Journal of Open Innovation: Technology, Market, and Complexity 11 (2025) 100628

Contents lists available at ScienceDirect

Journal of Open Innovation: Technology, Market, and Complexity

journal homepage: www.sciencedirect.com/journal/journal-of-open-innovation-technology-market-and-complexity

Silicon safeguards: Open innovation as a shield against cyber risks

Jean-Paul Skeete [a,*], Siraj Ahmed Shaikh [b]

[a] Cardiff Business School, Cardiff University, Wales, United Kingdom
[b] Systems Security Group (SSG), Department of Computer Science, The Computational Foundry, Swansea University Bay Campus, Swansea, United Kingdom

ARTICLE INFO

Keywords:
Semiconductors
Supply Chain
Cybersecurity
Open Innovation
Sociotechnical
Systems

ABSTRACT

We live in an era where semiconductors underpin global technological infrastructures. However, the increasing complexity and cybersecurity vulnerabilities within semiconductor supply chains, exposes all technology-based industries to significant, cyber risks.This paper investigates how incumbent semiconductor fabrication plants (fabs) leverage Open Innovation (OI) within their supply chain ecosystems to enhance resilience and maintain business continuity in the face of cyber risks. Through an indepth case study of semiconductor supply chains in the United States and Europe this, research explores the collaborative dynamics between fabs and third-party suppliers focusing on their role in mitigating cybersecurity risks Our findings illustrate that third party, suppliers are identified as the most significant source of cybersecurity risks within OI frameworks. OI serves not only as a driver of technological advancement but also as a defense mechanism within the Multilevel Perspective (MLP) framework This.study emphasizes the importance of proactive collaboration supply chain transparency, and the integration of security measures across all levels of the supply.chain. By aligning with the UK's National Semiconductor Strategy and the Digital.Security by Design initiative, this research offers valuable insights for both practitioners.and policymakers on the interplay between innovation security, and resilience in the.semiconductor industry.

1. Introduction

In the last seven decades, semiconductor chips have become the cyber-physical backbone of modern society (Alsop, 2024). Semiconductors are integral to a wide range of technological infrastructures, powering everything from consumer electronics to critical systems in defence, healthcare, and telecommunications. Driven by rapid innovation and significant capital investments, the semiconductor industry has evolved into a focal point for global economic and strategic interests (Davies et al., 2024). However, the concentration of semiconductor manufacturing in specific geographical regions has amplified the industry's exposure to risks, such as geopolitical tensions, natural disasters, and other disruptions (Inagaki and Lewis, 2024).

At the core of this industry are semiconductor fabrication plants or 'fabs', which are pivotal in driving technological advancements and managing complex production processes that support the global economy. While fabs play a critical role in enabling essential technologies (Zhu et al., 2016), this reality also makes them vulnerable to cybersecurity[3] challenges[4] that threaten the integrity of the global semiconductor value chain (Datta Burton et al., 2024; Gotze, 2011; Weishäupl et al., 2018; Zhao et al., 2015). Cybersecurity at the fab level is no longer just an operational requirement, but a strategic imperative (Crouch et al., 2019), essential for protecting intellectual property, ensuring production integrity, and maintaining the continuity of global supply chains. A single cybersecurity breach in the semiconductor supply chain can trigger cascading effects, disrupting production and distribution across multiple sectors (Tomlinson et al., 2022; Ionescu et al., 2020; Khan and Estay, 2015).

Despite the growing focus on supply chain security, significant gaps remain in applied knowledge and regulatory frameworks (Datta Burton et al., 2024; Ahmad, 2020), and decision-making processes surrounding cybersecurity adoption within multi-tiered semiconductor supply chains

* Corresponding author.
E-mail addresses: skeetej@cardiff.ac.uk (J.-P. Skeete), s.a.shaikh@swansea.ac.uk (S.A. Shaikh).

[3] In this paper, cybersecurity refers to the protection of digital, operational, and physical assets within semiconductor fabrication environments and their associated global supply chain networks. This encompasses not only traditional IT security, but also the defence of Operational Technology (OT), cyber-physical systems (CPS), and embedded hardware systems critical to fab operations and semiconductor design (Tomlinson et al., 2022; Lezzi et al., 2018).

[4] Challenges in this paper is to be understood holistically as systems vulnerability, cyber threats, risks and countermeasures in industry 4.0 as laid out in the Lezzi et al (Lezzi et al., 2018). framework.

https://doi.org/10.1016/j.joitmc.2025.100628
Received 12 March 2025; Received in revised form 19 August 2025; Accepted 1 September 2025
Available online 2 September 2025

remain underdeveloped (Khan and Estay, 2015; Akter et al., 2020). While important contributions have been made to catalog fab-level cybersecurity risks—such as the threat taxonomies (Guin et al., 2014) and sector-specific analyses (Areno, 2025)—there remains a gap in understanding how these risks are managed strategically across global semiconductor supply chains. In particular, few studies explore how fabs collaborate with third-party suppliers to mitigate these threats using Open Innovation[5] frameworks or how these dynamics align with broader socio-technical transitions (Tomlinson et al., 2022).

This paper attends to these gaps by examining how semiconductor fabs leverage Open Innovation (OI) within their supply chain ecosystems to mitigate cybersecurity risks and reinforce resilience. We define resilience as the capability of a system to prepare for, absorb, recover from, and adapt to adverse events and disruptions, in line with the widely adopted definition by the National Academy of Sciences (National Research Council, 2012). In the context of semiconductor manufacturing, resilience refers to the ability of fabs and their supply chain partners to maintain operational continuity and protect core functions—despite cyber threats, technological shocks, or supplier disruptions (Ponomarov and Holcomb, 2009).

Guided by the UK's National Semiconductor Strategy (DSIT, 2024) and the Digital Security by Design (DSbD) initiative (DSbD, 2024), this research explores how collaborative efforts between fabs and third-party suppliers protect against disruptions and contribute to business continuity in the face of evolving cyber threats. More specifically, this paper seeks to answer the following:

- RQ1: How do incumbent semiconductor fabs leverage Open Innovation within their supply chain ecosystem to enhance resilience and business continuity in the face of cyber risks?
- RQ2: How can the findings from RQ1 be interpreted to explain the role of collaboration between semiconductor fabs and third-party suppliers in mitigating cyber risks within the Multilevel Perspective (MLP) framework?

Section 2 of this paper provides a focused overview of the semiconductor fabrication process, the role of cybersecurity in the industry, and the theoretical framing of fabs as 'regime actors' (Bergek et al., 2013; Skeete, 2019) within a multi-level socio-technical system (Geels and Kemp, 2012). Section 3 outlines our case study methodology and processes, presented within the CASET case study template framework (Goffin et al., 2019). Section 4 presents the empirical findings in response to RQ1, derived from a thematic analysis (Braun and Clarke, 2012) of coded data collected from the study's respondents. Section 5 addresses RQ2 by interpreting these findings through the lens of the MLP framework, highlighting the theoretical implications and exploring additional nuanced issues that have emerged. Finally, Section 6 offers concluding remarks, practical recommendations for industry stakeholders and policymakers, and acknowledges the limitations of this study's contributions.

While cybersecurity is a broad and evolving field, our focus lies in the industrial and supply chain dimensions of cybersecurity within the semiconductor sector. Specifically, we examine how fabs and their ecosystem partners manage cyber risks that threaten production continuity, intellectual property, and hardware-level integrity — extending beyond IT to include Operational Technologies (OT), Cyber-Physical Systems (CPS), and hardware security concerns.

[5] While this journal is rooted in Open Innovation thinking (Chesbrough, 2003), it is worth distinguishing OI from other innovation modes. Unlike closed innovation (in-house R&D) (Herzog and Leker, 2010), user innovation (von Hippel, 2005), or open-source collaboration (Johnson, 2006), OI strategically combines external knowledge flows with firm-level control. It is particularly suited to industries like semiconductors, where speed, complexity, and IP sensitivity demand both collaboration and coordination.

This study makes the following contributions to data-enabled Open Innovation (Lotfi et al., 2024):

- Empirically investigates how incumbent semiconductor fabs use Open Innovation to mitigate cyber risks across complex global supply chains.
- Extends the MLP by integrating cybersecurity and supplier collaboration into regime-level dynamics.
- Conceptually reframes Open Innovation as a strategic mechanism for resilience, not just growth.
- Offers practical insights for improving supply chain cybersecurity through trust-building, traceability, and joint standards.

2. Industry background: semiconductor fabrication supply chains and vulnerabilities

This literature review is not intended to define a narrow research gap in the conventional deductive sense. Instead, consistent with the exploratory and abductive nature of this study (detailed in Section 3), it provides contextual grounding by mapping the intersections of semiconductor manufacturing, open innovation, and cyber risk. This framing aligns with the aims of the commissioned project, which sought to surface insights rather than test pre-specified hypotheses.

The semiconductor fabrication supply chain is comprised of several stages, each integral to the production of semiconductor chips (Hurtarte et al., 2007). Fig. 1 summarizes these stages in a manner that conveys the logistical flow of materials and components, while highlighting potential cybersecurity threats that can compromise the supply chain at each phase. Segmenting these vulnerabilities helps to foster more informed discussions throughout this paper with regards to securing semiconductor supply chains (Rostami et al., 2013).

The vulnerabilities outlined in Fig. 1 do not exist in isolation; they create cascading effects that ripple across the entire semiconductor ecosystem. Security breaches at any stage in the supply chain can disrupt industry-wide collaborations by eroding trust between partners and stalling joint ventures. These disruptions can also delay innovation cycles, as companies may hesitate to share intellectual property or collaborate on new designs due to heightened cybersecurity risks. Moreover, given the geopolitical significance of the semiconductor industry, any compromise in the supply chain has the potential to destabilize global markets and strategic alliances (Melnyk et al., 2022). These cascading impacts illustrate the urgent need for robust cybersecurity measures throughout the semiconductor manufacturing supply chain.

