Partners Universal Journal of Artificial Intelligence Research (PUJAIR)
Volume: 01 Issue: 01 | April-May 2026| www.pujair.com

Skills to Level Up Operational Technology (OT) Cybersecurity: A Quadrant-Based Analysis of Workforce Capabilities, Demand Trajectories, and Strategic Development Pathways

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - With industrial control systems (ICS) becoming more interconnected with enterprise networks and cloud platforms and with global supply chains, operational technology (OT) cybersecurity has become critical discipline. This article considers a quadrant based skills framework, which categories twenty four professional skills on two dimensions, namely the dimension of essentialness, and the dimension of demand. The framework divides these competencies into four quadrants Core Skills, Emerging Skills, Steady Skills, and Out of Focus Skills, and further categorizes each of the skills into one of eight categories that encompass cognitive ability, technology fluency, management capability, interpersonal effectiveness, physical aptitude, self-efficacy, engagement traits, and ethical orientation. The discussion places the framework in the context of the history of the field of industrial cybersecurity, follows current workforce trends, outlines problems that remain and provides practical steps for individuals, organizations, and educators. The analysis shows that a successful OT cybersecurity program requires a multi-faceted portfolio of capabilities over and above a purely technical focus. The article ends by stating that organisations that can balance the basics of operations with the investment in new skills that will deal with future threats will have the best chance of maintaining the critical infrastructure upon which modern society relies, and that workforce strategies should continue to be adjusted to reflect changes in threats and technology.

Keywords: OT Cybersecurity, Workforce Skills, ICS Security, Critical Infrastructure, Skills Framework, Capability Development, Cyber-Physical Systems, Industrial Cybersecurity.

1. INTRODUCTION

Securing industrial systems is no longer just an engineering problem, but now a national security and economic issue. Digital control systems have come to support power grids, water treatment plants, oil and gas pipelines, manufacturing lines, transportation hubs, and pharmaceutical facilities all systems originally built for reliability not security. More than ever before, the people responsible for protecting these spaces need a wider skill set to protect them in the face of a larger threat landscape in a networked environment.

This complex picture is encapsulated in the figure we are analyzing, Skills to Level Up OT Cybersecurity. It maps out 24 competencies against two overlapping axes and categorizes the competencies according to their nature. In so doing, the figure challenges the legacy notion that cybersecurity is a "purely technical" career. Rather, it defines this domain as a synthesis of thinking, moral, social, and managerial skills. This article is a rendition of the figure in a more extended scholarly discussion. It discusses the framework, its structure and the placement of the skills and what implications it has for the future of the

OT cybersecurity profession. It also utilizes industry research, professional standards, and academic literature to support the analysis, as well as to illuminate directions for further research.

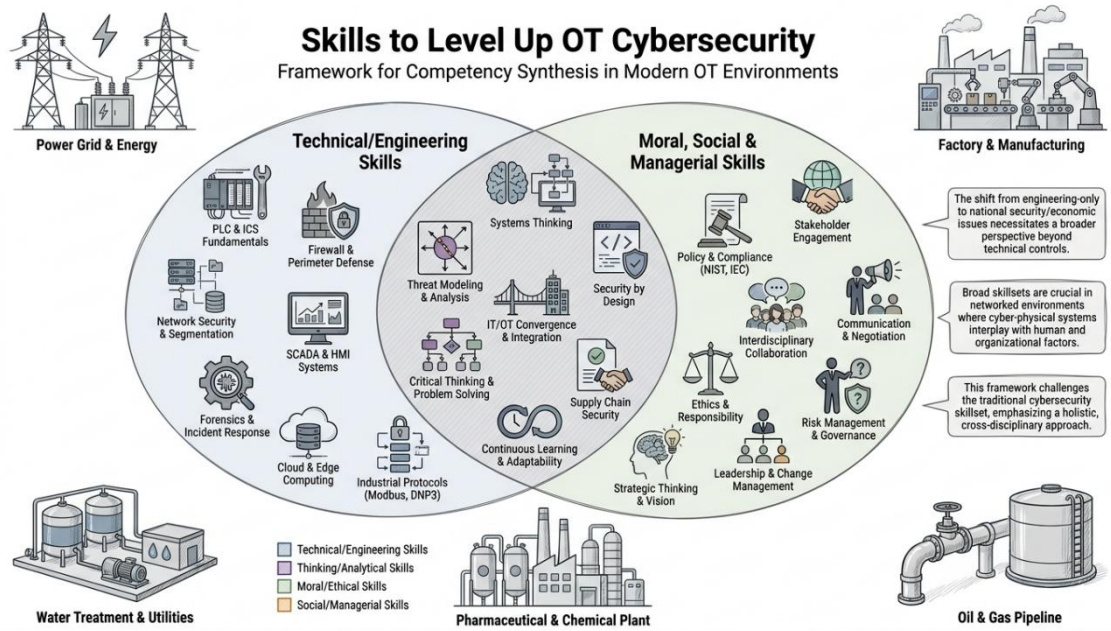

Fig -1: Skills to Level up OT Cybersecurity

2. OBJECTIVES OF THE STUDY

Study has several related objectives. First, it should make the meaning and structure of the quadrant based skills model clearer, to enable practitioners and academics to use it as a diagnostic tool. Second, it has the aim of studying each of the twenty four competencies in detail enough to reveal their relevance in the field, their interdependencies, and their common developmental pathways. Third, it aims to assess the link between essentialness and demand, which is sometimes more nuanced than the typical workforce narratives. Finally, it examines the meaning of the framework in terms of hiring, training, certifications, and curriculum development in OT cybersecurity. Fifth, it highlights issues organizations may encounter when working to turn skills frameworks into real skills and suggests solutions based on existing evidence. Lastly, the article casts an eye into the future, speculating on the potential trajectory of the framework in the face of changing technologies, regulations, and geopolitical uncertainties. The objectives set forth a framework for the ensuing analysis and keep the discussion both interpretive and actionable.

3. HISTORICAL BACKGROUND OF OT CYBERSECURITY

OT cybersecurity isn't something that has suddenly appeared out of nowhere. It went through several cycles of technological and operational evolution. In the early years of industrial automation, control systems tended to be independent. They were run by trained engineers and had few connections to other networks by using proprietary protocols. Security was viewed as something of a problem in physical access and equipment reliability as opposed to digital defence. Things started to change in the late 1990s, early 2000s when Ethernet based networking was introduced and industrial systems began using

Windows operating systems and remote access. This convergence has resulted in a lot of improvements in terms of productivity, but it has also added a risk of malware, unauthorized access, and supply chain risks. In 2010, Stuxnet proved to be a turning point in the history of cyber operations, as it showed that a cyber-attack could have a physical impact on industrial equipment. Since then, several more incidents, such as the attacks in the Ukraine power grid in 2015 and 2016, the use of Triton malware to target safety instrumented systems in 2017, and the ransomware attack on Colonial Pipeline in 2021, have underscored the need for dedicated OT protection capability.

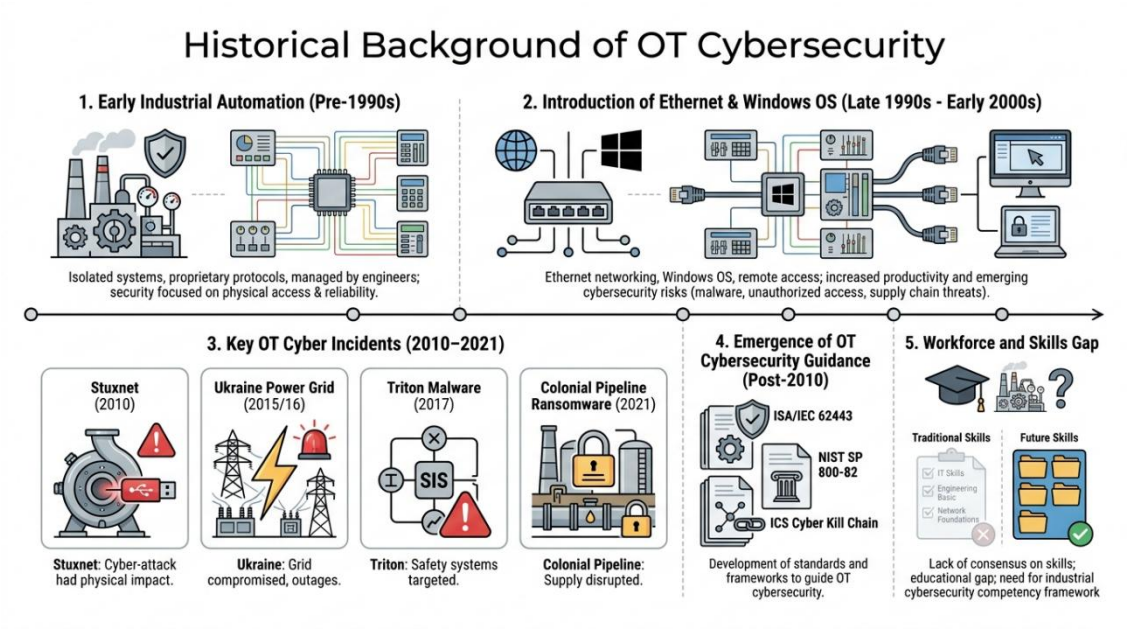

Fig -2: Historical Background of OT Cybersecurity

As a result, standards and frameworks have been developed including ISA/IEC 62443, NIST Special Publication and the ICS Cyber Kill Chain by Assante and Lee (2015). However, the workforce element was not as well developed, despite the technical guidance that is now available. There was a lack of consensus on the mix of skills required and educational institutions were not producing graduates who were able to work in the industrial environment. In response to this gap, a structured approach to thinking about competencies as a portfolio rather than checklist is envisioned in the skills framework examined in this paper.

