Paper Title	Notes
Abuabed, Z., Alsadeh, A., & Taweel, A. (2023). STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles. *Computers & Security* , *133* , 103391.	The paper describes the application of STRIDE to assess threats to Advanced Driver Assistance Systems (ADAS) and mentions other threat modelling frameworks such as HEAVENS.
Ahn, B., Kim, T., Smith, S. C., Youn, Y. W., & Ryu, M. H. (2021, February). Security threat modeling for power transformers in cyber-physical environments. In *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-5). IEEE.	The paper describes a security modelling approach for power transformers in cyber-physical environments, including both threat and attack modelling. Notably, the authors distinguish between threat and attack modelling, and provide details on the respective approaches.
Alexander, O., Belisle, M., & Steele, J. (2020). MITRE ATT&CK for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA, 29.	The paper highlights four fundamental concepts behind the philosophy of ATT&CK for ICS design and usage: a.Maintain the adversary's perspective; b.Incorporate and refine based on real-world event activity, derived from empirical examples and incidents; c.Represent content with appropriate levels of abstraction, to effectively connect offensive behavior with potential countermeasures; d.Capture distinctions in offensive action at multiple levels, which may result in self-revealing or non-self-revealing failures; e.Underscore the failures and consequences that can arise from these adversary behaviors.
Almohri, H., Cheng, L., Yao, D., & Alemzadeh, H. (2017, July). On threat modeling and mitigation of medical cyber-physical systems. In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)* (pp. 114-119). IEEE.	The paper proposes a generic threat and trust model mapping cybersecurity threats and stakeholders e.g, untrusted patients etc. in an architecture, and to potentially decouple components to improve security.
Amro, A., Gkioulos, V., & Katsikas, S. (2023). Assessing cyber risk in cyber-physical systems using the ATT&CK framework. *ACM Transactions on Privacy and Security* , *26* (2), 1-33.	An example of a consequence-driven and cyber-informed approach to assessing cyber risk in cyber-physical systems, in the context of maritime systems. The approach uses Failure Modes Effects and Criticality Analysis (FMECA) and the ATT&CK framework.

Paper Title	Notes
Asif, M. R. A., & Khondoker, R. (2020). Cyber Security Threat Modeling of A Telesurgery System. In *2020 2nd International Conference on Sustainable Technologies for Industry* (Vol. 4, pp. 1-6).	The paper presents an example of applying STRIDE threat modeling to a telesurgery system.
Ayrour, Y., Raji, A., & Nassar, M. (2018). Modelling cyber-attacks: a survey study. *Network Security*, *2018*(3), 13-19.	Magazine article with a simple summary of the various threat models.
Bakirtzis, G., Ward, G., Deloglos, C., Elks, C., Horowitz, B., & Fleming, C. (2020, June). Fundamental challenges of cyber-physical systems security modeling. In *2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)* (pp. 33-36). IEEE.	Bakirtzis et al. highlighted that security modeling of CPS should be based on quantitative data instead of qualitative data, as this data and probabilistic approaches to cybersecurity are limited (thereby limiting the usefulness of quantitative data). They also highlighted the general omission of CPS challenges in threat modeling tools e.g. STRIDE.
Bernardi, S., Gentile, U., Marrone, S., Merseguer, J., & Nardone, R. (2021). Security modelling and formal verification of survivability properties: Application to cyber–physical systems. *Journal of Systems and Software*, *171*, 110746.	Bernardi et al. proposed a UML based approach to model survivability properties of CPS. The approach shares similar limitations as the previous paper.
Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis. *Threat Connect*, *298*(0704), 1-61.	The paper describes the Diamond Model of intrusion analysis, which allows integration of real-time intelligence into intrusion analysis, including the construction of attack threads, clusters and groups. This is useful for identifying and modelling threat actor tactics, techniques and procedures (e.g. MITRE's ATT&CK framework), similar to the paper's example of combining the diamond model with the kill chain.
Chen, T. M., Sanchez-Aarnoutse, J. C., & Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on smart grid*, *2*(4), 741-749.	The paper proposes the use of Petri nets to model coordinated cyber-physical attacks on the smart grid. The approach is flexible enough to consider timed and delayed intrusions, or even uncoordinated attacks by multiple threat actors.
Couretas, J. M. (2022). Taxonomy of Cyber Threats. In *An Introduction to Cyber Analysis and Targeting* (pp. 37-56). Cham: Springer International Publishing.	Book chapter that provides a good overview of cyber threats and threat models.