2.1. The evolution of cybersecurity in semiconductor supply chains

The semiconductor industry's approach to supply chain cybersecurity has evolved significantly, driven by the pressing need to address vulnerabilities and enhance security measures within the globalized supply chain ecosystem (Zhao et al., 2015). This evolution responds to the increasing cyber risks inherent in the complex, interconnected nature of semiconductor manufacturing, particularly where hardware-based cybersecurity threats are concerned (Rostami et al., 2013). As laid out in the cybersecurity reference framework developed by Lezzi et al. (2018), efforts to mitigate these risks include the exclusive procurement of materials from trusted vendors and the isolation of critical infrastructure from external networks (Latif et al., 2021). However, despite these efforts, the increasing digitization of supply chain processes—integrating industrial control systems (ICS) and cyber-physical systems (CPS)—has further exacerbated the potential for cyber risks, introducing new attack vectors (Khan and Estay, 2015).

To address these evolving risks, semiconductor fabs have proposed decision-making strategies such as scenario planning and portfolio analysis to enhance resilience against cyber-attacks (Collier and Sarkis, 2021). Moreover, the integration of embedded security measures at the hardware (chip) level has been explored to safeguard systems from both

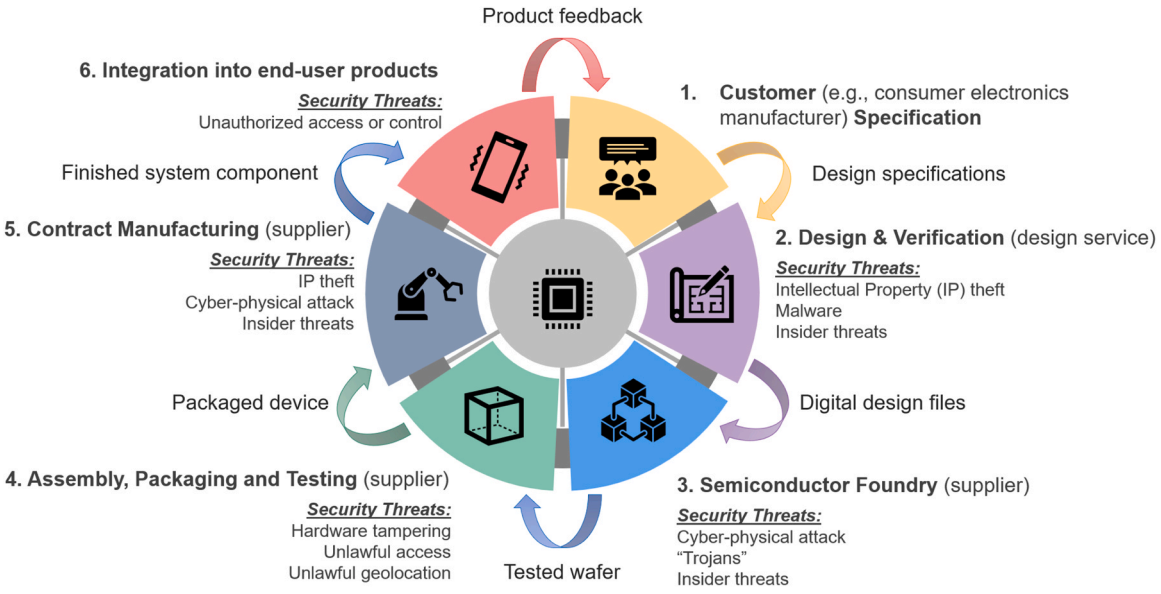

Fig. 1. Semiconductor supply chain showing segmented inputs, outputs and cybersecurity. Adapted from Duffield (Duffield, 2024).

targeted and non-targeted cyber threats (Tomlinson et al., 2022), reinforcing the multi-layered security approach recommended in cybersecurity frameworks (Lezzi et al., 2018). As digital and electronic technologies become increasingly embedded within supply chains, the range of potential cyber risks has expanded, necessitating comprehensive risk management strategies (Hammi et al., 2023).

In this context, blockchain technology has emerged as a potential tool for enhancing the supply chain visibility, providing robust mechanisms for securing transactions and ensuring the authenticity of information flows (Xu et al., 2019). Cybersecurity models (Lezzi et al., 2018) have also been applied to assess the security and trustworthiness of supply chain operations, offering deeper insights into the dynamics of cyber risks and guiding more effective mitigation efforts (Boyes, 2015).

2.2. *Theoretical framing: the semiconductor industry as a sociotechnical regime*

In the context of semiconductor manufacturing, innovation arises from a complex interdependence between design firms and foundries. While fabless firms typically lead product and architectural innovation, foundries such as the Taiwan Semiconductor Manufacturing Company (TSMC) and Global Foundries drive cutting-edge process innovations—in areas like advanced lithography, materials science, and yield optimization. These process innovations are critical enablers for realizing next-generation chip designs and are therefore foundational to the industry's innovation trajectory (Bergek et al., 2013). We situate our case study within the analytical framework of the MLP (Geels and Kemp, 2012), and label semiconductor foundries as incumbent 'regime actors' embedded within and reliant upon complex, globally distributed supply chains. The case study approach is appropriate here as it enables an in-depth exploration of complex socio-technical dynamics within their real-world context (Gephart, 2004; Pratt, 2008), capturing how semiconductor fabs and their supply chain partners respond to and manage cyber risks.

Classic economic literature characterizes innovation as a series of gradual, evolutionary improvements (Schumpeter, 1947), however, there is a growing focus on the interplay between creativity and the process of innovation accumulation. Creativity involves devising solutions that extend beyond the scope of the organization's current methodologies, often resulting in technological enhancements in efficiency, functionality, or quality compared to former versions (Geels et al., 2016). In contrast, accumulation involves the generation of knowledge that builds upon and extends existing methodologies, rather than rendering them redundant (Geels, 2011).

This leads us to the notion of 'creative accumulation' – developed by Bergek et al. (2013) – a concept Geels et al. (2016), refer to as the 'transformation pathway', and what other streams of business scholarship might call 'open innovation' (Chesbrough, 2003). Scholars have studied this phenomenon in various capital complex goods industries such as automobile manufacturing (Skeete, 2019), and demonstrated how Original Equipment Manufacturers (OEMs) are able to expand their competencies and maintain a competitive edge though OI with their network of suppliers.

Similarly, semiconductor manufacturers that engage in creative accumulation, must strike a balance between in-depth knowledge of individual components and a comprehensive understanding of overall systems architecture. This presents the continuous challenge of integrating and leveraging both established and new knowledge (Bergek et al., 2013). Creative accumulation underscores the importance of rapid development, technological exploration, and the assimilation of new skills. By integrating the dynamics of creative accumulation, incumbent semiconductor firms like TSMC sustain their competitive advantage in terms of knowledge assets and speed of innovation (Davies et al., 2024). Fig. 2 illustrates semiconductor fab industry within the MLP.

Previous research (Feldman, 2025) has also found the semiconductor industry to be characterized by a paradoxical relationship between innovation and imitation, where firms must share valuable intellectual property across a web of suppliers, even as the risk of IP theft and opportunism remains high. This tension is particularly acute in Open Innovation contexts, where collaboration is essential for technological advancement but exposes firms to strategic vulnerabilities.

The fabless-foundry division of labor exemplifies a regime-level structure in which innovation responsibilities are distributed: design firms lead product evolution, while foundries innovate in process and manufacturing scalability. Our MLP framing reflects this dual dynamic, situating fabs as regime actors whose innovations are not always visible to the consumer but are critical to sustaining the trajectory of Moore's Law (Schaller, 1997) and enabling system-wide resilience. The MLP framework is therefore particularly suitable for examining cyber risks in the semiconductor industry, as it allows us to capture not only technological vulnerabilities but also the institutional, organizational, and ecosystem-level dynamics that shape how such risks emerge and are managed.

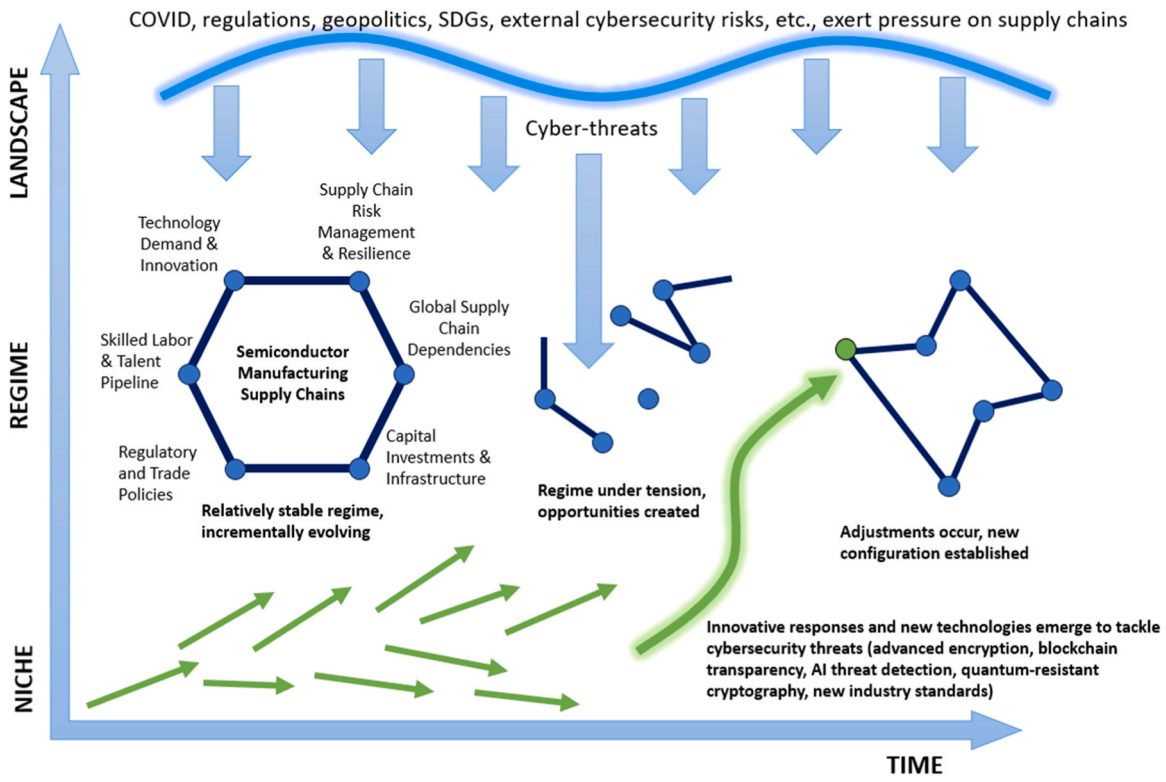

Fig. 2. MLP of the semiconductor industry, adapted from Geels and Kemp (Geels and Kemp, 2012).

