Post Event Summary Report

for

Trustworthy Systems in Distributed Manufacturing – The Future

30th September, 2024

Report Date:

17th October, 2024

Prepared by:

ACE-CSR Team at Warwick

Location:

University of Warwick, Coventry, United Kingdom

EXECUTIVE SUMMARY

On September 30, 2024, the University of Warwick hosted "Trustworthy Systems in Distributed Manufacturing – The Future," organised by ACE-CSR. The event gathered experts from academia and industry to discuss how Industry 4.0 is transforming manufacturing and the vital need to secure distributed manufacturing systems. As the industry becomes more connected and data-driven, relying heavily on artificial intelligence, the risks of cyberattacks and data breaches are increasing. The event aimed to explore how to address these risks while leveraging new manufacturing technologies.

Professor Carsten Maple from WMG and The Alan Turing Institute opened the event. He spoke about the shift toward data-driven manufacturing processes, noting that while this brings opportunities for greater efficiency and sustainability, it also introduces new vulnerabilities. In his presentation on cybersecurity in additive manufacturing supply chains, he introduced the RAMONA project. This initiative focuses on ensuring the authenticity and integrity of manufacturing artifacts using technologies like cryptographic anchors and homomorphic encryption.

A panel discussion followed with industry experts including Thomas Cornthwaite (COO of DiManEx), Tammy Archer (former CISO of Inchcape) and Professor Carsten Maple. They discussed current and future trends in trustworthy distributed manufacturing. Topics included building resilience into supply chains to detect disruptions and minimise downtime, protecting against counterfeit parts and ransomware attacks, and balancing operational flexibility with cybersecurity.

An interactive session allowed participants to share their insights through surveys and discussions. Key takeaways were that while distributed manufacturing offers benefits like increased resilience, flexibility, and efficiency, it also brings risks such as cybersecurity threats, quality control challenges, and trust issues within supply chains. Participants expect cyber threats to become more sophisticated over the next 5-10 years, requiring advanced defence strategies like AI-based security measures and zero-trust architectures.

In conclusion, the event highlighted the pressing need for better cybersecurity measures as distributed manufacturing grows. ACE-CSR is committed to collaborating with industry and academia to tackle these challenges. Next steps include organising workshops and publishing papers, enhancing research in areas like federated learning and anti-counterfeiting technologies, strengthening industry partnerships, and securing funding for collaborative projects. By focusing on practical solutions, ACE-CSR aims to improve the security and reliability of distributed manufacturing systems for the future.

TABLE OF CONTENTS

1. EVENT OVERVIEW

The University of Warwick recently hosted the "Trustworthy Systems in Distributed Manufacturing – The Future" event, organised by ACE-CSR. This event gathered experts from academia and industry to explore how manufacturing is changing with the rise of Industry 4.0 and how critical it is to secure distributed manufacturing systems. With increasing connectivity, data-driven processes, and the integration of artificial intelligence (AI), the risk of cyberattacks and breaches is becoming more prominent. This event aimed to foster dialogue on how to mitigate these risks while maximising the opportunities that new manufacturing technologies bring.

2. AGENDA

The event was held on the 30th of September, 2024 at the University of Warwick's campus. The details are as below:

Time	Session
14:00-14:15	Welcome and Opening Remarks
14:15-14:45	Presentation: Cybersecurity in Additive Manufacturing Supply Chains
14:45-15:45	Panel Discussion: Trustworthy Distributed Manufacturing – Current and Future Trends • Thomas Cornthwaite (COO, DiManEx) • Tammy Archer (Former CISO, Inchcape), • Professor Carsten Maple (Professor, WMG; Fellow, The Alan Turing Institute)
15:45-16:15	Coffee Break
16:15-17:15	Interactive Session with Q&A
17:15-17:30	Closing Remarks

3. KEY PRESENTATIONS

A. WELCOME SESSION: MANUFACTURING IN THE DIGITAL AGE

The event opened with remarks from Professor Carsten Maple, Head of Secure Cyber Systems at WMG and a Fellow at The Alan Turing Institute. He provided an overview of how Industry 4.0 is reshaping the manufacturing sector, highlighting the transition from traditional to data-driven processes. Professor Maple emphasised that this shift offers opportunities to enhance sustainability and efficiency, but also creates new vulnerabilities, especially as manufacturing becomes more distributed and dependent on digital systems.

B. CYBERSECURITY IN ADDITIVE MANUFACTURING SUPPLY CHAINS

Professor Maple continued with a detailed presentation on the role of cybersecurity in additive manufacturing supply chains. He introduced the RAMONA project, an EPSRC-funded initiative designed to ensure the authenticity and integrity of both physical and digital manufacturing artefacts. Key technologies discussed included cryptographic anchors and homomorphic encryption, which play crucial roles in safeguarding data and protecting against issues such as counterfeit parts and ransomware attacks.