4. FIGURE INTERPRETATION AND ANALYTICAL FRAMEWORK

4.1 The Two Axes

There are two perpendicular axes on which the rest of the analysis is organized. The horizontal axis is essentialness and is an indicator of how critical or basic a skill is in day-to-day OT cybersecurity work. Skills located to the right on the chart are believed to be essential in today's current role. The vertical axis indicates the demand level and thus the interest trend of the market and organizations in the skill. Recruitment pressure on skills is higher the higher the skill appears on the chart and stable or stagnant the lower the skill appears on the chart.

The intersection of these two axes generates a 2 x 2 matrix, which can be used as a diagnostic tool as well as a strategic map to look forward.

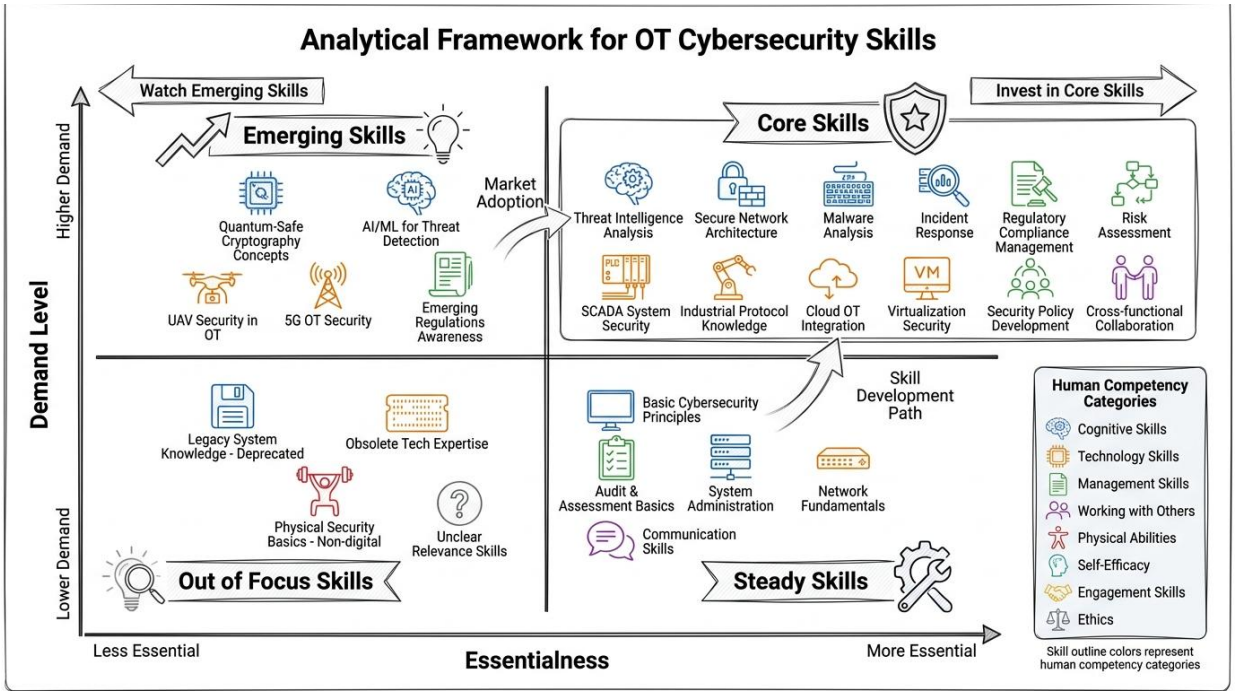

Fig -3: Analytical Framework for OT Cybersecurity Skills

4.2 The Four Quadrants

Core Skills in the upper right quadrant are the skills needed today and which are becoming more important. These are the key workers in the field and are in constant need of investment. In the upper left quadrant, Emerging Skills are skills that are not yet commonly understood as a must-have skill but have a growing demand. These are indicative of the future for discipline. Steady Skills in the lower right quadrant are the skills that continue to be critical for operation despite the levelling off hiring pressure. The Out of Focus Skills quadrant (lower left) shows competencies that are currently on the fringes of organizational focus but have potential value.

4.3 The Eight Skill Categories

The figure also categories each skill by means of a colour coded legend that categorizes the skill into 8 categories. They are divided into eight categories Cognitive Skills, Technology Skills, Management Skills, Working with others, Physical Abilities, Self efficacy, Engagement Skills, and Ethics. The taxonomy is designed to be all-inclusive of the various human competencies pertinent to protecting an industrial environment, not only limiting competency to technical knowledge. This two-way classification by quadrant and category enables the reader to see both the place of the skill in the field and how it is a human capacity.

5. CURRENT TRENDS SHAPING THE OT CYBERSECURITY WORKFORCE

There are several trends influencing the current state of the OT cybersecurity workforce and strengthening the applicability of the quadrant model.

Qualified practitioners are still in short supply, and this is the first trend. According to industry reports, there is a global shortage of cybersecurity staffing of over 4,000,000 professionals, and particularly the shortage of OT specific staff members, as they must have a hybrid mix of engineering and security expertise (ISC2, 2023). The scarcity of these skills creates a critical need for mentoring, leadership and knowledge transfer, the latter of which are both in the Core and Emerging quadrants of the figure.

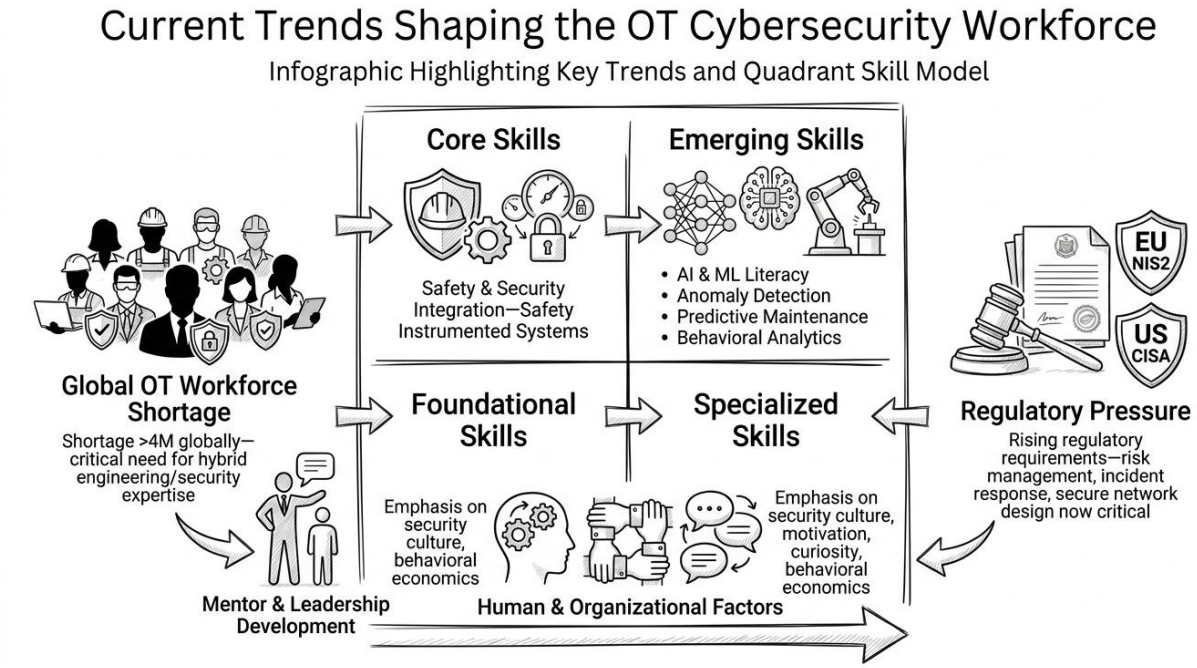

Fig -4: Current Trends Shaping the OT Cybersecurity Workforce

The second trend is an increase in Artificial Intelligence (AI) and Machine Learning (ML) use in industrial defense. Anomaly detection, predictive maintenance, and behavioural analytics with AI have made the jump from research labs to commercial platforms. This positioning of AI and ML in the Emerging Skills quadrant highlights the acceleration of AI and ML and identifies practitioners who build literacy in these technologies will be in a strong position.