3. Methodology

The methodological design of this study is inspired by van de Ven (de Ven, 2007) and follows an engaged scholarship-based case study approach aimed at bridging the theory-practice gap by integrating collaborative problem-solving with data-driven research (Guertler et al., 2020; Maestrini et al., 2016). This approach is well-suited for addressing real-world challenges in organizational and industrial settings (Touboulic and Walker, 2016; Wieland et al., 2023), as it balances solving practical problems with advancing academic knowledge (Dick, 2014; Lim et al., 2017; Sundarakani et al., 2021).

As the field of innovation management evolves, exploratory, theory-building research becomes essential, and high-quality case studies are widely regarded as effective for such inquiries (Gephart, 2004; Pratt, 2008). This study employs the Case Study Evaluation Template (CASET), which structures the research around four key categories: research design, data collection, data analysis, and post hoc reflection on rigor, ensuring alignment with the key stages of robust case study methodology (Goffin et al., 2019). Table 1 is our own CASET report and Fig. 3 illustrates the core framework of the case study.

Knowledge-Value co-creation: This recursive, central step facilitates monitoring and prioritizes the collaborative creation of knowledge for the mutual advancement of theory and practice, underscoring the 'centrifugal' benefits and connections across all phases of the research cycle (Guertler et al., 2020).

3.1. Case context and scope

This study adopts an industry-level case design, focusing on the global semiconductor supply chain with particular emphasis on the United States and Europe. Access to participants was facilitated by SEMI (the global semiconductor industry association, semi.org), which allowed the research team to engage directly with stakeholders at two flagship international events: SEMICON West 2023 (San Francisco) and SEMICON Europa 2023 (Munich). At SEMICON West, we recruited delegates and members from leading multinational semiconductor firms, industry suppliers, and cybersecurity experts. At SEMICON Europa, SEMI facilitated three invitation-only workshops designed and run by the research team, ensuring broad yet targeted representation of the sector's key actors.

Rather than centering the case on a single organization, this design reflects the structure of the semiconductor industry itself: a globally interconnected ecosystem where supply chains, manufacturing, and cybersecurity challenges transcend firm and jurisdictional boundaries. The companies and professionals represented in our study are leaders in semiconductor manufacturing, design, equipment provision, and standards development, with all respondents working for multinational firms active across multiple regions. Framing the case study at this industry level allows us to capture systemic issues and collaborative dynamics more effectively than a firm-specific focus would.

3.2. Participant recruitment

Building on this case framing, participant recruitment was conducted in two sequential phases during 2023.

Phase 1 – United States: We carried out in-person, semi-structured interviews and a follow-up panel discussion with eight senior professionals in the semiconductor and cybersecurity sectors. Recruitment leveraged SEMI's industry networks and professional associations to ensure participation from decision-makers in roles spanning policy advisement, executive management, research, and information security.

Phase 2 – Europe: We organized three in-person focus groups with thirteen stakeholders during SEMICON Europa 2023. SEMI facilitated access to participants, and the research team curated invitations to ensure a diverse mix of perspectives. These workshops also served as structured validation sessions, where findings from Phase 1 were reviewed and refined.

In both phases, participation was not limited to specific firms but represented a broad cross-section of the semiconductor ecosystem. All participants were screened to confirm their involvement in supply chain

Table 1
Case study evaluation template (CASET) overview.

Evaluation criteria	Application in this study
Theoretical foundation	We adopted an abductive approach (Bell et al., 2022) combining our expertise in technology supply chains with key insights from the open innovation literature.
Pilot study	Although we did not conduct a formal pilot study, the iterative rounds of data collection and analysis (as shown in Figure 3) enabled us to refine our research protocols recursively.
Theoretical sampling	We employed non-probability sampling to selectively include key institutional actors (Tansey, 2007). While this approach may introduce selection bias and limit generalizability, the respondents, representing competing multinational firms, provided perspectives that extended beyond national borders.
Triangulation	The competing interests of respondents (e.g., policy versus commercial) and multiple modes of primary data collection supported evidence triangulation, strengthening the validity of the findings (Creswell, 2015). To further contextualize respondents' insights into the rapidly evolving global semiconductor landscape, we also used secondary sources such as industry reports, government documents, reputable business news, and academic journals.
Review and validation of evidence	We validated our evidence through feedback sessions with project participants and interviewees. In addition, the second researcher—who was independent from Phase 1 data collection in the USA—facilitated the Phase 2 workshops in Europe, where Phase 1 findings were tested and refined through multiple rounds of respondent feedback. This staged involvement ensured both external perspective and methodological rigor, consistent with CASET validation guidelines (Goffin et al., 2019).
Transparency of data collection	Interviews were in-person and semi-structured, focusing on interviewees' perspectives on cybersecurity within the semiconductor industry. All interviews were digitally recorded and transcribed verbatim. The interview protocol is available upon request. Our in-person stakeholder workshops were conducted under 'Chatham House Rule,' shorthand notes were taken.
Inter-coder agreement	After the initial coding, cross-analysis of workshops and interviews refined the codes into major themes (Fereday and Muir-Cochrane, 2006; Vaismoradi et al., 2016; Maguire and Delahunt, 2024) and two independent researchers coded each dataset (King, 2016).
Case presentation	We clearly demonstrate how the empirical data led to our findings by providing a 'trail of evidence' through ample quotes in the results section, along with a visual illustration that synthesizes and summarizes our results (Moschko et al., 2023).
Case interpretation	We moved beyond descriptive analysis by rigorously engaging with sociotechnical and innovation literature, systematically aligning empirical findings with the MLP. Through iterative cycles of refinement and theoretical reflection, we identified key tension points shaping our results. These critical insights are visually represented in Figure 5, offering a clear synthesis of the conceptual outcomes from our analysis.
Reflection on validity and reliability	We address validity and reliability throughout the Methodology section to demonstrate the rigor of our qualitative approach and discuss issues with generalizability in the Limitations section of paper.

cybersecurity at a regime level, ensuring the data reflected sector-wide issues rather than narrow organizational contexts.

3.3. Ecosystem representation and interviewee profile

We strived for an effective representation drawn from stakeholders across the ecosystem. Participants are professionals working at organizations ranging from leading multinational corporations to specialized firms, providing a diverse range of perspectives. We have categorized the participants into distinct stakeholder groups and assigned new participant codes to ensure confidentiality. Below is an overview of each category, including an indication of the operational context and sectoral focus.

Manufacturing and Design [PMD1–PMD8]: This group comprises senior security officers, automation and analytics developers, and leadership from major semiconductor manufacturing companies and design firms. Their expertise spans semiconductor fabrication, cybersecurity practices in manufacturing environments, and technological innovations.

- PMD1: Senior Security Officer at a leading global semiconductor company.
- PMD2: Senior Security Officer at an international semiconductor manufacturing firm.
- PMD3: Senior Security Officer at a prominent semiconductor equipment supplier.
- PMD4: Leadership at a key supplier of semiconductor manufacturing equipment.
- PMD5: Senior Security Officer at a major semiconductor process technology company.
- PMD6: Senior Security Officer at an advanced photolithography systems manufacturer.
- PMD7: Senior Automation/Analytics Developer at a top semiconductor corporation.
- PMD8: Leadership at a significant player in semiconductor equipment and services.

Policy and Standards [PPS1–PPS3]: Participants in this category are senior advisors and leadership figures from national institutes and standard-setting organizations. They provide policy-oriented perspectives on cybersecurity standards, regulations, and their impact on the semiconductor supply chain.

- PPS1: Senior Advisor at a national standards and technology institute.
- PPS2: Leadership at a consulting firm specializing in semiconductor industry strategies.
- PPS3: Leadership at an international consultancy with expertise in technology and innovation.

Systems Integration and End Users [PSI1–PSI5]: This group includes managers, development leaders, engineers, and leadership from major automotive, electronics, and technology companies. Their focus is on integrating semiconductor components into complex systems and products, highlighting security considerations from an end-user and systems integration perspective.

- PSI1: Manager at a leading automotive consulting firm.
- PSI2: Development Leadership at a major automotive manufacturer.
- PSI3: Engineer at a global technology company specializing in industrial automation.
- PSI4: Leadership at a multinational semiconductor and telecommunications equipment company.
- PSI5: Leadership at a company specializing in secure connectivity solutions.

Consulting and Research [PCR1–PCR5]: This diverse group comprises leadership from cybersecurity firms, research institutions, and specialized consulting companies. Their roles involve advancing cybersecurity research, advising on best practices, and developing strategic solutions to emerging threats in the semiconductor supply chain.

- PCR1: Leadership at a cybersecurity research and consulting firm.
- PCR2: Leadership at a high-tech materials company specializing in semiconductor substrates.

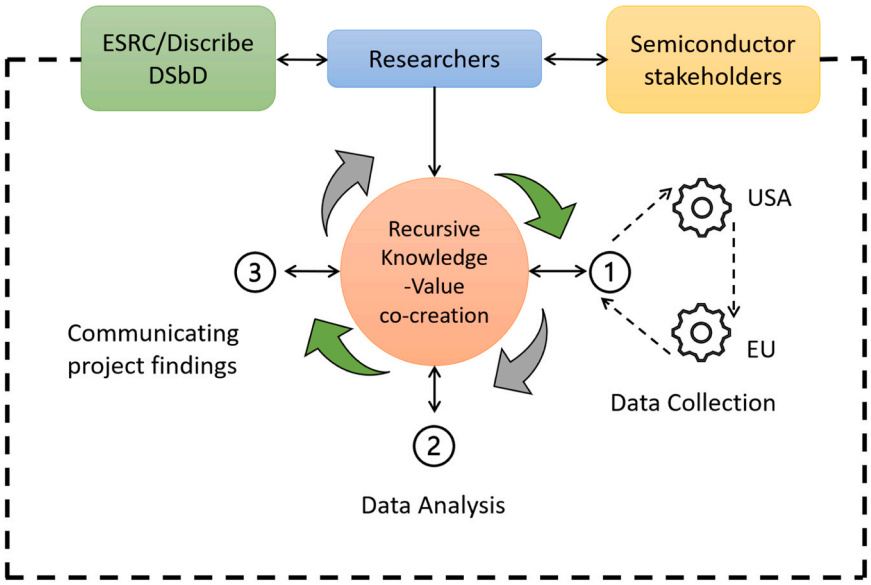

Fig. 3. Case study framework adapted from Guertler et al. (2020)., and Maestrini et al. (2016).