- **Resilient Supply Chains:** Professor Maple stressed the importance of building resilience into supply chains to detect disruptions and minimise downtime.
- **Cryptographic Anchors:** These ensure the authenticity of assets, which is particularly important in industries like automotive and aerospace.
- **Homomorphic Encryption:** This method allows secure data sharing while preserving privacy, making it an essential tool for industries that require exchanging sensitive information.

4. PANEL DISCUSSION

The panel session, featuring experts Thomas Cornthwaite, Tammy Archer, and Professor Carsten Maple, explored the shift from centralised to distributed manufacturing systems and the rising cybersecurity challenges that accompany this transition. The panellists emphasised the importance of collaboration between academia, industry, and governments in tackling these risks. They discussed the transformative potential of emerging technologies such as AI, quantum computing, and edge computing, highlighting the need for robust cybersecurity measures to protect sensitive data and ensure trust across supply chains. The session reinforced the idea that securing distributed manufacturing will be a critical focus for the future.

5. INTERACTIVE SESSION WITH SURVEY FINDINGS

The interactive session provided participants with an opportunity to engage in a Q&A and share their perspectives through survey questions. Key insights from the session include:

A. BENEFITS OF DISTRIBUTED MANUFACTURING OVER DECENTRALISED MANUFACTURING

When respondents reflected on the **benefits** of distributed manufacturing, several common themes emerged, showcasing a variety of positive attributes that distinguish it from decentralised manufacturing.

- **Resilience** emerged strongly, with multiple mentions highlighting its ability to adapt to disruptions and maintain continuity.
- **Flexibility** was frequently noted, indicating adaptability in meeting diverse manufacturing needs.
- **Speed and efficiency** were also highlighted, with terms like fast, speed, and agile suggesting the capacity for quicker production cycles.
- **Environmental benefits** were raised, with sustainability mentioned as a key factor.
- **Security and privacy** were noted as potential strengths, particularly in intelligent manufacturing environments.

B. RATING OF BENEFITS IN THE NEXT 5-10 YEARS

Participants expect that distributed manufacturing will bring **significant benefits** over the next 5-10 years, particularly in terms of **efficiency** and **cost savings**. However, a substantial portion of respondents felt that these benefits might be **limited** due to **technological and operational challenges**. The optimistic minority foresees **substantial long-term gains**, especially in industries where customisation and localised production play critical roles.

C. RISKS OF MOVING TO DISTRIBUTED MANUFACTURING

Respondents identified a wide range of risks associated with the transition to distributed manufacturing, especially concerning security and control.

- **Security** risks dominated, with mentions of cyberattacks, IP theft, data breaches, and privacy concerns.
- **Quality control** emerged as another major risk, with issues around maintaining standards and preventing counterfeit or poor-quality products.
- **Intellectual property (IP)** risks were cited frequently, reflecting concerns about theft or infringement in distributed networks.
- **Coordination complexity** and **compliance** with regulatory standards were highlighted, indicating challenges in managing and enforcing consistency across distributed systems.
- **Higher costs** and concerns about **skills gaps** and **training** also appeared, suggesting potential financial and human resource challenges.

D. CHANGE IN RESILIENCE OVER THE NEXT 5-10 YEARS

Most participants agreed that distributed manufacturing would likely result in a **moderate increase in resilience**, allowing companies to better manage **supply chain disruptions** and improve **redundancy**. A smaller group predicted a **substantial increase**, emphasising the advantages of being able to localise production and adapt to changing conditions. A few respondents, however, expressed concerns that the added complexity of managing a distributed system could actually reduce resilience in some cases.

E. TRUST ISSUES IN FUTURE SUPPLY CHAINS

Several **trust-related concerns** were raised, with many revolving around the integrity of materials, data, and suppliers.

- **Material validation** was a key issue, with respondents questioning how to ensure that materials meet required standards.
- **Supplier reliability** and the **chain of trust** were highlighted, with concerns about verifying third-party partners.
- **IP protection** was frequently noted, with worries about intellectual property theft and confidentiality.
- **Transparency and accountability** issues were also raised, focusing on the ability to trace and validate actions across the supply chain.

F. CHALLENGES IN ENSURING QUALITY AND SECURITY WITH REMOTE PARTNERS

Trust was the dominant issue when considering how to ensure quality and security with remote manufacturing partners.