The third trend has to do with regulatory pressure. Operators of essential services are subject to greater compliance requirements because of frameworks like the European Union NIS2 Directive and the United States Cybersecurity and Infrastructure Security Agency directives, as well as sector-specific regulations in energy and water. All of this makes risk management, incident response planning, and secure network design even more critical, as shown in the Core Skills quadrant.

The fourth trend relates to the merging of the safety and security disciplines. Traditionally, process safety and cybersecurity have been distinct functions, and their respective cultures and reporting structures have been different. There's been a concerted call to action from organizations recently including the International Society of Automation for tighter integration, especially for safety instrumented systems that are vulnerable to cyber threats. The figure confirms this trend with safety being placed at the top of the Core Skills quadrant.

The fifth trend is the increased focus on the role human and organizational factors play in cybersecurity results. The studies on security culture, behavioral economics, and organizational learning have shown that technical measures are not sufficient to be resilient. This overarching transition towards human centric cybersecurity is also visible in the included skills, including motivation, mission, curiosity, and active listening.

6. DETAILED DISCUSSION OF THE SKILL CATEGORIES

6.1 Core Skills as the Operational Backbone

The Core Skills quadrant contains skills that are highly essential but see increasing demand. Safety is ranked highest on both axes, and indeed OT cybersecurity is about ensuring the safety of physical processes, which can put people, property and the environment at risk. The inclusion of safety as an ethics related competency and not just a procedural competency implies that safety is not a checkbox but a moral commitment.

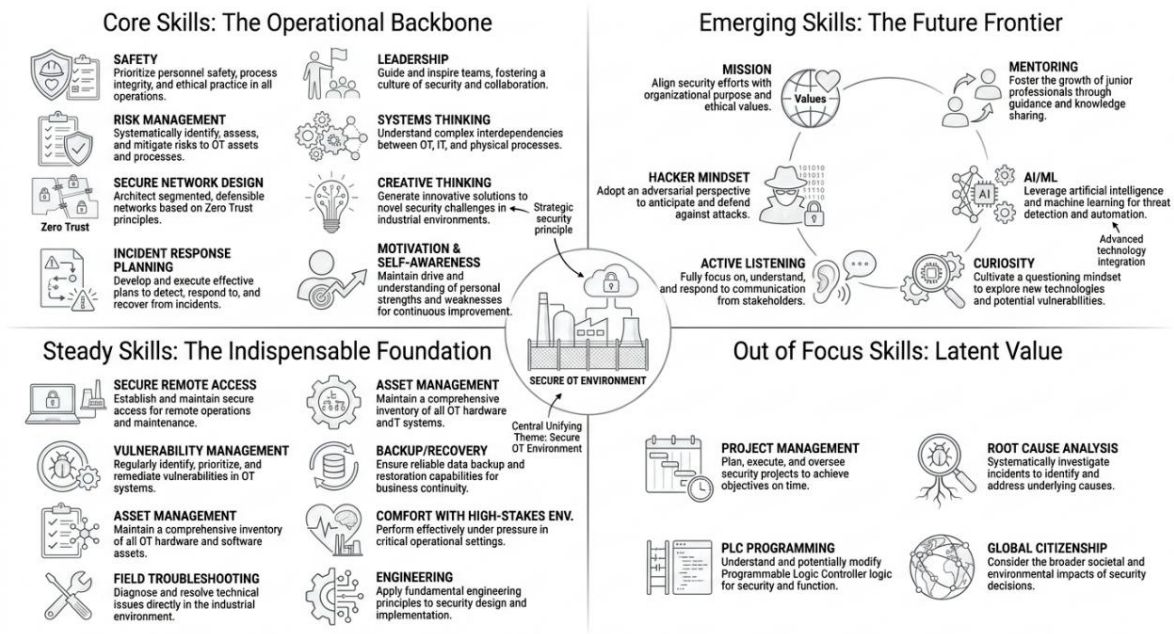

Fig -5: Discussion of the Skill Categories

Risk management is a management skill and is prominently located in the quadrant. Risk management is effective and consistent with the organisation's risk appetite, regulatory requirements, and operational limitations. It involves skills in qualitative and quantitative analysis, scenario planning, and communication to stakeholders. ISA/IEC 62443 3 2 standard codifies this practice in industrial setting.

Technical skills that hold the technical core of the quadrant are secure network design and incident response planning. Secure network design is based on defensible architectures, segmentation, conduits, zones and zero trust principles. With the need for ongoing operations in industrial environments, incident response planning is a way to ensure that an organization can detect and manage a cyber event, recover from it, and learn from it.

Leadership, part of working with others, is the human aspect of crisis management and transformation. Cybersecurity leaders not only have to sell difficult risks to executives but also must manage the work of other functional areas and maintain personnel morale during an incident that can last days or even weeks. The field requires intellectual demands of systems thinking and creative thinking, which are cognitive skills. Systems thinking helps practitioners to understand the interactions between the technical, human, and organizational subsystems, and creative thinking helps to facilitate a new approach to threat modeling and adaptive defense. The quadrant is completed by motivation and self-awareness, which are included in the concept of self-efficacy. These characteristics enable them to learn all the time and maintain stress resilience. It is a critical factor in an industry already facing worker shortages and even technically skilled employees are known to hit a ceiling without them or burn out.

6.2 Emerging Skills as the Future Frontier

The Emerging Skills quadrant is for skills that are increasingly in demand and have not yet been recognized. Mission, under the category of ethics, is an insight into growing values based engagement to attract and retain cybersecurity professionals. Youth practitioners prefer employment that is more meaningful and purposeful such as energy, health, and water, all of which relate to the betterment of society.

Mentoring, which is in the working with others category, serves to directly tackle the workforce shortage. With the departure of experienced professionals coming and going into related positions, there is a real need for knowledge transfer in organizations. Mentoring also helps to rapidly develop mid-career professionals by getting them on the inside scoop of how operations work, which is hard to pick up from a textbook or curriculum.

The technically most loaded competency in the quadrant is the use of artificial intelligence and machine learning (under the umbrella of technology). They can be used for anomaly detection in network traffic or for predicting maintenance needs in physical assets, among other examples, in OT environments. A practitioner knowledgeable about their strengths, limitations and adversarial vulnerabilities will become more important as adoption takes off.

Curiosity is an engagement skill and while seemingly soft, it is the basis for nearly all cybersecurity practice improvement. The people who find new ways of attacking, new ways of defending, and new technology tend to be interested in "how things work. Active listening (working with others) contributes to cross disciplinary communication. OT environments rely on collaboration between engineers, security analysts, executives and operators and listening helps to minimize miscommunications that can lead to vulnerabilities or operational disruptions.

Hacker mindset is also an engagement skill and relates to thinking like an adversary. This is a feature that is useful for proactive defense, threat hunting, and red team exercises. The significance of such a mindset is rising, even though many traditional OT professionals have been skeptical about this mindset, as industrial threats have been evolving into more sophisticated ones.

6.3 Steady Skills as the Indispensable Foundation

While Steady Skills are still important, demand for these are flattening as the supply is catching up or because they are seen as expectations. Secure remote access, a technology skill, is now a permanent requirement for operation in a distributed industrial environment, as vendors, contractors and field engineers come and go from different locations. Vulnerability management is a cognitive skill that needs identification, prioritization, and remediation of assets across complex technology stacks. The practice is

well developed, however, legacy systems and constraints in patching make it challenging to do well in OT contexts.

Management encompasses asset management and is the foundation of any control system security program. Defense is impossible if you don't have an accurate list of all devices, versions of their firmware and network connections. Backup/recovery a technology skill supports resilience/disaster recovery. Although ransomware isn't growing as in-demand in industrial environments as other more prominent Core Skills, it remains an operational asset and is becoming more prevalent.

Physical abilities include field troubleshooting, which is a special aspect to OT cybersecurity professionals having to work with equipment in physical environments. OT specialists can walk the plant floor, understand the instrumentation, and react to various physical issues that are not found in IT. There is a close relationship between the self-efficacy component called comfort with high stakes environments. Work in critical infrastructure requires psychological preparedness to deal with critical situations where errors have serious consequences.

Engineering is a cognitive skill that will make sure that cybersecurity controls don't affect physical processes. When a control engineer understands network security, or a cybersecurity engineer understands process control, these sorts of misaligned interventions can be avoided, preventing both forms of risk from being injected in either direction.

6.4 Out of Focus Skills and Their Latent Value

Skills in the Out of Focus quadrant are not being valued by many organisations but could have strategic value. Project management, also in the management realm, might not seem as at the heart of cybersecurity programs as risk management, but it's just as essential for the successful execution of cybersecurity programs. The reason why many initiatives fail is not necessarily because of the deficiency of technical content, but because of poor coordination, scheduling, or stakeholder management.

Root cause analysis is a cognitive skill and is worthy of special attention. It is a bit surprising where it falls in the Out of Focus quadrant as it is a key component in incident learning, reliability engineering, and continuous improvement. This may reflect an organization's culture and practice of investigations as compliance work, instead of a learning opportunity for a system. In all the literature on high reliability organizations, it is always stated that the ability to conduct effective root cause analysis is a key contributor to resilient operations.