- PCR3: Leadership at a renowned research institute focused on integrated circuits and systems.
- PCR4: Senior Science Officer at a company specializing in secure communication technologies.
- PCR5: Leadership at a firm providing advanced connectivity solutions.

The study aimed to ensure diversity among the participants, considering attributes such as age, gender, race, disability, religion, and sexual identity. Participants were based primarily in the U.S. and Europe, holding positions ranging from C-level executives (including CEOs, CTOs, CISOs and Chief Engineers) to senior roles such as project managers, technical leads, and senior consultants. This diverse representation provided a well-rounded view of semiconductor supply chain cybersecurity from various operational and strategic perspectives.

While this study does not seek to quantify consensus, indicative frequency labels are used in reporting findings to convey the relative prevalence of themes across participants. In this paper, most refers to 10 or more participants, several refers to 4–9 participants, and a few refers to 1–3 participants. These terms are applied throughout the findings (Table 2) to provide additional transparency regarding patterns in the data.

4. Findings

The findings presented below draw on perspectives from 21 participants representing semiconductor fabs, third-party suppliers, and industry experts (see Section 3.2). Participants held senior technical, managerial, and security-related roles, with professional experience ranging from 7 to 25 years in the semiconductor ecosystem.

Research Question 1 (RQ1) – *How do incumbent semiconductor fabs leverage Open Innovation within their supply chain ecosystem to enhance resilience and business continuity in the face of cyber risks?* – is addressed through our empirical data analysis. Our coded data reveals key insights, which we have categorized into distinct themes, emerging from our thematic analysis samples in Table 2**.** These themes provide a structured understanding of how Open Innovation practices contribute to mitigating cyber risks and ensuring operational continuity within the semiconductor industry.

The themes around challenges underscore the ongoing tension between maintaining manufacturing efficiency and implementing effective cybersecurity measures within semiconductor fabs. Participants highlighted the critical need for solutions that provide robust security without disrupting production schedules. Additionally, the integration and implementation of new technologies continue to present significant barriers to achieving comprehensive cybersecurity in semiconductor manufacturing.

5. Discussion

This section addresses Research Question 2 (RQ2): *How can the findings from RQ1 be interpreted to explain the role of collaboration between semiconductor fabs and third-party suppliers in mitigating cyber risks within the MLP framework?* While RQ1 was examined empirically in Section 4, RQ2 requires an interpretive analysis. Accordingly, we integrate the empirical findings with targeted references to relevant literature and the MLP framing, drawing on interviewee insights and illustrative industry examples to explain how collaborative mechanisms across the supply chain reinforce resilience—particularly at the regime and niche levels. The core cybersecurity challenges are summarized in Table 2 and visualized in Fig. 4; in what follows, we discuss these challenges across the landscape, regime, and niche layers of the MLP rather than under a single "challenges" heading. The section concludes by synthesising these analyses into a bespoke MLP-informed representation of the semiconductor supply chain.

In the findings section, we addressed RQ1 by identifying several challenges that incumbent semiconductor fabs face when leveraging Open Innovation (OI) within their supply chain ecosystems, as well as opportunities to enhance resilience and ensure business continuity in the face of cyber risks. The main headline from our findings is that exposure to third-party/supplier cybersecurity risks is the primary concern of large technology firms engaging in open innovation. Fig. 4. highlights how these risks permeate all phases of the semiconductor supply chain lifecycle.

Our findings emphasize that addressing third-party risks requires systematic changes (Geels and Kemp, 2012) across all levels of the MLP framework. Specifically, targeted governance mechanisms are critical for mitigating these risks. For instance, establishing mandatory supplier audits and enforcing supply chain transparency can significantly reduce vulnerabilities introduced by lower-tier suppliers. Additionally, fostering pre-competitive collaboration among industry players to develop shared cybersecurity standards could address gaps in compliance and risk assessment. By framing third-party risks as central to the regime-level dynamics of OI, this study underscores the need for

Table 2
Description of emerging themes.

Core Theme	Description	
Security Challenges in Semiconductor OI	While Open Innovation drives technological advancements in the semiconductor industry, it also introduces significant security risks, particularly in protecting intellectual property and managing vulnerabilities across complex, global supply chains.	
Subtheme	***Description***	***Representative Quotes***
Industry-specific challenges – **A FEW**	The semiconductor industry's dependence on intellectual property (IP) sharing and Operational Technologies (OT) creates distinct security vulnerabilities, requiring the implementation of robust cybersecurity measures.	"In most other industries, we don't share IP; we sell it in the form of a finished product. The semiconductor industry shares IP to collectively come up with a finished product." – PCR1 "From an IT standpoint we are all the same regardless of industry. Same challenges, organizational inertia, history etc. It's the OT space where it starts to get unique. [OT] has to be resilient coming through the door and has to stay that way for 10 years. The threat won't come in the front door, everybody's got that figured out. It's the back door that's the problem." – PMD3
Supply Chain Visibility and Monitoring - **MOST**	Supply chain visibility and monitoring present significant challenges, as inadequate oversight of suppliers can lead to severe cybersecurity risks, emphasizing the need for comprehensive transparency and control.	"A lot of the risks come down to vendor and supply chain issues. [Industry leaders] have found that 66–90 % of severe cybersecurity incidents related to the supply chain, and thus a supplier problem becomes a manufacturer problem. Therefore, transparency along the supply chain when there is an incident is important." – PMD5 "Visibility & monitoring across your supply chain or ecosystem is everything, because without those you will start getting phone calls from 'three-letter agencies' saying you have a problem, and you don't want to be there." – PSI2
Risks from Lower-Tier Suppliers - **SEVERAL**	Limited visibility and control over tier 2 and tier 3 suppliers introduce significant security risks, as vulnerabilities in these lower tiers can propagate through the entire supply chain.	"In many cases, companies do not know who their tier 2 or tier 3 suppliers are, and this is often kept confidential by design; however, [these] suppliers can create problem[s]." – PCR2 "You might be surprised at how much third-party stuff you are using. Who are your suppliers? If there is a vulnerability, when are you going to patch it? How quickly can you patch it? Are you going to patch it?" – PMD4
Technology Integration and Implementation - **SEVERAL**	Integrating cybersecurity measures without compromising manufacturing efficiency presents a significant challenge, underscoring the importance of designing security into systems from the outset as well as the IT/OT dichotomy.	"They face legacy install-base challenges in several thousand tools of production. Now what happens when it's time for a software upgrade in the fab? What is the risk of interfering with tool performance? How much downtime are we going to suffer to do that upgrade? Is that change so significant, we have to re-qualify this tool? Taking it out of production for even longer." – PMD1 "Security cannot be considered after the fact and must be 'designed in'. How do we patch software in the field with zero downtime? You cannot take tens or even hundreds of millions of dollars of equipment out of production for an hour for a patch. Needs to be quick, and if it does not work, it needs to be able to revert to the older patch." – PMD6 "OT Security on the facility side, e.g, bulk gases in the foundry. If the supply is disabled, it shuts down the entire [fab] in 10 min. Also, the difference between IT security and OT security despite having similar protocols, in IT security you have instant response, you can isolate the host immediately via network segmentation. But with OT security, you cannot auto-block a lot of situations." – PMD2
CORE THEME	**DESCRIPTION**	
Enhancing Security through Collaborative Open Innovation	Fabs are strengthening security through OI by enhancing supply chain visibility, implementing rigorous supplier assessments, and integrating advanced security technologies, fostering resilience while maintaining innovation and competitiveness.	
Subtheme	***Description***	***Representative Quotes***
Improving Supply Chain Visibility and Risk Monitoring - **MOST**	Enhancing Supply Chain Visibility and Monitoring is a key desired outcome, as participants stressed its vital role in strengthening cybersecurity within the semiconductor industry. With complex, globalized supply chains, manufacturers must maintain a comprehensive	"Here is a good exercise for manufacturers' leadership: Exactly where are my suppliers integrated into my processes? This is not meant to seek out vulnerability, but just to map suppliers to processes in an honest assessment." – PMD7

(*continued on next page*)

Table 2 (*continued*)

Core Theme	Description	
	understanding of supplier integration to effectively manage and mitigate risks.	
		"Finished product security is important. People want to know who made it, they want a transparent supply chain, which factory, what wafer, who touched it during testing and fitment." – PSI3
Supplier Assessment and Compliance - **SEVERAL**	Implementing rigorous, pre-competitive evaluation processes, including third-party assessments and increased compliance demands.	"SEMI 187 is prescriptive for the OEM, giving guidelines they must follow. One of those guidelines is 'don't ship unsupported operating systems.' But there are gaps in the standards. For example, what happens when a supported operating system loses that support two weeks later, or in 6 months—is that okay? The standard does not address this. Industry-wide standards would help here. Homogeneity." – PCR4
		"Your [tier 2 and 3 suppliers'] technology will be secure, it will be scrutinized, and if it's not…the consequences can be dire." – PMD7
		"Come together as an industry, get better together, work on standards in a pre-competitive environment, as an industry avoiding a situation where others (regulators) tell us how to behave." – PMD4
Security Strategies and Technologies - **SEVERAL**	Employing layered defence strategies and advanced technologies to bolster cybersecurity	"What is the organization's software bill of materials? Those will be scanned against known vulnerabilities. Scan third-party libraries and their own libraries. And the reports that result from scanning are then triaged." – PCR3
		"Manufacturing supply chain traceability through blockchain. How do we take the blockchain tool and try and build supply chain traceability through that?" – PSI5

industry-wide coordination to implement robust cybersecurity measures effectively.

5.1. Socio-technical landscapes

At the landscape level, our findings reveal several broad, external factors are shaping the industry's approach to cybersecurity. The rise in both the prevalence and sophistication of cyberattacks—particularly from nation-states and well-funded hacker groups—has placed increasing pressure on the industry to strengthen its security measures. These advanced threats elevate the cybersecurity landscape to unprecedented levels, requiring robust defenses against organized threat actors and zero-day vulnerabilities.[6]

Simultaneously, heightened regulatory scrutiny and the potential for intervention by authorities such as "three-letter agencies" are driving the need for improved visibility and compliance across the supply chain. Regulations and standards like the UNECE WP.29 Regulation No. 155 and ISO/IEC 27001 are influencing operations and cybersecurity strategies, emphasizing the importance of adhering to international standards.

