob, PREE)	Debugger, emulator, dynamic analysis tools
Necessary Conditions	Physical access to the device	Significant volume of network traffic	Access to the firmware executable
Dependence on Network	Minimal (works offline)	High (for traffic collection)	Low (offline analysis)
Reliability & Completeness	Sufficient for the specific task, may be incomplete	High, depends on traffic diversity	Very high, can reveal full parser logic
Applicability in Crisis	High	Low (due to traffic and environmental requirements)	Low (due to complexity and software requirements)

The code fragment shown in Figure 1 implements a UDP shim between the microcontroller bridge and the inverter's serial interface, providing the minimally necessary handshake and subsequent telemetry request. It relies on standard socket-API functions: a UDP socket is created, a receive timeout is configured, and the socket is bound to a local port; thereafter, the microcontroller initiates its characteristic identity-verification sequence (Are You Espressif IOT Smart Device?), followed by the construction and transmission of the principal request encoded in the dialect corresponding to the QPIGS command variant. The fixed-length reply is received and subjected to rudimentary syntactic parsing via string truncation and whitespace tokenisation, attesting to the prototype's predominantly heuristic character and its orientation toward field trials rather than parser completeness or universality.

```php
// UDP shim between our MCU bridge and the inverter's serial port
function readInverter($client, $inverter, $port, $oPort, $timeout) {
  $s = socket_create(AF_INET, SOCK_DGRAM, SOL_UDP);
  socket_set_option($s, SOL_SOCKET, SO_RCVTIMEO, ["sec"=>$timeout,"usec"=>0]);
  socket_bind($s, $client, $oPort);

  // Bind dance the MCU expects
  socket_sendto($s, "Are You Espressif IOT Smart Device?", 36, 0, $inverter, $port);

  // Main query (QPIGS variant), response holds volts/amps/temps
  $cmd = urldecode("%51%50%49%47%53%b7%a9%0d");
  socket_sendto($s, $cmd, strlen($cmd), 0, $inverter, $port);
  socket_recvfrom($s, $rx, 2048, 0, $inverter, $oPort);

  socket_close($s);
  return explode(" ", substr($rx, 1, 106)); // crude framing in field tests
}
```

Fig. 1. UDP Shim for Inverter Handshake and Telemetry Readout

Another key element of the system was a bespoke implementation for estimating the battery pack's state

of charge (SoC). Analysis of the case-study function socFromVoltage indicates that engineers favoured a custom estimate because they deliberately eschewed the inverter-reported percentage SoC. Their method of cell voltage uses a pre-specified discharge curve to guide interpolation. This solves the problem in a heuristic manner and in a straightforward way, without requiring intensive computing.

Standard SoC-estimation algorithms widely represented in the scholarly literature should be contextualized in relation to the proposed approach. Baseline methods do include coulomb counting. The battery current is integrated in time by this method. This method, despite its simplicity of implementation, is prone to drift due to measurement errors and the neglect of self-discharge (Chang, 2013). Equivalent-circuit-model (ECM) methods, representing the battery as a circuit of resistive as well as capacitive elements, afford a higher accuracy. Their drawback is in that complex parameterisation is needed, sensitive to temperature and ageing (Tao et al., 2024). The most accurate techniques are adaptive-filtering methods, such as the Kalman filter, which dynamically reconcile model predictions—e.g., from an ECM—with measured voltage and current. Their principal limitation is high computational complexity (Chang, 2013).

Juxtaposing the case's heuristic with these more elaborate algorithms surfaces a second principle of crisis engineering: the Primacy of Trustworthiness over Precision. The Odesa engineers explicitly distrusted the inverter's SoC readings—a black-box algorithm of unknown provenance and potentially dubious reliability. Their own solution, though less precise than a Kalman filter, was fully transparent, intelligible, and controllable. Where system operation bears on life support, a slightly less accurate yet predictably reliable measurement from a system one trusts is more valuable than high-precision data from an opaque device liable to fail at any moment. This choice underscores that in ad-hoc safety-critical systems, attributes such as transparency, simplicity, and operator trust may justifiably outweigh pure technical accuracy.