Technology is highlighted with PLC programming. While not every cyber security practitioner needs to have an extensive understanding of programming, those with such skills will have a unique advantage when they're looking at how attackers can manipulate logic controllers. Global citizenship (under ethics) refers to a greater understanding of geopolitics and society. Although this competency is at the margins of relevance now, as cyber threats become more closely linked to nation state activity and greater interdependency of supply chains, it could increase in significance. The positioning of these skills needs to be understood well. Don't mistake low demand with low value and history shows that some backside skills could be the ones to become prominent in the future.

7. THE RELATIONSHIP BETWEEN ESSENTIALNESS AND DEMAND

An important nuance in the framework is that essentiality does not necessarily go hand in hand with demand. The two dimensions are interrelated in different ways in each quadrant. In the Core Skills

quadrant, high essentialness and high demand signal chronic pressures with a supply consistently falling behind demand. High essentialness combined with stable demand (typical of the Steady Skills quadrant) indicates that there are areas where supply has matured. Low essentialness/High demand (Emerging Skills quadrant) refers to areas where organizations are investing in areas that are not widely recognized yet. Areas of low essentialness and low demand, like the Out of Focus quadrant, indicates areas that may need a reassessment or are at risk of erosion.

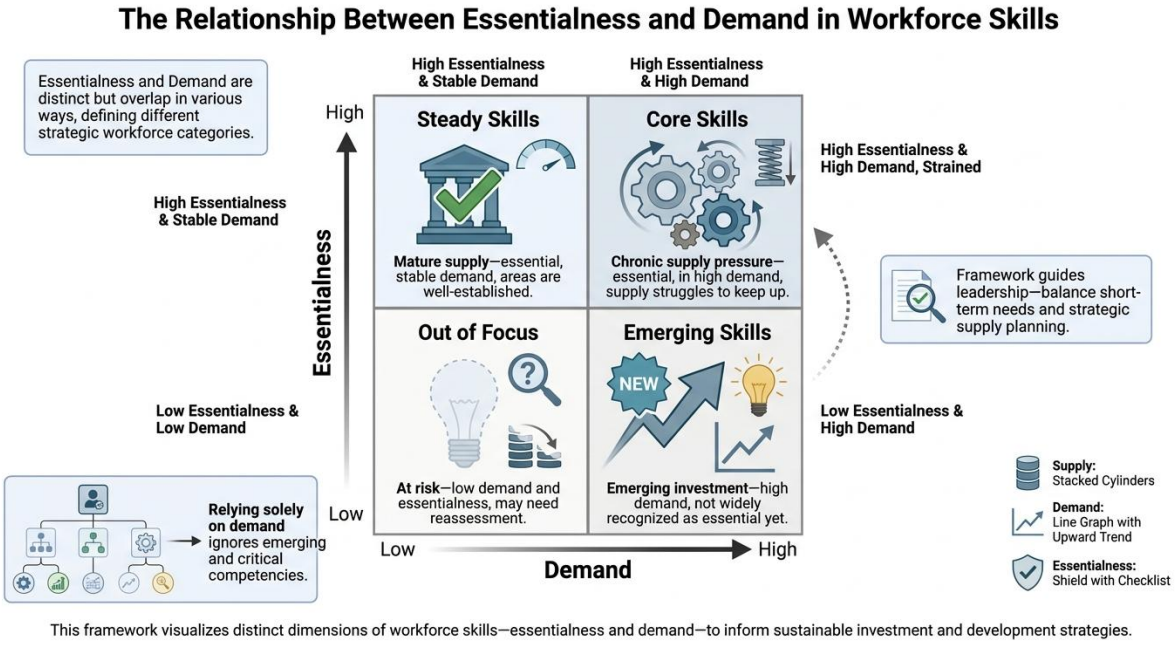

Fig -6: The Relationship Between Essentialness and Deman in Workforce Skills

There are practical implications in this decoupling. Only relying on visible demand signals for workforce strategies can result in under investing in the capabilities that are emerging and ignore the importance of competencies that are not discernible. The framework is a corrective lens, thus pushing leaders to consider both short-term needs and strategic positioning.

8. CHALLENGES IN BUILDING OT CYBERSECURITY CAPABILITY

Even with the clarity of frameworks like this, organisations still face some challenges in making the frameworks work. There are five levels of difficulty.

The first challenge is associated with the cultural gap between IT and OT teams. Each of these groups may have differing priorities, jargon, and risk tolerances. Historically the IT teams have focused on confidentiality and on quick patching, the OT teams on availability and safety and operational continuity. Creating shared understanding is not something that just happens it takes time and effort, such as shared training, governance, and collaboration mechanisms.

The second challenge relates to legacy infrastructure. Many industrial facilities have equipment that has been running for decades with no security factors considered. The application of modern controls on top

of these systems requires ingenuity, a thorough understanding of engineering controls and an appreciation for the measures that must be taken to compensate.

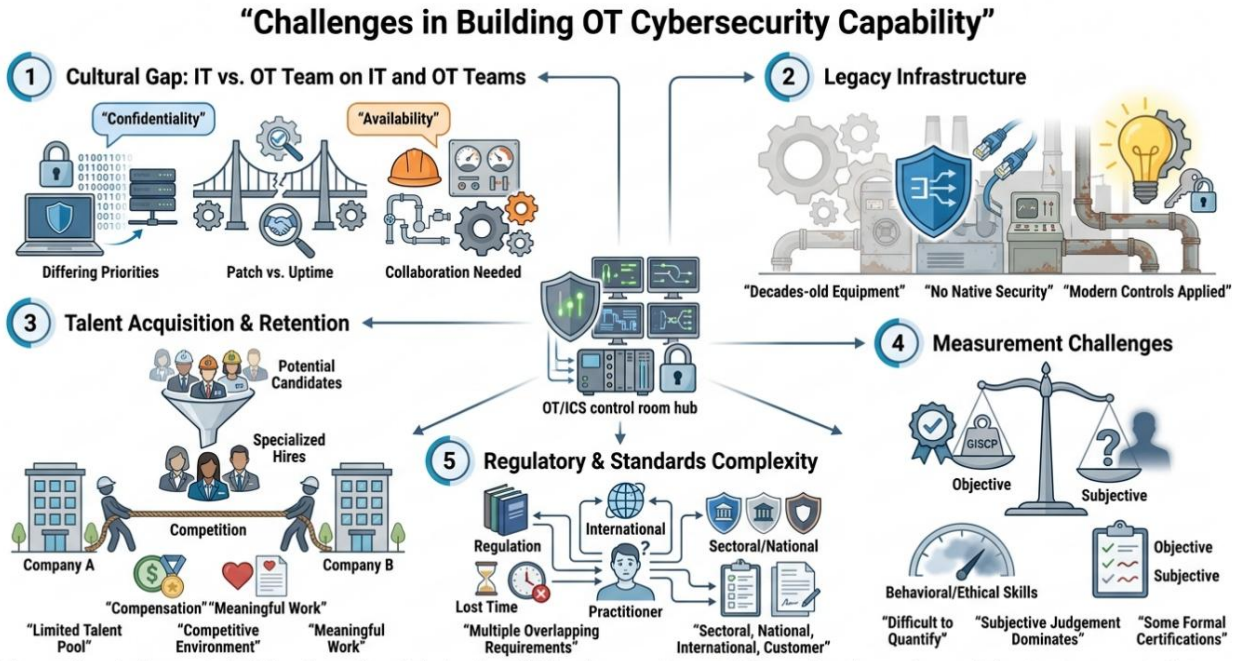

Figure: Key challenges in building Operational Technology (OT) cybersecurity capability—cultural gaps, legacy infrastructure constraints, talent shortages, measurement difficulties, and regulatory complexity—all must be addressed for successful application of frameworks.

Fig -7: Challenges in Building OT Cybersecurity Capability

Talent acquisition and retention is the third challenge. Competition for cybersecurity talent makes it a costly endeavor, and more specifically, OT positions further limit the talent pool. Retention is directly tied to the mission of the framework and the self-efficacy theme, as well as competitive compensation and meaningful work, which is connected to the mission and self-efficacy themes.

This fourth challenge is around measurement. It is still difficult to quantify skill levels and capability maturity especially for behavioural and ethical skills. Some structure is provided by certifications like the Global Industrial Cyber Security Professional, but subjective judgment and informal evaluation are the basis for much of the assessments.

The fifth challenge involves complexity of regulatory and standards issues. Practitioners need to deal with the requirements of sectoral bodies, national schemes and international standards and customer specific requirements. This complexity takes time and focus away from doing the things that defend.

9. SOLUTIONS AND STRATEGIC PATHWAYS

Solutions to these challenges must be undertaken at several levels.