We also saw that globalization and the increasing complexity of supply chains introduce further challenges. Companies often have limited knowledge of their tier 2 and tier 3 suppliers, who are frequently shrouded in confidentiality by design. These lower-tier suppliers hold the potential to introduce significant disruptions, as evidenced by incidents like the MOVEit[7] file transfer software breach, which caused widespread disruption unbeknownst to some manufacturers. The financial repercussions of third-party cybersecurity assessments and audits are also becoming increasingly apparent, influencing factors such as insurance premiums and loan rates. For large incumbent firms, even minor fluctuations in interest rates can translate into substantial financial burdens.

Finally, the convergence of Information Technology (IT) and Operational Technology (OT) systems stood out as a significant landscape-level challenge. Historically, IT and OT systems have evolved along distinct trajectories, each with its own set of priorities, protocols, and practices. However, modern cybersecurity threats do not respect these boundaries. The integration of IT and OT systems, driven by the digital transformation within manufacturing, necessitates a new paradigm of collaboration and understanding. This convergence is crucial not only for operational efficiency but also for the industry's ability to withstand and respond to cybersecurity threats.

These factors collectively underscore the imperative for strategic oversight, transparency (Dalal et al., 2024; Singh et al., 2024), and collaboration to navigate future disruption risks in the semiconductor industry's complex global supply chains (Sodhi and Tang, 2019).

5.2. Socio-technical regimes

At the regime level, we found established industry norms, standards, and collaborative efforts played a crucial role in shaping cybersecurity practices within the semiconductor industry. Manufacturers and suppliers are increasingly aligning with national and international cybersecurity organizations, standards and regulations, such as NIST, ISO/IEC 27001, UNECE WP.29 Regulation No. 155, and SEMI 187 and 188, which provide common frameworks for security measures. The industry's desire for homogeneous standards underscores a collective effort to ensure a unified approach to cybersecurity, aiming to pre-empt external regulation through "pre-competitive" collaboration, which was a term often used.

Stakeholders also described an intricate web of challenges and imperatives that define their cybersecurity landscape. Central to their concerns is the increasing complexity of supply chains—a phenomenon

[6] A zero-day cybersecurity risk involves a software vulnerability that is unknown to those who would be interested in mitigating the vulnerability, including the software vendor. This type of risk is particularly dangerous because it allows hackers to exploit the flaw before developers have an opportunity to create and distribute a fix, potentially leading to unauthorized access and significant damage.

[7] The MOVEit cybersecurity breach was a significant incident impacting a widely used file-transfer service, trusted across various industries for its compliance with regulatory standards. This breach has notably affected major financial institutions, law firms, insurance companies, healthcare providers, education services, and government agencies, highlighting vulnerabilities in critical data transfer infrastructures.

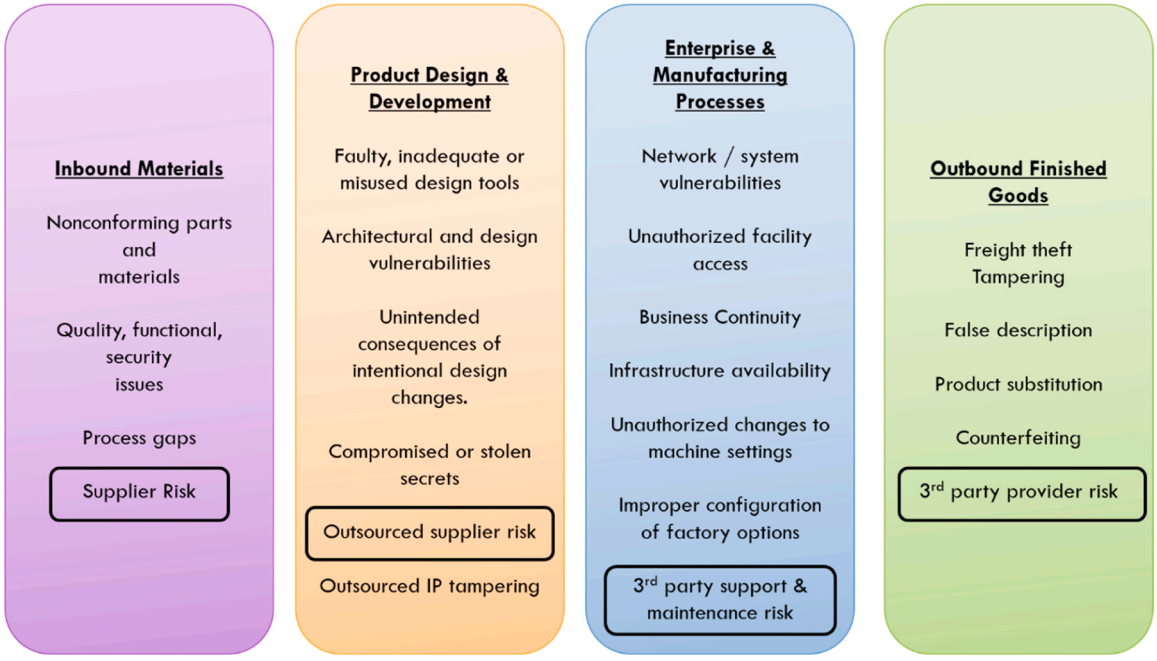

Fig. 4. Semiconductor supply chain lifecycle risks (adapted from respondents, unpublished).

that shows no signs of abating. The preference within the industry for cultivating long-term relationships with suppliers reflects the depth of integration required for sophisticated supply chains. However, this preference poses challenges when juxtaposed with the imperative for supplier diversification—a strategy increasingly advocated for in the realm of cybersecurity risk management and supply chain resilience (Chen et al., 2025; Junaid et al., 2023).

A pivotal theme that emerged is the difficult task of diversifying suppliers, particularly those that are currently "single source" and may be indispensable yet pose significant risks. The geography and context of supply chains sometimes make it infeasible to move away from such suppliers. Larger firms, with their vast network of suppliers, face a paradox of scale; while not all suppliers wield equal significance, a few critical ones have the potential to severely disrupt operations or, in dire circumstances, compromise the OEM. This tension between the desire for stable, long-term collaborations and the need to diversify supplier bases to mitigate supply chain risks (Xie et al., 2021), prompts a crucial question: How can manufacturers reconcile these seemingly conflicting priorities of ensuring both supply chain resilience and cybersecurity integrity? As manufacturers diversify their supplier base in the name of resilience, their organizational 'attack surface' broadens, increasing exposure to cybersecurity risks, especially considering that many cybersecurity incidents originate from within the supply chain ecosystem.

The industry's approach to collaboratively managing cybersecurity risks reflects a regime-level understanding of shared responsibility. Security teams inclined towards a zero-trust approach with legacy networking mindsets were identified as one pain point. The human factor, including insider trust and threat measures, was also recognized as a significant concern, underscoring the importance of winning over the "hearts and minds" of decision-makers and acknowledging the relatively unexplored terrain of insider risk. Insider risk management is acknowledged as an integral part of security programs, emphasizing the need for comprehensive strategies that address both technological and human elements.

Regulatory pressures are adding another layer of complexity to the industry's operational landscape. The increasing involvement of government regulations, such as various chips acts[8] and technology export controls, introduces challenges in maintaining operational efficiency while adhering to an expanding regulatory framework. This development has led several Chief Information Security Officers (CISOs) we interviewed to advocate for industry-led efforts to establish best practices, aiming to manage client costs effectively while enhancing security.

Interestingly, respondents conveyed that their customers now perceive cybersecurity not as a unique selling proposition, but as a fundamental expectation—a "hygiene factor" that should be inherently present in products. This shift indicates that while customers may not explicitly prioritize cybersecurity in their purchasing decisions, its absence or inadequacy could dissuade them from considering a product. Participants noted that cybersecurity is expected rather than highlighted, and its effectiveness can significantly impact customer trust and business relationships.

The nature and extent of engagement with suppliers on cybersecurity issues are significantly influenced by a supplier's position within the supply chain and the specifics of the data being exchanged. Suppliers positioned at points in the supply chain perceived to carry higher risks are more likely to attract discussions on cybersecurity. This observation suggests that the impetus for engaging on cybersecurity issues is often a function of perceived vulnerability or exposure to risk, rather than a uniform standard applied across all segments of the supply chain.

These regime-level dynamics illustrate the necessity for the semiconductor industry to navigate complex supply chain relationships (Skeete, 2019), regulatory demands, and evolving customer expectations to collaboratively enhance cybersecurity practices. While this

[8] The recent US, EU, and UK 'Chips Acts' refer to a series of legislative measures aimed at bolstering the semiconductor industry within these regions. Each act allocates significant funding and resources towards achieving this goal, reflecting a strategic push to secure technological sovereignty and economic security in the face of global semiconductor challenges.

study highlights the importance of trust, pre-competitive collaboration, and shared standards as mechanisms for enhancing supply chain resilience, our findings underscore a key limitation: these mechanisms often assume baseline trust or capability, which may not exist—particularly among lower-tier, offshore, or non-certified suppliers. As several participants noted, smaller firms may lack the resources or incentives to comply with evolving cybersecurity expectations. Prior work in the electronics sector has emphasized the need for traceability and vetting procedures (Livingston, 2007) but these approaches rely on voluntary alignment. Emerging game-theoretic models of supply chain security offer promising alternatives (Gopalakrishnan and Sankaranarayanan, 2023), illustrating how strategies like third-party audits, reputational penalties, escrow mechanisms, and selective traceability can reshape the cost-benefit calculus for compliance. In this sense, trust is not just relational — it can be engineered through systemic incentives and governance interventions Fig. 5.

5.3. Niche innovations

At the niche level, specific collaborative initiatives and emerging technologies are being developed to address cybersecurity challenges within the semiconductor industry. One promising innovation is the integration of "security-by-design," reflecting an innovative shift in system development where cybersecurity measures are embedded from the earliest stages. This approach emphasizes the importance of network isolation, security optimization on the factory floor, and embedding security into the development environment—from software design to the deployment of secure tools and the training of employees and third parties in security practices.

