

Research Skills 3

Task 9

Abdulaziz Alarfaj



Introduction

The cybersecurity of Operational Technology (OT) environments has become a major concern due to the increasing convergence between IT systems and industrial control systems. OT environments differ from traditional IT systems because they prioritize availability and safety over confidentiality, which limits the direct application of conventional cybersecurity controls (Research in the Arab context الحمادي، 2021، ص. 41). (41). Research in the Arab context indicates that the lack of dedicated OT cybersecurity governance frameworks increases the exposure of critical infrastructure to cyber threats (العتيبي، 2020، ص. 58؛ الزهراني، 2022، ص. 83؛ القحطاني، 2023، ص. 112). International studies emphasize that securing industrial control systems requires specialized risk management approaches tailored to operational constraints and safety requirements (Stouffer, 2015, p. 15). Kassner (2020, p. 72) further argues that OT cybersecurity governance must integrate technical, organizational, and human dimensions.

Several regional collaborative studies highlight the importance of aligning OT cybersecurity strategies with national critical infrastructure protection programs (السبيعي وآخرون، 2021، ص. 223؛ الحمد وآخرون، 2022، ص. 64). Likewise, international multi-author research confirms that effective OT cybersecurity depends on socio-technical coordination and sector-specific standards such as IEC 62443 (Boyes et al., 2018, p. 9; Imran et al., 2022, p. 11).

Single author

Arabic – single author (4)

الحمادي (2021)

العتيبي (2020)

الزهراني (2022)

القحطاني (2023)

Foreign – single author

Foreign – single author (2)

Stouffer (2015)

Kassner (2020)

Arabic – multiple authors

Arabic – multiple authors (2)

السبيعي وآخرون (2021)

الحمد وآخرون (2022)

Arabic – multiple authors

Arabic – multiple authors (2)

السبيعي وآخرون (2021)

الحمد وآخرون (2022)

Foreign – multiple authors

Foreign – multiple authors (2)

Boyes et al. (2018)

Imran et al. (2022)