Paper Title	Notes
Dahl, O. M., & Wolthusen, S. D. (2006, April). Modeling and execution of complex attack scenarios using interval timed colored petri nets. In *Fourth IEEE International Workshop on Information Assurance (IWIA'06)* (pp. 12-pp). IEEE.	This paper described a mechanism for the modeling, partial analysis, and automatic execution of multi-agent, multi-stage attacks based on interval timed colored Petri nets. It suggests a possible research direction to address concurrent attack paths and attack agents.
Da Silva, M., Puys, M., Thevenon, P. H., Mocanu, S., & Nkawa, N. (2023, August). Automated ICS template for STRIDE Microsoft Threat Modeling Tool. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-7).	The paper proposes an ICS template to automate the collective analysis of ICS and CVE in the Microsoft Threat Modeling Tool (MTMT).
Ertaul, L., & Mousa, M. (2018). Applying the kill chain and diamond models to Microsoft advanced threat analytics. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 252-258). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).	The paper describes the complementary applications of the Diamond and Kill Chain models. The Diamond model helps security teams develop an understanding of how to assemble the necessary information in order to apply the Kill Chain model, while Kill Chain analysis helps security teams understand the phases of the intrusion.
Fernandez, E. B. (2016, August). Threat modeling in cyber-physical systems. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 448-453). IEEE.	The paper suggested the use of patterns to model cyber-physical threats. Importantly, it raises reflection that Mitigation (not explicit in this paper) should include graceful failure or degradation, and contextualised for cyber resilience.
Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1* (1), 80.	This paper proposed the concept of a kill chain with respect to computer network attack (CNA) and computer network espionage (CNE), comprising reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2) and lastly, actions on objectives.

Paper Title	Notes
Jamil, A. M., Ben Othmane, L., & Valani, A. (2021, November). Threat modeling of cyber-physical systems in practice. In *International Conference on Risks and Security of Internet and Systems* (pp. 3-19). Cham: Springer International Publishing.	The authors observe that most of the participants practice continuous threat modeling, and there is no common continuous threat modeling approach. This mixed input shows the importance of continuous threat modeling of CPS for the industry and the lack of rigorous and efficient approaches to do so.
Jamil, A. M., Khan, S., Lee, J. K., & Othmane, L. B. (2021, August). Towards automated threat modeling of cyber-physical systems. In *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)* (pp. 614-619). IEEE.	The paper has a good summary of other related work on cyber-physical threat modelling. The proposed automation approach is based on source code extraction and not successfully implemented.
Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry* , *137* , 103611.	The paper proposes an end-to-end threat modeling methodology that addresses the attacker perspective, but does not close the loop on whether risks have changed or have been effectively mitigated. This presents an interesting opportunity to follow up on dynamic / adaptive threat modeling.
Khalil, S. M., Bahsi, H., & Korõtko, T. (2023). Threat modeling of industrial control systems: A systematic literature review. *Computers & Security* , 103543.	Informative and useful systematic literature review (SLR) of papers related to threat modelling of industrial control systems, with useful examples of classification and selection of papers.
Khalil, S. M., Bahsi, H., Ochieng'Dola, H., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems-A Case Study of a Microgrid System. *Computers & Security* , *124* , 102950.	Khalil et al. proposed a threat modeling methodology supported by asset identification, system modeling and threat elicitation procedures for CPS. The paper highlights the importance of physical controls (in addition to logical controls) in the identification of trust boundaries between cyber and physical spaces. However, the use cases tend to be theoretical and applied on testbeds. They cited the MITRE ATT&CK for ICS framework, but considered that their attack categories should be more abstract for their case study.