Industry leaders highlighted the indispensable need for a layered defence strategy aimed at securing the environment from multifaceted threats. A central theme is elevating all vendors to meet minimum security standards, ensuring that the entire supply chain operates "above the poverty line" in cybersecurity measures. The panelists endorsed the utilization of third-party services for monitoring the cybersecurity posture of vendors, akin to a credit rating agency grading stakeholders from A to F. This system enables organizations to demand accountability based on these assessments and to drive improvements in cybersecurity practices across the supply chain.

Acknowledging the inevitability of cybersecurity incidents, there is also a focus on rapid recovery strategies to minimize downtime and ensuring the continued shipment of "clean" parts. Secure collaboration is identified as crucial, with industry stakeholders advocating for the adoption of unified frameworks for protecting both physical and intellectual property, promoting transparency and traceability. The semiconductor industry is also explicitly drawing lessons from the automotive industry's segmented approach to supplier assessment—which ranges from standard questionnaires to on-site visits—this method minimizes auditing while fostering improvements in cybersecurity practices.

Enhancing supply chain visibility was a recurring theme in our findings, but participants emphasized that transparency cannot be achieved without robust traceability mechanisms—tools that enable fabs and OEMs to track component provenance, handling, and risk exposure throughout the supply chain. This aligns with previous research (DiMase et al., 2016), which argues that conventional supply chain risk management often overlooks the covert risks posed by counterfeits and advocate for enhanced traceability and risk-informed decision making. Our respondents echoed this shift, calling for digital product passports, secure serialization, and blockchain-enabled tracking—not only to detect tampering and prevent counterfeits, but also to support prioritization of high-risk parts, compliance auditing, and proactive cybersecurity assurance. These traceability systems represent a move beyond passive conformity checks toward active management of supply chain resilience.

Other automotive best practices are being emulated, such as the implementation of Over-The-Air (OTA) updates demonstrated by models like Uptane,[9] highlight the potential for efficient and secure remote updates of software. OTA updates represent a critical capability in maintaining cybersecurity throughout the operational life of products, allowing manufacturers to promptly address vulnerabilities and deploy improvements without requiring physical access. This approach emphasizes considering the entire lifecycle of a product when devising cybersecurity strategies, identifying measures that need to be implemented upfront and those that can be addressed through software interventions.

Furthermore, emerging semiconductor technologies like ARM's CHERI (Capability Hardware Enhanced RISC Instructions)[10] represent potential future innovations in enhancing hardware-level security (Tomlinson et al., 2022). Although most industry respondents did not have sufficient knowledge to comment meaningfully on CHERI, its development underscores the ongoing exploration of advanced technologies to fortify cybersecurity at the foundational hardware level. The role of new technologies like CHERI could play a significant part in future strategies, potentially offering robust solutions for "security at the hardware level" and complementing efforts in "security-by-design."

Lastly, while large OEMs boast significant security teams, mid-tier and smaller OEMs must also integrate security into their operations, underscoring a community-based approach to cybersecurity that spans from the source to the endpoint. This inclusive strategy ensures that all participants in the supply chain contribute to a robust cybersecurity posture, reflecting a collective commitment to mitigating risks through innovation and collaboration. Fig. 5 is a visual presentation of our findings overlaid onto the MLP framework.

As our participants emphasized, the ability to coordinate rapid responses to supply chain threats, conduct supplier audits, and share threat intelligence across fabs and vendors directly supports rapid recovery and system-level adaptability—core dimensions of resilience. This positions OI not as a soft collaboration mechanism, but as a hard strategic capability for absorbing and adapting to cyber disruptions.

5.4. A critique of the MLP's conceptual boundaries

This study raises important questions about the fluidity and sometimes ambiguous boundaries within the MLP framework, particularly when applied to industries characterized by rapid technological advancement and complex interdependencies. Distinguishing between landscape pressures and regime-level dynamics, for instance, becomes challenging in cases like the IT/OT dichotomy, where what initially appears as an endogenous regime practice can, over time, evolve into a landscape standard. This suggests that established practices within the regime may gradually shape and redefine landscape expectations, blurring the lines between internal regime pressures and external structural forces.

Similarly, the interaction of OI with third-party actors complicates the separation between regime-driven innovation and niche solutions. Collaborative innovation across supply chain ecosystems often bridges niche experimentation and regime adaptation, positioning OI as a cross-level mechanism that both introduces niche innovations to the regime and adapts to broader landscape pressures, such as evolving cybersecurity threats. These observations underscore the need to view the MLP not as a rigid hierarchy but as a more dynamic, interwoven model—particularly in industries where collaboration and rapid technological evolution drive continuous feedback across levels.

By acknowledging these fluid boundaries, this study offers a critical

[9] Uptane is the first software update security system for the automotive industry capable of resisting even attacks by nation-state level actors (Uptane, 2024)

[10] CHERI is an advanced security feature designed to protect computer systems from various cyber threats.

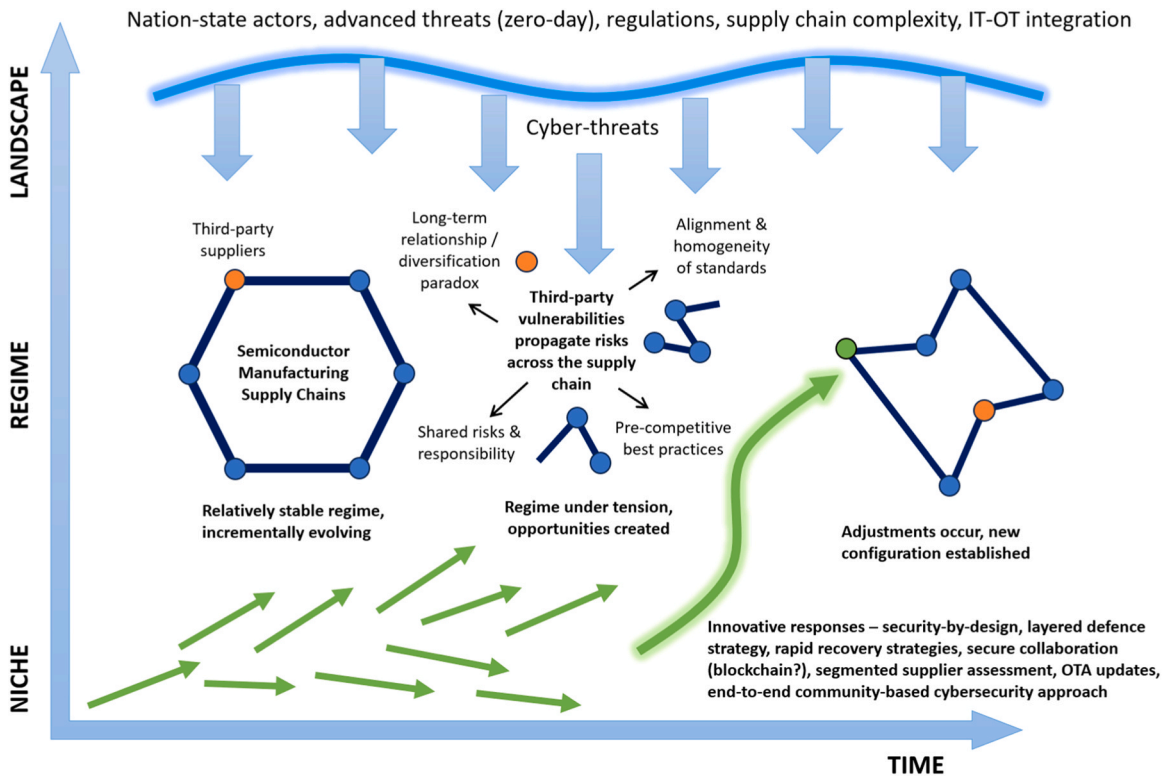

Fig. 5. Research findings nested within the MLP.

reflection on the MLP framework, suggesting that it may benefit from a more flexible interpretation in contexts where regime practices and landscape standards frequently intersect, and where innovation flows seamlessly between niche and regime levels.

6. Conclusion

6.1. Advancing MLP and open innovation: a pathway to resilience

This study demonstrates how the MLP framework can incorporate Open Innovation principles, showing that OI functions as a strategic tool not only for fostering growth but also for *reinforcing resilience and business continuity* in the semiconductor industry—a sector particularly susceptible to cybersecurity threats. By demonstrating how collaboration acts as a cross-cutting mechanism within the MLP framework, this research reveals that OI actively supports niche-level innovations while simultaneously driving regime-level shifts in industry norms and standards. Rather than serving solely as a pathway for growth, *OI is shown to be instrumental in strategic defence*, as collaborative efforts across the supply chain respond dynamically to landscape-level pressures, such as evolving cyber threats. This interplay between MLP levels highlights how landscape-level challenges prompt regime adaptations, such as enhanced compliance requirements, while encouraging niche innovations like new security technologies and protocols—ultimately positioning *OI as a critical mechanism for resilience* within the semiconductor ecosystem.

By defining resilience as the ability to prepare for, absorb, recover from, and adapt to disruptions, this study shows that Open Innovation practices—through shared standards, collaborative audits, and security-by-design initiatives—actively reinforce resilience within semiconductor supply chains.

6.2. Practical implications: industry guidance

This study provides a real-world case study of how OI can be leveraged as a strategic defence against cyber risks within the semiconductor industry, offering a concrete example of how collaboration between fabs and third-party suppliers enhances resilience. A critical insight from our findings is that *third-party suppliers represent the most significant source of cybersecurity risks,* necessitating targeted interventions. Industry stakeholders are encouraged to *adopt OI practices that facilitate joint development of security technologies and strategies*, enabling proactive risk mitigation through collaborative innovation. *Strengthening relationships with suppliers,* including those at lower tiers, is critical to improving supply chain visibility and ensuring consistent cybersecurity practices across all levels. Additionally, stakeholders should *work collaboratively to address gaps in existing standards*, and also consider the challenge of engaging suppliers who may lack incentives or capabilities to meet enhanced security expectations. Developing trust cannot rely solely on voluntary compliance or legacy relationships. It may require the strategic use of third-party certifications, auditing frameworks, and shared platforms that *shift the cost-benefit calculus for lower-tier suppliers*—especially those in opaque or loosely regulated contexts. *Promoting transparency and trust remains essential*, as fostering a culture of openness—where information about vulnerabilities and incidents is shared promptly—will enable more effective collective responses. Finally, *investing in security-by-design is crucial*; integrating security measures early in the development process reduces the challenges associated with retrofitting security into existing infrastructures, thereby strengthening overall resilience.