On an individual basis practitioners gain from self-evaluation with purpose and structure to plan their development. Using the quadrant scheme can be a starting point for people to recognise their strengths and development needs before going on to formal learning, practical experience, training, mentoring, and exposure to working environments. Reflective practice (journaling, peer review and after action analysis) is used to deepen learning, as opposed to passively consuming training material.

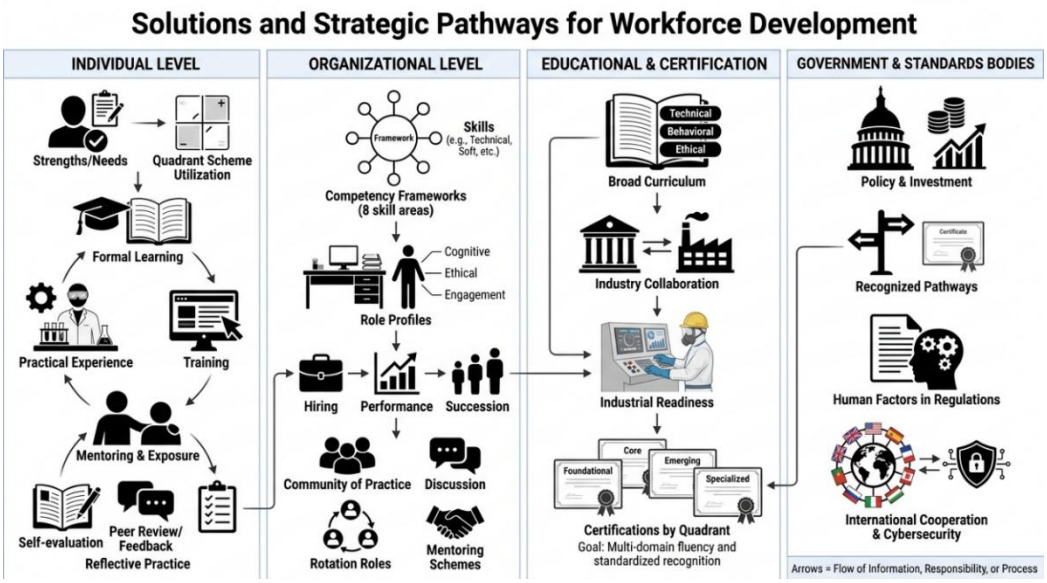

Fig -8: Solutions and Strategic Pathways for Workforce Development

Organisational level All eight skill areas should be incorporated into building competency frameworks to prevent technology only approaching the field that has historically occurred. Organizations can create role profiles that explicitly consider cognitive, ethical and engagement traits and they can consider these as part of the hiring, performance management, and succession planning process. Mentoring schemes, communities of practices and rotation roles help to speed up learning and decrease reliance on a few key experts.

In the educational and certification aspect, the subject matter of a curriculum should include behavioral and ethical knowledge in addition to technical knowledge. Universities and training providers can work together with industry for graduates to be fluent in an industrial setting understand control systems, field and operational decision making. The certifications can be developed to align with the four quadrants and there can be different trajectories for foundational, core, and emerging competencies. Governments and standards bodies can help develop the workforce at the policy level by investing in training, recognizing training pathways, and incorporating human factors into their regulatory requirements. International cooperation is now and with increasing significance a necessity, as critical infrastructure is more reliant on cross border value chains and shared threat intelligence.

10. IMPLICATIONS FOR WORKFORCE DEVELOPMENT

The figure has five key implications for the OT cybersecurity workforce development.

Firstly, holistic competency models are now of utmost importance. Focusing on cybersecurity as just a technical certification de-credentializes the profession and creates practitioners that lack the skills to work in senior level positions.

Second, it is safety that acts as the gravitational center of OT cybersecurity. The positioning of safety at the top-right corner of the figure reinforces that the discipline is not about the integrity of data; it's all about human life and physical processes.

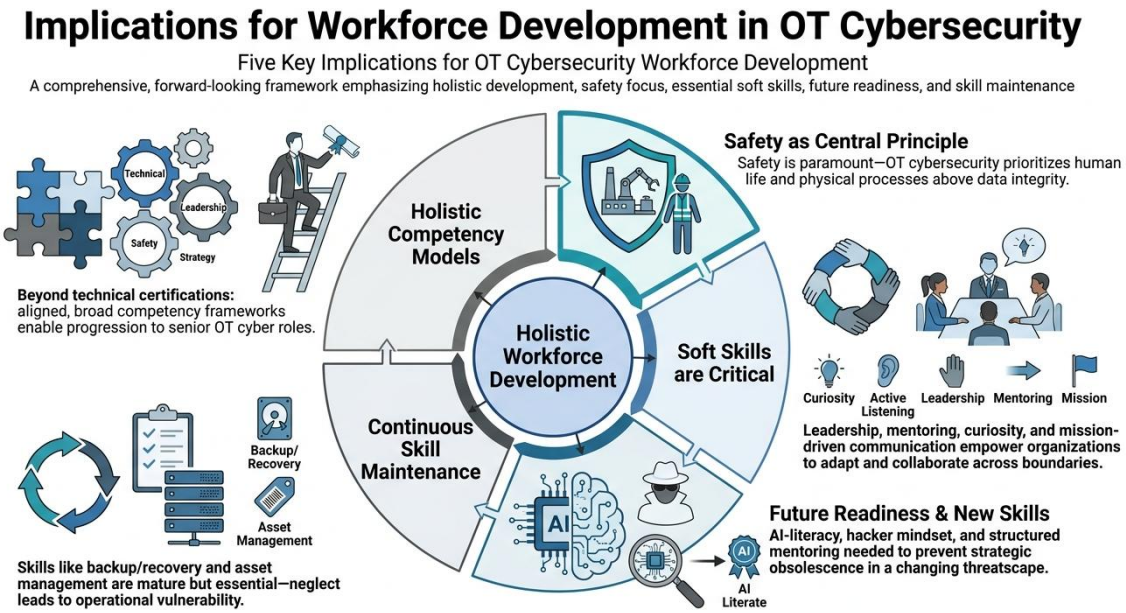

Fig -9: Implications for Workforce Development in OT Cybersecurity

Third, Soft skills are not soft. Critical points in the framework are Leadership, Mentoring, Mission, Active Listening and Curiosity. These skills help people work between organizational lines, remain motivated when under pressure and adjust to the changing threats.

Fourth, future readiness is based on new skills. As artificial intelligence grows, skills like AI literacy, a hacker mentality, and structured mentoring are crucial for organizations to avoid strategic obsolescence.

Fifthly, Continuous maintenance of the skills is needed, and not neglect. However, the leveling off demand for skills like backup or recovery, and for asset management, is not a sign of a fading skill but simply indicates that the skill is mature in the supply market. These skills are essential and if not used will be lost and will compromise operational resilience.

These implications indicate a more comprehensive, purposeful, and forward-looking approach to workforce development.

11. RECOMMENDATIONS FOR PRACTITIONERS, ORGANIZATIONS, AND WORKFORCE PLANNERS

The framework provides a clear, explicit, and systematic pathway for practitioners to engage with professional development. Persons can start with self-assessment and grade themselves for each skill and then determine 2 or 3 priority areas in the various quadrants. By making a conscious effort to invest in new skills like AI and ML literacy, hacker mindset, and listening, practitioners can set themselves up for future opportunities. Senior leaders know that they must build cognitive and self-efficacy competencies such as systems thinking, creative thinking, and motivation to make them more than just technically competent and narrowly focused contributors.

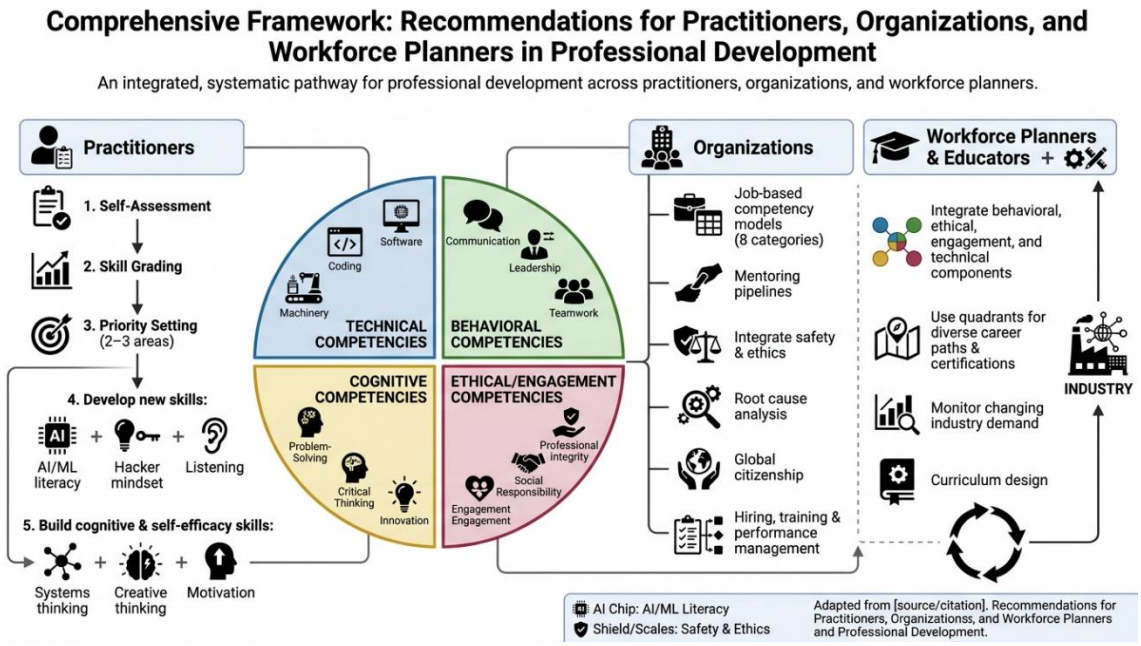

Fig -10: Recommendations for Practitioners, Organizations, and Workforce Planners