The code fragment in Figure 2 demonstrates a linear-interpolation function for computing the battery pack's state of charge based on the averaged single-cell voltage and an empirical percentage–voltage correspondence curve, thereby obviating reliance on the inverter's often unreliable built-in indicator. The algorithm's logic reduces to locating the bracketing points of the reference curve surrounding the present voltage and computing the position of the measured value between them by proportional division. Implemented within a minimalist software scaffold and without heavyweight frameworks, this yields robust battery metrics and actionable indicators for forecasting residual runtime and timely generation of emergency notifications.

```php
function socFromVoltage($packV, $cells, $curve /* percent=>V */) {
  $v = $packV / $cells;
  $loPct = 0; $hiPct = 100;
  foreach ($curve as $pct => $cv) {
    if ($cv <= $v && $pct > $loPct) $loPct = $pct;
    if ($cv >= $v && $pct < $hiPct) $hiPct = $pct;
  }
  if ($hiPct == $loPct) return $loPct;
  $t = ($v - $curve[$loPct]) / ($curve[$hiPct] - $curve[$loPct]);
  return $loPct + ($hiPct - $loPct) * $t; // linear between curve points
}
```

Fig. 2. State-of-Charge Estimation via Voltage Curve Interpolation

Arguably, reverse engineering in the Odesa case is an acute instantiation of resourcefulness and rapid recovery—key components of infrastructure resilience, as per theoretical models (Panteli & Mancarella, 2017). By deconstructing a proprietary system, the engineers adapted available technology to meet a critical need, thereby elevating the resilience of their local energy infrastructure amid a systemic failure of the centralised grid.

However, the process has a darker obverse. The very act of reverse engineering—and especially the publication

of results for an undocumented protocol—creates a new potential attack vector. The vulnerability lies in proprietary protocols, which often lack proper security mechanisms, such as authentication and encryption. Malicious actors, deploying the same methods as the Odesa engineers, could develop exploits to commandeer or disable analogous inverters at scale remotely (Vodapally & Ali, 2023). A coordinated attack on a large population of network-connected smart inverters could have profound implications for power-system stability (McCarthy et al., 2024).

This contradiction precipitates the central theoretical contribution of the present work—the Resilience–Vulnerability Nexus (Figure 3). The Odesa case presents a paradox: an action taken to enhance local resilience (making one's own system work) inadvertently exposes—and renders public—a systemic vulnerability (demonstrating how this class of inverters can be controlled).

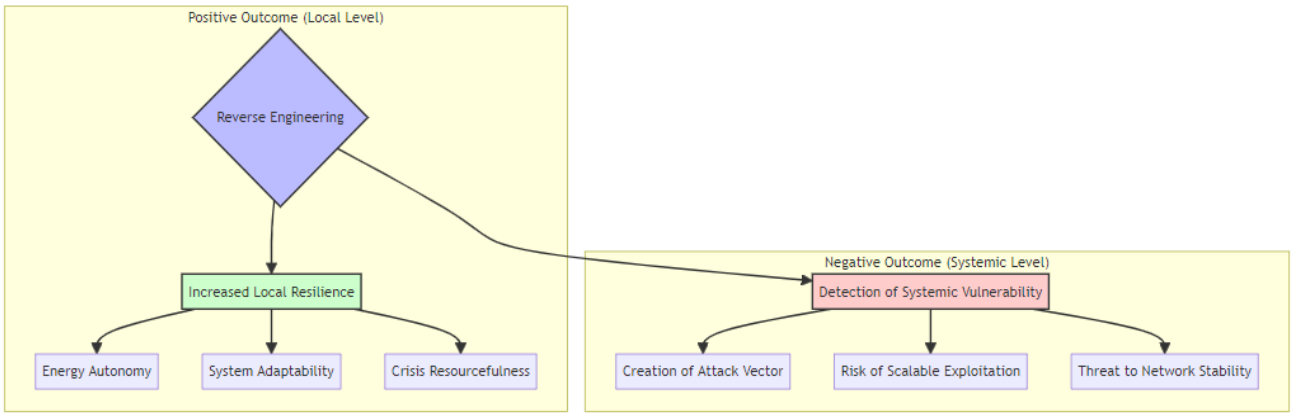

Fig. 3. Conceptual Model of the Resilience-Vulnerability Nexus

This is not a mere trade-off but a fundamental interdependence: the need for reverse engineering arises from a lack of openness (a vendor-side vulnerability), and the act of reverse engineering, while resolving a local problem, publishes a method to exploit that vulnerability on a global scale. A feedback loop thus emerges, wherein the pursuit of resilience at one network node may amplify risk across the network. This Nexus extends resilience theory by directly coupling it to cybersecurity externalities induced by the dominance of proprietary technologies in critical infrastructure.

Conclusion

Grounded in an analysis within the Odesa case study, this research shows that engineers, when compelled under crisis, can improve local resilience as a powerful instrument. As failure happens in central infrastructure the monitoring system made models showing emergent resilience. Key trade-offs surfaced for engineers under extreme constraints included analyzing realistic technical choices, reverse-engineering a proprietary protocol, and heuristically estimating SoC feasibility versus strictness and trust versus accuracy.