Key findings of this study include:

- Third-party cyber risks, especially from lower-tier suppliers, are the primary resilience concern in Open Innovation ecosystems.
- Supply chain transparency and trust are central, but require mechanisms like traceability and standardized compliance.
- IT/OT convergence introduces novel vulnerabilities that challenge traditional regime boundaries within the MLP.
- Security-by-design and OTA updates represent promising niche-level innovations aligned with regime shifts.

6.3. Limitations and future scope

This study may be constrained by *its sample size and the diversity* of organizations represented, which could limit the generalizability of the findings. Additionally, the research primarily focuses on the *perspectives of semiconductor manufacturers (fabs) and tier 1 suppliers*, potentially overlooking the viewpoints of suppliers, particularly those at lower tiers.

Future studies should aim to incorporate *perspectives from suppliers* at various tiers to provide a more comprehensive view of the collaborative dynamics involved in mitigating cyber risks. *Longitudinal research* could also offer valuable insights by tracking how collaborative practices and industry approaches to cybersecurity evolve over time. Finally, *evaluating the effectiveness of specific collaborative initiatives* and technologies would provide empirical evidence to support a prioritization of best practices.

Acknowledgment of Funding

We extend our heartfelt thanks to the ESRC Digital Security by Design Social Science Hub+ (Discribe) – Connecting Capabilities Fund (grant number: ES/V003666/1), whose generous funding made this research possible. We gratefully acknowledge the University of Bath School of Management for supporting our work. We also acknowledge Laith Altimime, Bettina Weiss, Pantelitsa Paraskeva Markus, and Ana Bernado at SEMI for their support with SEMICON West and SEMICON Europa.

Declaration of generative AI in scientific writing

During the preparation of this work the author(s) used ChatGPT in order to improve readability and language. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

CRediT authorship contribution statement

Siraj Shaikh: Writing – review & editing, Validation, Supervision, Resources, Funding acquisition. **Skeete Jean-Paul H:** Writing – original draft, Visualization, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Jean-Paul Skeete reports financial support was provided by UK Research and Innovation Economic and Social Research Council. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We extend our heartfelt thanks to the ESRC Digital Security by Design Social Science Hub+ (Discribe) – Connecting Capabilities Fund (grant number: ES/V003666/1), whose generous funding made this research possible. We are also deeply grateful for the support provided by the University of Bath School of Management and Semiconductor Equipment and Materials International (SEMI), which significantly contributed to the success of our work.

References

Ahmad, A., 2020. Automotive semiconductor industry - trends, safety and security challenges', In: Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Jun. 2020, pp. 1373–1377. doi: 10.1109/ICRITO48877.2020.9197894..

Akter, N., Karabiyik, M., Wright, A., Shur, M., Pala, N., 2020. AI powered THz testing technology for ensuring hardware cybersecurity', In: Proceedings of the 2020 IEEE Research and Applications of Photonics in Defense Conference (RAPID), Aug. 2020, pp. 1–2. doi: 10.1109/RAPID49481.2020.9195662..

T. Alsop, 'Semiconductor market size 2024'. 2024. Accessed: Feb. 06, 2024. [Online]. Available: https://www.statista.com/statistics/266973/global-semiconductor-sales-since-1988/.

M. Areno, 'Supply chain threats: integrated circuits', Intel, 2020. Accessed: Jun. 15, 2025. [Online]. Available: https://www.intel.com/content/www/us/en/security/security-practices/docs/supply-chain-threats-integrated-circuits.html.

E. Bell, B. Harley, and A. Bryman, Business research methods, New Edition, Sixth Edition. Oxford, New York: Oxford University Press, 2022.

Bergek, A., Berggren, C., Magnusson, T., Hobday, M., 2013. Technological discontinuities and the challenge for incumbent firms: destruction, disruption or creative accumulation?'. Res. Policy 42 (6), 1210–1224.

Boyes, H., 2015. Cybersecurity and Cyber-Resilient supply chains. Technol. Innov. Manag. Rev. 5 (4), 28–34.

Braun, V., Clarke, V., 2012. Thematic analysis'. APA Handbook of Research Methods in Psychology, Vol 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological, in APA Handbooks in Psychology®. American Psychological Association, Washington, DC, US, pp. 57–71. https://doi.org/10.1037/13620-004.

Chen, Y., Li, B., Huo, B., 2025. Building operational resilience through digitalization: the roles of supply chain network position (Feb.). Technol. Forecast. Soc. Change 211, 123918. https://doi.org/10.1016/j.techfore.2024.123918 (Feb.).

H.W. Chesbrough, Open innovation: the new imperative for creating and profiting from technology. Harvard Business Press, 2003.

Collier, Z.A., Sarkis, J., 2021. The zero trust supply chain: managing supply chain risk in the absence of trust (Jun.). Int. J. Prod. Res. 59 (11), 3430–3445. https://doi.org/10.1080/00207543.2021.1884311 (Jun.).

J.W. Creswell, Qualitative inquiry and research design: Choosing among five approaches. Sage publications, 2012. Accessed: Mar. 07, 2015. [Online]. Available: https://books.google.co.uk/books?hl=en&lr=&id=OJYEbDtkxq8C&oi=fnd&pg=PR1&dq=qualitative+inquiry+and+research+design&ots=eO2hfKMkeo&sig=YylXGnFpVTA-po5Kk5MeROBP6Cw.

A.L. Crouch *et al.*, 'Innovate practices on cybersecurity of hardware semiconductor devices', In: Proceedings of the 2019 IEEE 37th VLSI Test Symposium (VTS), Apr. 2019, pp. 1–1. doi: 10.1109/VTS.2019.8758665.

Dalal, S., Lilhore, U.K., Simaiya, S., Radulescu, M., Belascu, L., 2024. Improving efficiency and sustainability via supply chain optimization through CNNs and BiLSTM (Dec.). Technol. Forecast. Soc. Change 209, 123841. https://doi.org/10.1016/j.techfore.2024.123841 (Dec.).

S. Datta Burton, L.M. Tanczer, S. Vasudevan, S. Hailes, and M. Carr, 'The UK Code of Practice for Consumer IoT Cybersecurity: where we are and what next', Department for Digital, Culture, Media & Sport, London, UK, Report, Apr. 2021. Accessed: Feb. 06, 2024. [Online]. Available: ⟨https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport⟩.

C. Davies, K. Hille, S. Jung-a, and Q. Liu, 'Semiconductor giants race to make next generation of cutting-edge chips', Financial Times, Dec. 11, 2023. Accessed: Feb. 29, 2024. [Online]. Available: https://www.ft.com/content/e9be182f-ec9e-4426-9cd2-d5181fd64778.

B. Dick, Qualitative methodology: a practical guide. SAGE Publications, Inc., 2014. doi: 10.4135/9781473920163.

DiMase, D., Collier, Z.A., Carlson, J., Gray Jr., R.B., Linkov, I., 2016. 'Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex Systems'. Risk Anal. 36 (10), 1834–1843. https://doi.org/10.1111/risa.12536.

DSbD, 'Digital security by design', digital security by design. Accessed: Feb. 06, 2024. [Online]. Available: https://www.dsbd.tech/.

DSIT, 'National semiconductor strategy', GOV.UK. Accessed: Feb. 06, 2024. [Online]. Available: https://www.gov.uk/government/publications/national-semiconductor-strategy/national-semiconductor-strategy.

M. Duffield, 'The semantics of data sharing across the semiconductor supply chain | AWS for Industries'. Accessed: Sep. 30, 2024. [Online]. Available: https://aws.amazon.com/blogs/industries/the-semantics-of-data-sharing-across-the-semiconductor-supply-chain/.

R. Feldman, 'Intellectual property as a law of organization - Article by Jonathan M. Barnett', Southern California Law Review. Accessed: Jun. 15, 2025. [Online]. Available: https://southerncalifornialawreview.com/2011/05/04/intellectual-property-as-a-law-of-organization-article-by-jonathan-m-barnett/.

Fereday, J., Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development (Mar.). Int. J. Qual. Methods 5 (1), 80–92. https://doi.org/10.1177/160940690600500107 (Mar.).

Geels, F.W., 2011. The multi-level perspective on sustainability transitions: responses to seven criticisms. Environ. Innov. Soc. Transit 1 (1), 24–40.

Geels, F.W., et al., 2016. The enactment of socio-technical transition pathways: a reformulated typology and a comparative multi-level analysis of the German and UK low-carbon electricity transitions (1990–2014) (May). Res. Policy 45 (4), 896–913. https://doi.org/10.1016/j.respol.2016.01.015 (May).

F.W. Geels and R. Kemp, The multi-level perspective as a new perspective for studying socio-technical transitions. na, 2012.

Gephart, R.P., 2004. Qualitative research and the academy of management journal (Aug.). Acad. Manag. J. 47 (4), 454–462. https://doi.org/10.5465/amj.2004.14438580 (Aug.).

Goffin, K., Åhlström, P., Bianchi, M., Richtnér, A., 2019. Perspective: state-of-the-art: the quality of case study research in innovation management. J. Prod. Innov. Manag 36 (5), 586–615. https://doi.org/10.1111/jpim.12492.

Gopalakrishnan, S., Sankaranarayanan, S., 2023. Cooperative security against interdependent risks. Prod. Oper. Manag. 32 (11), 3504–3520. https://doi.org/10.1111/poms.14047.

Gotze, K., 2011. A survey of frequently identified vulnerabilities in commercial computing semiconductors', In: Proceedings of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, Jun. 2011, pp. 122–126. doi: 10.1109/HST.2011.5955008..

Guertler, M.R., Kriz, A., Sick, N., 2020. Encouraging and enabling action research in innovation management. RD Manag. 50 (3), 380–395. https://doi.org/10.1111/radm.12413.

Guin, U., DiMase, D., Tehranipoor, M., 2014. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead (Feb.). J. Electron. Test. 30 (1), 9–23. https://doi.org/10.1007/s10836-013-5430-8 (Feb.).