The framework can help organizations with their hiring, training, and performance management. When competency models are based on jobs and related to all eight categories instead of technology they provide a more accurate view of the competency requirements of jobs. Creating mentoring pipelines not only helps alleviate the shortage of workers, but it helps pass along knowledge from one generation to another. Incorporating safety and ethics into cybersecurity training, instead of as a distinct coursework, helps to remind people of the protective nature of cyber. Skills like root cause analysis and global citizenship can be underutilized and might present new avenues for developing capability.

Workforce planners and educators use the behavioral, ethical, and engagement components in the curriculum along with the technical components to help prepare students for the realities of the OT environment. There are various career paths with the four quadrants that lead to certification. Consultation with industry to monitor changes in demand patterns means that the framework is responsive to changes.

12. FUTURE PROSPECTS OF THE FRAMEWORK

There are several events that will impact the future development of the framework. As a defensive measure, artificial intelligence will continue to grow in importance in OT cybersecurity, and as an attack surface, it will assume an even greater importance. Practitioners will require skills in adversarial machine learning, ethical AI governance, and model validation in critical decisions as models get integrated.

The threat of landscape will change due to geopolitical pressure. Increased sophistication and frequency of state sponsored cyber operations against critical infrastructure, and a multitude of supply chain risks across the globe. The Out of Focus quadrant might be shifting some skills towards the centre, such as skills for global citizenship, intelligence analysis, and cross border coordination.

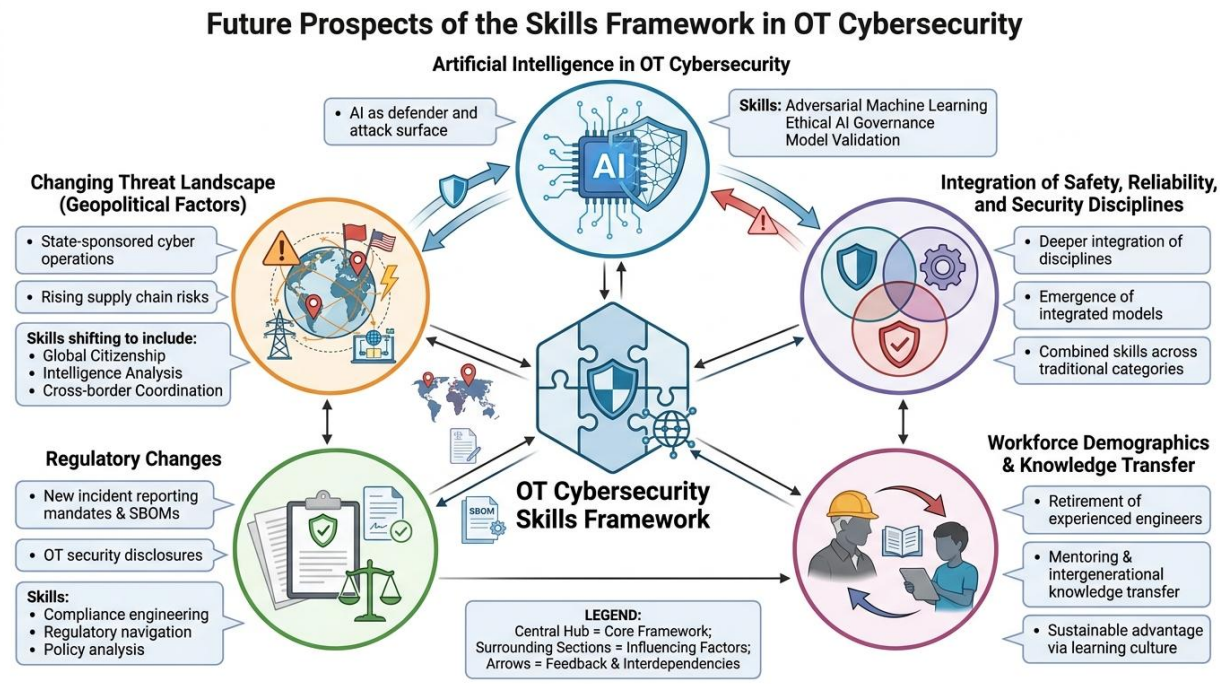

Fig -11: Future Prospects of the Skills Framework in OT Cybersecurity

Demand will remain to be driven by regulatory change. How organizations allocate resources and what skills they need will be impacted by new regulations for incident reporting, software bill of materials, and operational technology security disclosures. Those who can navigate regulatory issues, manage compliance engineering, and analyse policies will be increasingly valuable.

The makeup of the workforce will also shape the framework. The need for mentoring and planned knowledge transfer will increase as more experienced engineers retire. Those organizations that can create a learning culture and intergenerational collaboration will have a sustainable advantage over those that rely on the 'transactional' approach for hiring.

Finally, the embedding of safety, reliability and security disciplines are likely to become deeper. The divide between these functions has resulted in inefficiencies and gaps and Integrated Models that integrate process safety, functional safety and cybersecurity are taking hold. Future skills frameworks may combine skills that are currently found in several skills categories.

13. GAPS IN THE LITERATURE AND AREAS FOR FURTHER RESEARCH

While OT cybersecurity guidance has matured, there are still several research gaps. There is a lack of empirical research on the effectiveness of specific training interventions and most evidence is anecdotal and vendor produced. Likewise, there is a lack of research that correlates models of workforce competencies with actual security outcomes. Although the behavioural and ethical aspects of cybersecurity are becoming increasingly acknowledged, there are not yet sufficiently well-developed assessment tools which are applicable for industrial settings.

Additional studies might focus on organizations' efforts to measure progress in relation to multidimensional skills frameworks, mentoring relationships and capability transfer, and cross-

disciplinary working and its impact on security and safety. Some studies that could be compared between sectors, geographies, and organisational sizes would also be good in terms of providing the empirical basis of the field.

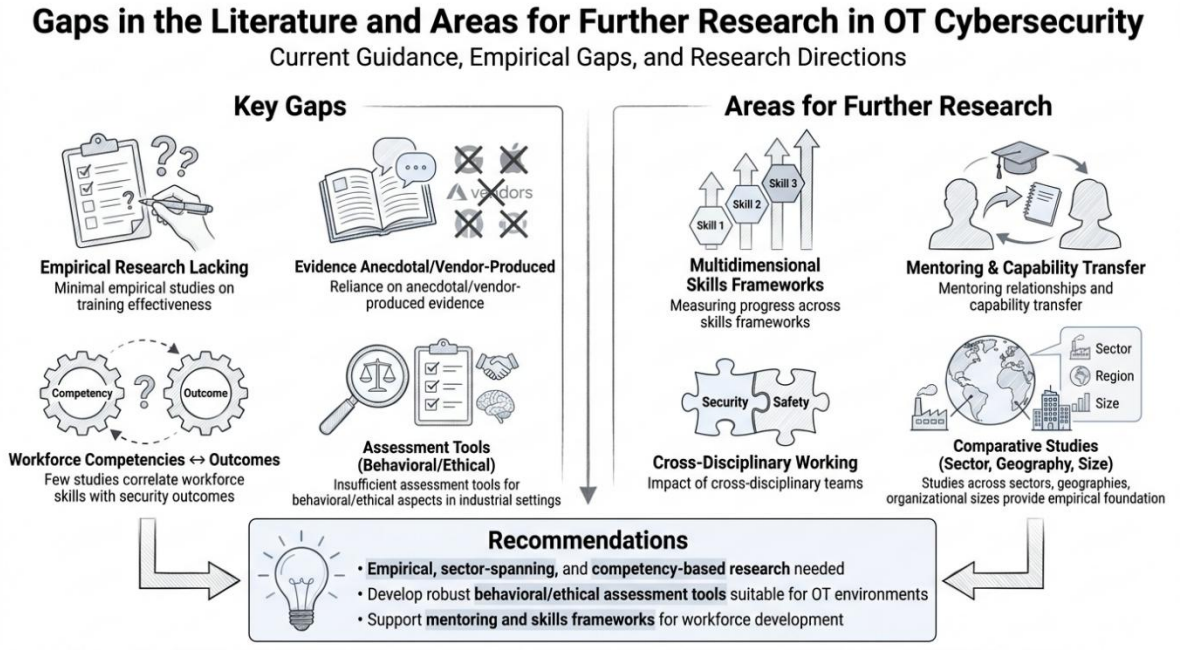

Fig -12: Gaps in the Literature and Areas for Further Research in OT Cybersecurity

14. CONCLUSION

More than just a visual taxonomy of skills, the framework Skills to Level Up OT Cybersecurity is a framework that supports prioritization. It reflects a philosophy of strategy on the discipline's future development to address the increasing risk in industry. The model shows the multidimensional, human-centered, and future-oriented nature of modern OT cybersecurity work by portraying twenty four skills along two axes and eight categories. Practitioners who use the framework as a personal development tool can create purposeful plans for growth that integrate what they have learned to operate within with what they need to be prepared for. Focusing on workforce strategies based on essentialness and demand can help organizations steer clear of optimizing based on only the visible market signals. Teachers and certifies who include the aspects of behaviour, ethics, and engagement in the programs they deliver can create learners who will be more ready for the industrial world. The final words that the figure gives are not just pep talking, but operational. In an industry where the failure to build strengths and continually improve weaknesses is not an option, the consequences of failure are the potential harm to people, ecosystems, and societal stability. The framework provides a viable and orderly way forward.