- **Trust** was overwhelmingly the most cited issue, affecting every aspect of remote collaboration.
- **Supplier processes** were mentioned, with concerns about ensuring partners maintain high standards.
- **Enforcing compliance** was also highlighted, particularly the difficulty of ensuring adherence to standards remotely.
- Other mentions include **network segmentation** and **oversight**, both indicating a need for stronger control mechanisms.

G. BALANCING OPERATIONAL FLEXIBILITY AND CYBERSECURITY RESILIENCE

When considering how manufacturers can balance **flexibility** with **cybersecurity resilience**, opinions varied but leaned towards security prioritisation.

- Most advocated for **building robust security frameworks**, even at the cost of some flexibility.
- Several respondents believed that **trade-offs are inevitable**, acknowledging the difficulty of balancing both aspects.
- A few supported **prioritising flexibility** with reactive security measures.
- Others suggested **specific security contracts** and **scalable digital infrastructure** as alternative approaches.

H. EVOLUTION OF ATTACKS AND ATTACKERS

There was a consensus that cyber threats will become more sophisticated over the next 5-10 years, with **AI-driven attacks** and **state-sponsored threats** expected to play a prominent role.

- **AI-based attacks** were frequently mentioned, with predictions that **AI** will be a key tool for both attackers and defenders.
- **Geopolitical influences** were noted, with concerns about state-sponsored attacks.

- **Cyber warfare** and **supply chain attacks** were highlighted, particularly in scenarios where competitors could exploit vulnerabilities.
- **Device vulnerabilities** and **insider threats** were also expected to grow in prominence.

I. FUTURE DEFENCE MECHANISMS

Defensive strategies were expected to become increasingly **AI-driven**.

- **AI-based defences** were the most frequently mentioned solution, seen as essential for countering evolving threats.
- **Zero trust architecture** was highlighted as a robust framework to ensure tighter security.
- **Collaboration frameworks** were also seen as critical, particularly for **educating people** and fostering better cooperation.
- **Network segmentation** and **adaptive defences** were noted as key strategies to mitigate potential attacks.

J. RESEARCH AND DEVELOPMENT PRIORITIES

- **Federated learning** was frequently mentioned, alongside **anti-counterfeit technologies**.
- **Quantum encryption** and **privacy-preserving techniques** were also noted as cutting-edge developments.
- **AI assurance** and **MBDE (Model-Based Digital Engineering)** were mentioned as research areas contributing to improved resilience.
- **Threat intelligence** and **data science** were key components of future development.

K. NEXT STEPS FOR COLLABORATION IN TRUSTWORTHY MANUFACTURING

When considering the next steps for collaboration, respondents largely favoured **interactive and knowledge-sharing events**.

- **Workshops** were the most popular suggestion, with respondents indicating a preference for hands-on, practical collaboration involving industry and academia.
- **Seminars** and **white papers** were also mentioned, with respondents seeing value in more structured knowledge dissemination efforts.
- **Collaborations and working groups** to summarise challenges and propose solutions were also seen as important for future progress.

L. CONTRIBUTIONS TO THE TRUSTWORTHY MANUFACTURING AGENDA

When asked how they could contribute to advancing the **trustworthy manufacturing agenda**, respondents provided various options.

- Many offered to **participate in proposals** and **collaborative efforts**, showing a willingness to engage in future projects.
- **Funding** for research, particularly for **digital twin models**, was offered by some respondents, indicating financial support for innovation.
- Others suggested **leading workshops** and **collaborating** with their industry use cases, demonstrating a commitment to shared learning and practical application of solutions.

6. CONCLUSION

The event underscored the increasing importance of cybersecurity in the context of distributed manufacturing. Participants acknowledged the benefits of transitioning to distributed models, but also raised concerns about the associated risks, particularly around cybersecurity and trust within supply chains. The discussions reinforced ACE-CSR's commitment to fostering collaborations between industry and academia to address these challenges. The need for further research, particularly in areas like AI-based threat detection, federated learning, and privacy-preserving technologies, was also highlighted.

7. NEXT STEPS FROM ACE-CSR AT WARWICK

Based on the discussions and insights from the event, the ACE-CSR at Warwick will prioritise several key areas:

- **Workshops and white** papers will be organised and produced to address specific challenges in distributed manufacturing, focusing on cybersecurity and supply chain resilience.
- **Research and development initiatives** will concentrate on federated machine learning, privacy-preserving AI, anti-counterfeiting technologies, and digital passports for product traceability.
- **Industry collaboration** will continue with partners, government bodies, and stakeholders to co-develop solutions that enhance the trustworthiness and security of distributed manufacturing systems.
- **Funding and collaboration opportunities** will be pursued to support joint initiatives aimed at advancing research and implementing security frameworks within distributed manufacturing.