Paper Title	Notes
Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017, September). STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE.	The paper describes the application of STRIDE threat modeling in a CPS use-case, and provides a systematic approach for doing so at both component and interaction levels.
Kim, K. H., Kim, K., & Kim, H. K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*, *44*(6), 991-1003.	The article explains the application of STRIDE for threat modelling of a DCS and DREAD for risk evaluation and prioritisation.
Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, *37*, 100521.	The paper describes the use of attack trees to model APT attacks in ICS, and to construct composite models from past known incidents. Interestingly, the sequential conjunctive (SAND) logical gate construct can be considered a phase in the attack kill chain, and could benefit from intervention in a self-healing context.
Lee, C. C., Tan, T. G., Sharma, V., & Zhou, J. (2021). Quantum computing threat modelling on a generic cps setup. In *Applied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21–24, 2021, Proceedings* (pp. 171-190). Springer International Publishing.	Paper describes the application of PASTA threat modeling method coupled with STRIDE and attack trees.
Li, K., Rashid, A., & Roudaut, A. (2021, October). Vision: Security-Usability Threat Modeling for Industrial Control Systems. In *Proceedings of the 2021 European Symposium on Usable Security* (pp. 83-88).	Paper proposes a security-usability threat model (lack of usability exacerbates security issues).
Maidl, M., Münz, G., Seltzsam, S., Wagner, M., Wirtz, R., & Heisel, M. (2021). Model-Based Threat Modeling for Cyber-Physical Systems: A Computer-Aided Approach. In *Software Technologies: 15th International Conference, ICSOFT 2020, Online Event, July 7–9, 2020, Revised Selected Papers 15* (pp. 158-183). Springer International Publishing.	The book chapter proposes a metamodel to show the dependencies between aspects of threats and different elements of a system, reflecting the relation between actions across the CPS threat taxonomy.

Paper Title	Notes
Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). IEEE.	The paper proposes that Cyber threat intelligence could be categorised according to various taxonomies such as MITRE ATT&CK.
Mekdad, Y., Bernieri, G., Conti, M., & Fergougui, A. E. (2021, May). A threat model method for ICS malware: the TRISIS case. In *Proceedings of the 18th ACM International Conference on Computing Frontiers* (pp. 221-228).	The paper proposed a threat model method for industrial malware based on the Diamond Model of intrusion analysis, comprising an extraction stage and modeling stage. In particular, TRISIS cyber attack was cited as a use case.
Moradi, F., Abbaspour Asadollah, S., Sedaghatbaf, A., Čaušević, A., Sirjani, M., & Talcott, C. (2020). An actor-based approach for security analysis of cyber-physical systems. In *Formal Methods for Industrial Critical Systems: 25th International Conference, FMICS 2020, Vienna, Austria, September 2–3, 2020, Proceedings 25* (pp. 130-147). Springer International Publishing.	Moradi et al. propose using an actor-based modeling language, Rebeca, for security analysis of CPS at the design phase. STRIDE model was employed as reference for attack classification.
Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Computing Surveys* , *55* (10), 1-36.	The paper proposes combining the MITRE ATT&CK and the cyber kill chain threat modeling approach for Smart Grid CPS.
Neubert, T., & Vielhauer, C. (2020). Kill chain attack modelling for hidden channel attack scenarios in industrial control systems. *IFAC-PapersOnLine* , *53* (2), 11074-11080.	The paper describes the use of kill chain modeling to identify defensive measures specific to each phase of the kill chain. Importantly, the approach elaborates defensive controls that would directly address sophisticated TTPs, and which would not be obvious from traditional IT threat or attack modeling.
Paudel, S., Smith, P., & Zseby, T. (2017, April). Attack models for advanced persistent threats in smart grid wide area monitoring. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (pp. 61-66).	The paper introduces the idea of including physical threats in attack trees, on top of cyber threats that can invoke cyber-physical security issues.
Pell, R., Moschoyiannis, S., Panaousis, E., & Heartfield, R. (2021). Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK. *arXiv preprint arXiv:2108.11206* .	The paper suggests that attack graphs could be used to model CPS threats adaptively over time to track and identify paths that (potentially different) intruders may take in multi-stage attacks.