REFERENCES

[1] Gartner. (2024). Hype Cycle for Security Operations, 2024. [online] Available at: https://www.gartner.com/en/documents/5622491.

[2] Ellinas, G., Panayiotou, C., Kyriakides, E., & Polycarpou, M. (2015). Critical infrastructure systems: Basic principles of monitoring, control, and security. Studies in Computational Intelligence. https://doi.org/10.1007/978-3-662-44160-2_1
[3] Fischer, P. J. (2022). A cybersecurity skills framework. Research Anthology on Advancements in Cybersecurity Education. https://doi.org/10.4018/978-1-6684-3554-0.ch010
[4] George, R. (2008). Critical infrastructure protection. International Journal of Critical Infrastructure Protection, 1, 4-5. https://doi.org/10.1016/j.ijcip.2008.08.010
[5] Radvanovsky, R., & Mustard, S. (2026). Continuous improvement in OT cybersecurity. Risk Management for Operational Technology (OT) Systems. https://doi.org/10.4324/9781003610557-11
[6] Ramezan, C., Coffy, P., & Lemons, J. (2023). Building the operational technology (OT) cybersecurity workforce: What are employers looking for?. Journal of Cybersecurity Education Research and Practice, 2024(1). https://doi.org/10.32727/8.2023.31
[7] Schubert, M. (2008). Enterprise integration. Nagios 3 Enterprise Network Monitoring. https://doi.org/10.1016/b978-1-59749-267-6.00006-1
[8] Simuth, J. (2015). E-learning tool for improving managerial strategic thinking skills. Procedia - Social and Behavioral Sciences, 197, 703-706. https://doi.org/10.1016/j.sbspro.2015.07.072
[9] (2017). Assessing non-technical skills. Safety at the Sharp End. https://doi.org/10.1201/9781315607467-11
[10] (2020). Overview of the skills-based model. Counselling Skills in Action. https://doi.org/10.4135/9781036232511.n2
[11] Bazyak, G. V. (2025). STAFFING SHORTAGE IN THE RUSSIAN IT SECTOR: PROBLEMS AND SOLUTIONS THROUGH THE INTERACTION OF BUSINESS AND PROFESSIONAL EDUCATION. STAFFING SHORTAGE IN THE RUSSIAN IT SECTOR: PROBLEMS AND SOLUTIONS THROUGH THE INTERACTION OF BUSINESS AND PROFESSIONAL EDUCATION. https://doi.org/10.46916/10122025-978-5-00215-943-7
[12] Hashim, H., & Haron, Z. A. (2007). A study on industrial communication networking: Ethernet based implementation. 2007 International Conference on Intelligent and Advanced Systems. https://doi.org/10.1109/icias.2007.4658557
[13] Iturbe, E., Rios, E., Mansell, J., & Toledo, N. (2023). Information security risk assessment methodology for industrial systems supporting ISA/IEC 62443 compliance. 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). https://doi.org/10.1109/icecet58911.2023.10389369
[14] Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society. https://doi.org/10.1109/iecon.2011.6120048
[15] Knapp, E. D., & Langill, J. T. (2015). Industrial cyber security history and trends. Industrial Network Security. https://doi.org/10.1016/b978-0-12-420114-9.00003-4
[16] Knapp, E. D. (2024). Industrial cybersecurity history and trends. Industrial Network Security. https://doi.org/10.1016/b978-0-443-13737-2.00009-9
[17] Krishna Parimala, V. (2024). Introductory chapter: Anomaly detection – recent advances, AI and ML perspectives and applications. Artificial Intelligence. https://doi.org/10.5772/intechopen.113968
[18] Patterson, W., & Winston-Proctor, C. E. (2020). Behavioral cybersecurity. Behavioral Cybersecurity. https://doi.org/10.1201/9781003052029-2
[19] Radvanovsky, R., & Mustard, S. (2026). Continuous improvement in OT cybersecurity. Risk Management for Operational Technology (OT) Systems. https://doi.org/10.4324/9781003610557-11
[20] Soest, H. V. (2025). Cybersecurity in the european electricity system: The role of the NIS2 directive. European Energy Law Report, 345-362. https://doi.org/10.1017/9781839704635.016
[21] Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in ukraine show the vulnerability of the U.S. power grid. The Electricity Journal, 30(3), 30-35. https://doi.org/10.1016/j.tej.2017.02.006
[22] (2015). Session 1: Industrial control systems. 2015 World Congress on Industrial Control Systems Security (WCICSS). https://doi.org/10.1109/wcicss.2015.7420315
[23] КОВТУН И, И. (2023). METHODOLOGY FOR INFORMATION SECURITY RISKS ASSESSING AT THE PROCESS OF INDUSTRIAL PRODUCTION AUTOMATION. Приборы и системы. Управление, контроль, диагностика. https://doi.org/10.25791/pribor.11.2023.1454
[24] Crilly, N. (2026). Critical thinking, creative thinking, systems thinking and many more: A comparative bibliometric analysis of prevalence and distribution. Thinking Skills and Creativity, 59, 102014. https://doi.org/10.1016/j.tsc.2025.102014
[25] Fischer, P. J. (2022). A cybersecurity skills framework. Research Anthology on Advancements in Cybersecurity Education. https://doi.org/10.4018/978-1-6684-3554-0.ch010