The principal scholarly contribution is focused on Resilience, about Vulnerability Nexus. It formulates as being the main focus. This model highlights a very fundamental paradox: actions have an aim to strengthen local autonomy and resilience when they act to deconstruct closed systems. Still, actions can unintentionally make systemic weaknesses then reveal them thereby raising danger across technology. The interplay of openness drive, security need, also adaptive practices for sure is highlighted by this dualism as critical infrastructure becomes reliant on proprietary black boxes.

Based on the analysis, several practical recommendations are presented for various stakeholders. Equipment manufacturers are strongly encouraged to transition to open standards and protocols, such as SunSpec Modbus, and to provide comprehensive technical documentation for the communication interfaces of safety-critical components, including inverters. Such an approach enlarges user capacity for integration as well as adaptation while also reducing its attendant security risks and the need for reverse engineering. Grassroots, community-oriented, and also open-source energy initiatives do require some social and policy level support. These endeavours diminish dependence on opaque commercial solutions and also elevate technological literacy, as they can foster more transparent, adaptable, and resilient local energy systems. More study about compelled engineering's security impacts should occur within research. It should also develop more lightweight, reliable, and open

monitoring and control tools tailored for resource-constrained environments.

The Odesa case demonstrates that genuine resilience is crucial now, given the growing instability. People do achieve that resilience not just by strengthening concrete and steel but also through opening code, accessing knowledge, and using human ingenuity.

References

1. Abbey, C., Cornforth, D., Hatziargyriou, N., Hirose, K., Kwasinski, A., Kyriakides, E., Platt, G., Reyes, L., & Suryanarayanan, S. (2014). Powering Through the Storm: Microgrids Operation for More Efficient Disaster Recovery. *IEEE Power and Energy Magazine*, *12*(3), 67–76. https://doi.org/10.1109/MPE.2014.2301514
2. Chang, W.-Y. (2013). The State of Charge Estimating Methods for Battery: A Review. *ISRN Applied Mathematics*, 1–7. https://doi.org/10.1155/2013/953792
3. Coffey, A. (2025, March 20). *Community Microgrids: Powering Resilience in Frontline & Disaster-Impacted Communities*. Initiative for Energy Justice. https://iejusa.org/community-microgrids-powering-resilience-in-frontline-disaster-impacted-communities/
4. Dubasi, Y., Khan, A., Li, Q., & Mantooth, A. (2021). Security Vulnerability and Mitigation in Photovoltaic Systems. *2022 IEEE 13th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 1–7. https://doi.org/10.1109/pedg51384.2021.9494252
5. McCarthy, J., Marron, J., Faatz, D., Rebori-Carretero, D., Wiltberger, J., & Urlaub, N. (2024). Cybersecurity for smart inverters: *NIST*. https://doi.org/10.6028/nist.ir.8498
6. Panteli, M., & Mancarella, P. (2017). Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events. *IEEE Systems Journal*, *11*(3), 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272
7. Qarahasanlou, A. N., Barabady, J., & Barabady, A. (2025). Unveiling the Intersection of Crisis Management and Resilience in Tackling Real-world Uncertainty in Infrastructure's Emergency Events. *Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference (ESREL SRA-E 2025)*. https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P2919-cd
8. Qasim, S. A., Jo, W., & Ahmed, I. (2023). PREE: Heuristic builder for reverse engineering of network protocols in industrial control systems. *Forensic Science International Digital Investigation*, *45*. https://doi.org/10.1016/j.fsidi.2023.301565
9. Rosales-Asensio, E., Elejalde, J.-L., Pulido-Alonso, A., & Colmenar-Santos, A. (2022). Resilience Framework, Methods, and Metrics for the Prioritization of Critical Electrical Grid Customers. *Electronics*, *11*(14). https://doi.org/10.3390/electronics11142246
10. Tao, Z., Zhao, Z., Wang, C., Huang, L., Jie, H., Li, H., Hao, Q., Zhou, Y., & See, K. Y. (2024). State of charge estimation of lithium batteries: Review for equivalent circuit model methods. *Measurement*, *236*, 115148. https://doi.org/10.1016/j.measurement.2024.115148
11. Vodapally, S. N., & Ali, M. H. (2023). Overview of Intelligent Inverters and Associated Cybersecurity Issues for a Grid-Connected Solar Photovoltaic System. *Energies*, *16*(16). https://doi.org/10.3390/en16165904