Paper Title	Notes
Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat modeling using attack trees. *Journal of Computing Sciences in Colleges* , *23* (4), 124-131.	The paper describes the use of attack trees for threat modeling, weighted with cost of attack and damage cost.
Shevchenko, N., Frye, B. R., & Woody, C. (2018). Threat modeling for cyber-physical system-of-systems: Methods evaluation. *Software Engineering Institute: Pittsburgh, PA, USA* .	The paper highlights that STRIDE is focused on the defender perspective and for threat discovery, i.e. to identify threats (in the STRIDE classification) and mitigate them at the design stage. Therefore it is not suited for CPS, as the mitigation may not be applicable due to technology or operational limitations, and does not address APT threats and extended campaigns.
Sridhar, A., & Aditya, M. (2016). Generalized attacker and attack models for cyber physical systems. *40th IEEE COMPSAC* .	Adepu and Mathur proposed a common, unified (domain model) framework to design a variety of cyber physical attacks for assessing attack detection methods and tools. There are several limitations to the approach as it does not consider the difficulty of designing and launching an attack.
Stojanović, B., Hofer-Schmitz, K., & Kleb, U. (2020). APT datasets and attack modeling for automated detection methods: A review. *Computers & Security* , *92* , 101734.	The paper highlights that there is no unique path that all APT attacks follow. Reflecting on this, my take is that even though the attack cycle in CPS could be simplified based on the assumption that the goal is different, it is likely that the attacker has access to the IT network which would have a different attack model. Therefore it is not enough to look at CPS in silo, but as a system-of-systems even if they are not connected.
Straub, J. (2020, November). Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks. In 2020 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 148-153). IEEE.	The paper describes a generalised solution for modeling framework/paradigm-based attacks that go beyond the deployment of a single exploit against a single identified target.
Suo, D., Siegel, J. E., & Sarma, S. E. (2018). Merging safety and cybersecurity analysis in product design. *IET Intelligent Transport Systems* , *12* (9), 1103-1109.	This paper proposes a model that combines safety hazard analysis and cybersecurity threat assessment using the STRIDE framework.

Paper Title	Notes
Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon* , *7* (1).	Literature review covering threat modelling strengths and limitations, in the context of APT attacks. Every model has a use-case that it is suited for, and there is potential to combine different models together to address specific scenarios or needs.
Valenza, F., Karafili, E., Steiner, R. V., & Lupu, E. C. (2022). A hybrid threat model for smart systems. *IEEE Transactions on Dependable and Secure Computing* .	The paper proposes a model for mapping the dependencies and threats facing smart systems across cyber, physical and human aspects.
UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis* . John Wiley & Sons.	This book describes PASTA, a high-level analysis approach to among other capabilities, derive threat classes less from preventive security processes (e.g. STRIDE/DREAD) but more from detective security measures (e.g. threat intelligence feeds, incidents).
Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. *Computers & security* , *84* , 53-69.	Systematic literature review on cybersecurity threat modeling.
Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling* , *21* (1), 157-177.	The paper proposes a threat modelling language (meta attack language) used to generate attack graphs from MITRE ATT&CK matrix.
Yang, Y., & Zhang, M. (2023, July). From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 336-344). IEEE.	The paper describes a systematic (shorthand) approach for describing an attack model, anchored on TTPs employed by APT actors in ICS.
Zahid, S., Mazhar, M. S., Abbas, S. G., Hanif, Z., Hina, S., & Shah, G. A. (2023). Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. *Internet of Things* , *22* , 100766.	Mapping of NIST controls against threats modeled using MITRE ATT&CK.

Paper Title	Notes
Zalewski, J., Drager, S., McKeever, W., & Kornecki, A. J. (2013, January). Threat modeling for security assessment in cyberphysical systems. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop* (pp. 1-4).	The paper presents two important concepts. First, that a security breach in CPS is not a binary event - there is a degraded state and the paper proposes using threat modeling to derive the probabilities of landing in a degraded state in a Markov chain model. Second, that fault tree analysis is broader than attack trees, as it covers failures beyond what the attacker's action may result in. This sets cyber physical threats apart from traditional STRIDE taxonomy.
Zenitani, K. (2023). Attack graph analysis: an explanatory guide. *Computers & Security* , *126* , 103081.	The paper provides a detailed explanation of different types of attack graphs, derived metrics and limitations
Zhang, S., Shi, P., Du, T., Su, X., Han, Y., & Chen, P. (2022, December). Threat Modeling and Reasoning for Industrial Control System Assets. In *2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* (pp. 468-475). IEEE.	The paper proposes a formal ontology to describe ICS assets, threat consequences and their inter-relationships.
Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* , *9* , 29775-29818.	Zografopoulos et al. proposed a CPS threat modeling framework comprising (importantly): adversary model formulation and attack characteristics. They noted that while there is extensive research on threat modeling in the pre-attack context, the investigation of adversary behaviour post-compromise is also important. To this end, they incorporate core components of the MITRE ATT&CK for ICS framework to support CPS adversarial behaviour evaluations.