[26] Tariq, M. U. (2025). Micro-credentials for workforce development. Transforming the Workforce With Microcredentials. https://doi.org/10.4018/979-8-3373-2257-5.ch004
[27] Whiting, A. (2020). Constructing cybersecurity. Constructing cybersecurity. https://doi.org/10.7765/9781526123336.00009
[28] (2007). The africa competitiveness report 2007. Geneva: World Economic Forum. https://doi.org/10.1596/978-92-95044-03-6
[29] (2016). A focus on cybersecurity. https://doi.org/10.7249/cp871
[30] (2026). Peer review report for: Youth employment preferences in rwanda and sierra leone: A constrained comparative secondary analysis [version 1; peer review: 2 approved]. https://doi.org/10.21956/openresafrica.17718.r34614
[31] (2026). Overview of the ISA/IEC 62443 series. Security PHA Review for Consequence-Based Cybersecurity, 19-24. https://doi.org/10.1002/9781394442447.ch2
[32] Block, C., Bauer, T., & Henkel, F. O. (2014). Seismic qualification of equipment in industrial facilties. Seismic Design of Industrial Facilities. https://doi.org/10.1007/978-3-658-02810-7_22
[33] Johnson, D. (2024). Cybersecurity collaboration and international cooperation. Leadership Fundamentals for Cybersecurity in Public Policy and Administration. https://doi.org/10.4324/9781003496250-7
[34] Joseph, A., Ileleji, T., & Joseph, M. (2021). CYBERSECURITY TALENT SHORTAGE: GENDER AND ETHNIC/RACIAL DIVERSITY. EDULEARN Proceedings. https://doi.org/10.21125/edulearn.2021.1936
[35] MacDonald, S. (2019). An avid OT ambassador. BDJ Team, 6(3), 32-33. https://doi.org/10.1038/s41407-019-0006-9
[36] Makinde, O. F. (2026). Cybersecurity and data protection. Legal and Ethical Challenges in Data Privacy Rights and Cybersecurity. https://doi.org/10.4018/979-8-3373-4967-1.ch008
[37] Torrey, K. (2026). Cloudsec-pro: Palo alto networks cloud security professional certification. https://doi.org/10.55277/researchhub.dlclyu81
[38] Yüksel Haliloğlu, E. (2021). Efficiency assessment of university-industry collaboration. Advances in Higher Education and Professional Development. https://doi.org/10.4018/978-1-7998-3901-9.ch008
[39] (2013). Situated reflective practice. Reflective Practice in Education and Training. https://doi.org/10.4135/9781526402134.n9
[40] (2017). The U.S. federal government initiatives on cybersecurity research. Threat Level Red. https://doi.org/10.1201/9781315167558-1
[41] (2018). FRAMEWORK PROFILES. NIST Cybersecurity Framework. https://doi.org/10.2307/j.ctv4cbhfx.7
[42] Al Alawi, N. (2025). Evergreen OT security assurance: A sustainable approach to OT cybersecurity risk management. SPE Conference at Oman Petroleum & Energy Show. https://doi.org/10.2118/224964-ms
[43] Bendiek, A., & Pander Maat, E. (2021). The eu's cybersecurity policy: Building a resilient regulatory framework. Cybersecurity and Legal-Regulatory Aspects. https://doi.org/10.1142/9789811219160_0002
[44] Bishop, G. (2025). Threat landscape and cybersecurity culture. Cybersecurity Culture. https://doi.org/10.1201/9781003368496-3
[45] Fischer, P. J. (2022). A cybersecurity skills framework. Research Anthology on Advancements in Cybersecurity Education. https://doi.org/10.4018/978-1-6684-3554-0.ch010
[46] Göhler, V. (2025). Critical or confident? AI literacy and student–ai collaboration in higher education. Proceedings of the 26th ACM Annual Conference on Cybersecurity & Information Technology Education. https://doi.org/10.1145/3769694.3771145
[47] Hozza, D. (2024). Entering the cybersecurity workforce: Certification vs. college degree. Innovative Practices in Teaching Information Sciences and Technology. https://doi.org/10.1007/978-3-031-61290-9_16
[48] Musser, M. (2023). Adversarial machine learning and cybersecurity. https://doi.org/10.51593/2022ca003
[49] Radvanovsky, R., & Mustard, S. (2026). Continuous improvement in OT cybersecurity. Risk Management for Operational Technology (OT) Systems. https://doi.org/10.4324/9781003610557-11
[50] rofymenko, O., Savielieva, O., Prokop, Y., Loginova, N., & Dyka, A. (2023). SOFT SKILLS FOR SOFTWARE DEVELOPERS. Cybersecurity: Education, Science, Technique, 3(19), 6-19. https://doi.org/10.28925/2663-4023.2023.19.619
[51] Sarker, I. H. (2024). AI for enhancing ICS/OT cybersecurity. AI-Driven Cybersecurity and Threat Intelligence. https://doi.org/10.1007/978-3-031-54497-2_8

[52] Singh, T. (2025). Operational resilience and business continuity planning. Digital Resilience, Cybersecurity and Supply Chains. https://doi.org/10.4324/9781003604969-2
[53] Tripathi, A. (2025). Cybersecurity skill gap in india. Journal of Advanced Research in Electronics Engineering and Technology, 12(1&2), 145-149. https://doi.org/10.24321/2456.1428.202520
[54] (2020). Remedies against state-sponsored cyber operations. Cyber Operations and International Law, 379-492. https://doi.org/10.1017/9781108780605.013
[55] (2021). Cybersecurity for the future. Cybersecurity. https://doi.org/10.7551/mitpress/11656.003.0010
[56] (2023). Emerging trends in AI skill demand across 14 OECD countries. OECD Artificial Intelligence Papers. https://doi.org/10.1787/7c691b9a-en
[57] George, D., & George, A. (2025a). Transforming Healthcare with Artificial Intelligence: Strategies, Insights, and Frameworks for Innovation. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15685381
[58] (2025). Establishing a regulatory change management program. The Cybersecurity Control Playbook, 449-452. https://doi.org/10.1002/9781394331888.app6
[59] 2022 ICS/OT Cybersecurity Year in Review Report | Dragos. (n.d.). https://hub.dragos.com/ics-cybersecurity-year-in-review-2022
[60] George, D. (2025c). The Dual Partnership Future How Artificial Intelligence is Redefining Intimacy, Companionship, and the Institution of Marriage in the Digital Age. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15866401
[61] Bertone, F., Lubrano, F., & Goga, K. (2020). Artificial intelligence techniques to prevent cyber attacks on smart grids. Annals of Disaster Risk Sciences, 3(1). https://doi.org/10.51381/adrs.v3i1.42
[62] George, D. (2025b). India's multidimensional pathway to artificial intelligence supremacy. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14944290
[63] ISA/IEC 62443 Series of Standards | ISAGCA. (n.d.). https://isagca.org/isa-iec-62443-standards
[64] George, D. (2025a). Advancements in Artificial Intelligence for industrial robotics and Intelligent Drones: A Comprehensive review. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14911559
[65] ISC2. (2023). ISC2 Cybersecurity Workforce Study, 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
[66] George, D., & Dr.T.Baskar. (2025). Artificial intelligence transformation of digital interaction platforms and economic opportunity structures. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17147924
[67] Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9, 744. https://doi.org/10.3389/fpsyg.2018.00744
[68] George, D. (2024). The impact of IT/OT convergence on digital transformation in manufacturing. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.10895704
[69] George, D. (2026a). Architectural Convergence in Security Operations: a technical framework for AI-Augmented Threat Detection, Automated response, and Organizational cyber resilience. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19986642
[70] Holzbauer, J. (2026, May 12). OT Cybersecurity faces a skills gap | Nexus. Nexus. https://nexusconnect.io/articles/ot-cybersecurity-faces-a-skills-gap
[71] George, D. (2026d). Orbital Mirrors and Earthly Needs: A Multidimensional analysis of Space-Based Sunlight Redirection as a Transformative infrastructure technology. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19501167
[72] Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing Cybersecurity Challenges in Times of Crisis: Extending the sociotechnical systems perspective. Applied Sciences, 14(24), 11610. https://doi.org/10.3390/app142411610
[73] George, D. (2026c). Multi-Vendor firewall strategy: IT, OT, and edge networks. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19630402
[74] New study reveals gaps in common types of cybersecurity training - Department of Computer Science. (n.d.). Department of Computer Science. https://cs.uchicago.edu/news/new-study-reveals-gaps-in-common-types-of-cybersecurity-training/
[75] George, D. (2026b). IEC 62443 Wireless Security: Deploying OT wireless controllers in industrial factory networks. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19428491

[76]Knapp, E. D., & Langill, J. (2014). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress. https://pbio.akademia.mil.pl/wp-content/scans/2024/CYBERBEZPIECZENSTWO/OCR/26653_III_OCR.pdf

[77]Langner, R., The Langner Group, & Schneier, B. (2013). To kill a centrifuge. The Langner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[78]Papaphilippou, M., Moulinos, K., Theocharidou, M., European Union Agency for Cybersecurity, & Siemens. (2023). GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY. https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf

[79]Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, M., Computer Security Division, Information Technology Laboratory, Smart Connected Systems Division, Communications Technology Laboratory, & The MITRE Corporation. (2023). NIST SP 800-82R3 Guide to Operational Technology (OT) Security. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[80]World Economic Forum. (2023). Future of Jobs Report 2023. In Future of Jobs Report. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

[81]Beveridge, R. (2022). Effectiveness of increasing realism into cybersecurity training. Research Anthology on Advancements in Cybersecurity Education. https://doi.org/10.4018/978-1-6684-3554-0.ch028

[82]Bulda, O. (2019). «legal asymmetry»in the context of liability of the state and state-sponsored cyber attacks actors. Proceedings of the conference "Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks". https://doi.org/10.34054/bdc003

[83]De Marchi, M., Pomalo, M., Vallazza, R., Falcomatà, I., Aruväli, T., & Rauch, E. (2025). Enhancing IT/OT cybersecurity knowledge transfer through demonstrative workshops in cyber-physical production systems. Procedia Computer Science, 253, 2296-2305. https://doi.org/10.1016/j.procs.2025.01.290

[84]Kumar, T., & Kaur, S. (2023). Ethical aspects of cybersecurity in e-commerce. Cybersecurity for Decision Makers. https://doi.org/10.1201/9781003319887-19

[85]Prokop, D. J. (2017). Threats to supply chains. Global Supply Chain Security and Management. https://doi.org/10.1016/b978-0-12-800748-8.00003-0

[86]Radvanovsky, R., & Mustard, S. (2026). Continuous improvement in OT cybersecurity. Risk Management for Operational Technology (OT) Systems. https://doi.org/10.4324/9781003610557-11

[87]Ramezan, C., Coffy, P., & Lemons, J. (2023). Building the operational technology (OT) cybersecurity workforce: What are employers looking for?. Journal of Cybersecurity Education Research and Practice, 2024(1). https://doi.org/10.32727/8.2023.31

[88]Sarker, I. H. (2024). AI for enhancing ICS/OT cybersecurity. AI-Driven Cybersecurity and Threat Intelligence. https://doi.org/10.1007/978-3-031-54497-2_8

[89](2023). Process safety and cybersecurity. Towards Process Safety 4.0 in the Factory of the Future, 39-69. https://doi.org/10.1002/9781394226375.ch4