Hammi, B., Zeadally, S., Nebhen, J., 2023. Security threats, countermeasures, and challenges of digital supply chains (Jul.). ACM Comput. Surv. 55 (14s), 316:1–316:40. https://doi.org/10.1145/3588999 (Jul.).

Herzog, P., Leker, J., 2010. Open and closed innovation – different innovation cultures for different strategies (Jan.). Int. J. Technol. Manag 52 (3/4), 322–343. https://doi.org/10.1504/IJTM.2010.035979 (Jan.).

von Hippel, E., 2005. Democratizing innovation: the evolving phenomenon of user innovation (Mar.). J. F. üR. Betr. 55 (1), 63–78. https://doi.org/10.1007/s11301-004-0002-8 (Mar.).

Hurtarte, J.S., Wolsheimer, E.A., Tafoya, L.M., 2007. 'Chapter 4 - semiconductor manufacturing basics. In: Hurtarte, J.S., Wolsheimer, E.A., Tafoya, L.M. (Eds.), in Understanding Fabless IC Technology. Burlington: Newnes, pp. 41–45. https://doi.org/10.1016/B978-075067944-2/50005-9.

Inagaki, K., Lewis, L., 2024. Japan to restrict semiconductor equipment exports as China chip war intensifies'. Mar. 31, 2023. Accessed: Feb. 29 Financial. ⟨https://www.ft.com/content/768966d0-1082-4db4-b1bc-cca0c1982f9e⟩. Mar. 31, 2023. Accessed: Feb. 29.

Ionescu, O., Dumitru, V., Pricop, E., Pircalabu, S., 2020. 'Innovative hardware-based cybersecurity solutions', in Recent Developments on Industrial Control Systems Resilience, E. Pricop, J. Fattahi, N. Dutta, and M. Ibrahim, Eds., in Studies in Systems, Decision and Control., Cham: Springer International Publishing, 2020, pp. 283–299. doi: 10.1007/978-3-030-31328-9_12..

Johnson, J.P., 2006. Collaboration, peer review and open source software (Nov.). Inf. Econ. Policy 18 (4), 477–497. https://doi.org/10.1016/j.infoecopol.2006.07.001 (Nov.).

Junaid, M., Zhang, Q., Cao, M., Luqman, A., 2023. Nexus between technology enabled supply chain dynamic capabilities, integration, resilience, and sustainable performance: an empirical examination of healthcare organizations (Nov.). Technol. Forecast. Soc. Change 196, 122828. https://doi.org/10.1016/j.techfore.2023.122828 (Nov.).

Khan, O., Estay, D., 2015. Supply chain cyber-resilience: creating an agenda for future research. Technol. Innov. Manag. Rev. 5 (4), 6–12.

N. King, 'Template analysis.', 1998, Accessed: Feb. 10, 2016. [Online]. Available: http://psycnet.apa.org/psycinfo/1999-02931-006.

Latif, M.N. Abd, Aziz, N.A. Abd, Hussin, N.S. Nik, Aziz, Z.Abdul, 2021. Cyber security in supply chain management: a systematic review (Mar.). Logforum 17, 49–57. https://doi.org/10.17270/J.LOG.2021555 (Mar.).

Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for industry 4.0 in the current literature: a reference framework (Dec.). ' Comput. Ind. 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004 (Dec.).

Lim, C., Kim, M.-J., Kim, K.-H., Kim, K.-J., Maglio, P.P., 2017. Using data to advance service: managerial issues and theoretical implications from action research (Jan.). J. Serv. Theory Pract. 28 (1), 99–128. https://doi.org/10.1108/JSTP-08-2016-0141 (Jan.).

Livingston, H., 2007. Avoiding counterfeit electronic Components' (Mar.). IEEE Trans. Compon. Packag. Technol. 30 (1), 187–189. https://doi.org/10.1109/TCAPT.2007.893682 (Mar.).

Lotfi, R., Hazrati, R., Aghakhani, S., Afshar, M., Amra, M., Ali, S.S., 2024. A data-driven robust optimization in viable supply chain network design by considering open innovation and blockchain technology (Jan.). J. Clean. Prod. 436, 140369. https://doi.org/10.1016/j.jclepro.2023.140369 (Jan.).

Maestrini, V., Luzzini, D., (Rami) Shani, A.B., Canterino, F., 2016. The action research cycle reloaded: conducting action research across buyer-supplier relationships (Dec.). J. Purch. Supply Manag 22 (4), 289–298. https://doi.org/10.1016/j.pursup.2016.06.002 (Dec.).

Maguire, M., Delahunt, B., 2024. Doing a thematic analysis: a practical, step-by-step guide for learning and teaching scholars. Irel. J. High. Educ. 9 (3). ⟨https://ojs.aishe.org/index.php/aishe-j/article/view/335⟩. Art. no. 3, Oct. 2017, Accessed: Apr. 28.

Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F., Friday, D., 2022. New challenges in supply chain management: cybersecurity across the supply chain (Jan.). Int. J. Prod. Res. 60 (1), 162–183. https://doi.org/10.1080/00207543.2021.1984606 (Jan.).

Moschko, L., Blazevic, V., Piller, F.T., 2023. Paradoxes of implementing digital manufacturing systems: a longitudinal study of digital innovation projects for disruptive change. J. Prod. Innov. Manag 40 (4), 506–529. https://doi.org/10.1111/jpim.12667.

National Research Council, Disaster resilience: a national imperative. Washington, DC: The National Academies Press, 2012. doi: 10.17226/13457.

Ponomarov, S.Y., Holcomb, M.C., 2009. Understanding the concept of supply chain resilience (Jan.). Int. J. Logist. Manag 20 (1), 124–143. https://doi.org/10.1108/09574090910954873 (Jan.).

Pratt, M.G., 2008. Fitting oval pegs into round holes: tensions in evaluating and publishing qualitative research in Top-Tier north American journals (Jul.). Organ. Res. Methods 11 (3), 481–509. https://doi.org/10.1177/1094428107303349 (Jul.).

Rostami, M., Koushanfar, F., Rajendran, J., Karri, R., 2013. 'Hardware security: Threat models and metrics', In: Proceedings of the 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Nov. 2013, pp. 819–823. doi: 10.1109/ICCAD.2013.6691207..

Schaller, R.R., 1997. Moore's law: past, present and future (Jun.). IEEE Spectr. 34 (6), 52–59. https://doi.org/10.1109/6.591665 (Jun.).

Schumpeter, J.A., 1947. The creative response in economic history. J. Econ. Hist. 7 (02), 149–159.

Singh, G., Rajesh, R., Misra, S.C., Singh, S., 2024. Analyzing the role of digital twins in developing a resilient sustainable manufacturing supply chain: a grey influence analysis (GINA) approach (Dec.). Technol. Forecast. Soc. Change 209, 123763. https://doi.org/10.1016/j.techfore.2024.123763 (Dec.).

Skeete, J.-P., 2019. Concentration of power: a UK case study examining the dominance of incumbent automakers and suppliers in automotive sociotechnical transitions (Jan.). Glob. Transit 1, 93–103. https://doi.org/10.1016/j.glt.2019.06.001 (Jan.).

Sodhi, M.S., Tang, C.S., 2019. Research opportunities in supply chain transparency (Dec.). Prod. Oper. Manag 28 (12), 2946–2959. https://doi.org/10.1111/poms.13115 (Dec.).

Sundarakani, B., Ajaykumar, A., Gunasekaran, A., 2021. Big data driven supply chain design and applications for blockchain: an action research using case study approach (Jul.). Omega 102, 102452. https://doi.org/10.1016/j.omega.2021.102452 (Jul.).

Tansey, O., 2007. Process tracing and elite interviewing: a case for non-probability sampling'. PS Polit. Sci. Polit. 40 (04), 765–772.

Tomlinson, A., Parkin, S., Shaikh, S.A., 2022. Drivers and barriers for secure hardware adoption across ecosystem stakeholders. J. Cybersecur. 8 (1), tyac009. , doi: 10.1093/cybsec/tyac009.

Touboulic, A., Walker, H., 2016. A relational, transformative and engaged approach to sustainable supply chain management: the potential of action research (Feb.). Hum. Relat. 69 (2), 301–343. https://doi.org/10.1177/0018726715583364 (Feb.).

Uptane, 'Uptane | Uptane'. Accessed: Mar. 12, 2024. [Online]. Available: https://uptane.org/.

Vaismoradi, M., Jones, J., Turunen, H., Snelgrove, S., 2016. Theme development in qualitative content analysis and thematic analysis. Art. no. 5, Jan. J. Nurs. Educ. Pract. 6 (5). https://doi.org/10.5430/jnep.v6n5p100. Art. no. 5, Jan.

A.H.V. de Ven, Engaged Scholarship: A Guide for Organizational and Social Research, Illustrated edition. Oxford: Oxford University Press, USA, 2007.

Weishäupl, E., Yasasin, E., Schryen, G., 2018. Information security investments: an exploratory multiple case study on decision-making, evaluation and learning (Aug.). Comput. Secur 77, 807–823. https://doi.org/10.1016/j.cose.2018.02.001 (Aug.).

Wieland, A., Tate, W.L., Yan, T., 2023. A guided tour through the qualitative research city (vol. n/a, no. n/a). J. Supply Chain Manag.. https://doi.org/10.1111/jscm.12315.

Xie, Z., Wang, J., Miao, L., 2021. Big data and emerging market firms' innovation in an open economy: the diversification strategy perspective (Dec.). Technol. Forecast. Soc. Change 173, 121091. https://doi.org/10.1016/j.techfore.2021.121091 (Dec.).

Xu, X., Rahman, F., Shakya, B., Vassilev, A., Forte, D., Tehranipoor, M., 2019. Electronics supply chain integrity enabled by blockchain (May). ACM Trans. Des. Autom. Electron. Syst. 24 (3), 31:1–31:25. https://doi.org/10.1145/3315571 (May).

Zhao, S., Zhu, S., Guo, S., 2015. 'The information security in semiconductor industry', In: Proceedings of the 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Dec. 2015, pp. 1782–1785. doi: 10.1109/IEEM.2015.7385954..

Zhu, S., Guo, E., Lu, M., Yue, A., 2016. An efficient data leakage prevention framework for semiconductor industry', In: Proceedings of the 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Dec. 2016, pp. 1866–1869. doi: 10.1109/IEEM.2016.7798201..