Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
10th CIRP Global Web Conference – Material Aspects of Manufacturing Processes

Designing Resilient Manufacturing Systems using Cross Domain Application of Machine Learning Resilience

Avik Mukherjee*, Moritz Glatt, Waleed Mustafá, Marius Kloft, Jan C. Aurich

*Institute for Manufacturing Technology and Production Systems (FBK), TU Kaiserslautern, Kaiserslautern 67663, Germany

Machine Learning Group, TU Kaiserslautern, Kaiserslautern 67663, Germany

* Corresponding author. Tel.: +49 631 205 3224; fax: +49 631 205 3304. E-mail address: avik.mukherjee@mv.uni-kl.de

Abstract

The COVID-19 pandemic and crises like the Ukraine-Russia war have led to numerous restrictions for industrial manufacturing due to interrupted supply chains, staff absences due to illness or quarantine measures, and order situations that changed significantly at short notice. These influences have exposed that it is crucial to address the issue of manufacturing resilience in the context of current disruptions. This can be plausibly guaranteed by subjecting the ML model of a manufacturing system to attacks deliberately designed to fool its prediction. Such attacks can provide useful insights into properties that can increase resilience of manufacturing systems.

Keywords: manufacturing system; supply network; discrete-event simulation environment; resilience; machine learning; adversarial attacks; adversarial training; deep neural networks

1. Introduction

Modern day industries are affected by the VUCA assumption which characterizes the world of manufacturing by its dynamic, complex, and unpredictable nature. Rapidly changing consumer demands, shorter product life cycles, unforeseen technological innovations, natural disasters like earthquakes, floods, and political disruptions like war add on to the conformity of this assumption. Such a scenario combined with the complex; interwoven structure of today’s manufacturing systems makes tasks like turbulence predictions inaccurate leading to deviations from the estimated production plans [1]. Recently, disruptions caused due to the COVID-19 pandemic like supply chain hindrances, workforce unavailability and changing socio-economic scenario like the Ukraine-Russia war have led to material shortages which in turn have hampered manufacturing. The automotive industry in Europe as an example has been impacted due to the unavailability of car wiring harnesses which used to be supplied by the now war-torn country Ukraine. This has led to a stop in production in the Volkswagen Zwickau plant in Germany, which manufactures ID.4 electric vehicles for both the European and American markets. Such hindrances have made it clear that manufacturing systems should also consider externally caused emergencies like supply chain disruptions when planning production control. The ability of a manufacturing system to cope with changes caused due to disruption is termed as resilience. Resilience in manufacturing systems is seen as a combination of mainly two qualities: robustness and agility [2]. Robustness signifies the ability of a manufacturing system to
continue its normal operation even when faced by disruptions. Agility signifies the ability of a company to recover from a dip in normal operation due to disruptions.

Approaches to study resilience until date have focused on mathematical modeling of the internal operational conditions like material flow and availability of machines, prediction of disruptions on historically collected data and learning methods for mitigation after prediction, predicting disruptions from data generated using digital twins [3]. The highly non-linear and dynamic nature of modern manufacturing systems makes it difficult to find out the factors that can precisely affect its performance. Though studies have attempted at finding out the factors that can increase resilience [4], disruptions due to the pandemic and current socio-economic crises like wars followed by environmental disruptions like the droughts faced in 2018 and 2022 have added on to the demand for designing a more reliable and resilient model of a manufacturing system.

A potential approach to the development of such a resilient manufacturing system is provided by the cross-domain application of Machine Learning (ML) resilience. It can be assumed that the techniques used to increase the resilience of a ML model can also be used to increase the robustness of a ML model of a physical manufacturing system. Following this assumption, a manufacturing system ML model is proposed in this article which takes parameters relevant to the manufacturing system design and operation as input and learns the functionality of a design with respect to resilience related performance indicators given the set of operating conditions under possible disruptions. Adversarial attacks corresponding to the model will be generated and evaluated (on the ML model) to find the set of most robust design parameters for a manufacturing system. This article gives a cross disciplinary definition of resilience in the context of manufacturing system and machine learning followed by a description of the state of the art in Section 2. It then introduces the proposed approach in Section 3 and describes the pipeline with the help of an illustrative example in Section 4.

2. Resilience as a cross domain study

The resilience of a system signifies its capability to recover quickly from disruptions. Generally, resilient systems are characterized by their ability to spring back from adversities or disruptions that hinder their performance. Specifically, resilience is considered as quality inherent in systems by virtue of which they can continue performing under the effect of operational challenges within optimal time and cost parameters [5]. The system can either be well prepared for such operational challenges or can also recover from a degraded state led to by the sudden appearance of the challenges. Resilience is highly dynamic and non-linear and depends on the state the system is in at that point of time [5]. Some approaches have considered resilience as a vector dependent on time and the kind of threat posed to the system as the ability to recover from a degraded state within acceptable time and cost limits [6]. Resilience of a system in a very general sense can thus be characterized by non-linearity and a high degree of time variance. It is also highly dependent on the input to the system at that instant of time.

2.1. Resilience in Manufacturing Systems

Modern manufacturing systems are expected to be able to produce customized goods with high economic efficiency, which leads to internal and external complexities. Following the era of mass production, manufacturing systems are now influenced by products that can cater to a more diversified customer base increasing the necessity of flexibility in their design [7, 8]. This can be introduced by considering reconfigurable manufacturing systems and assembly systems and transformable factory on a structural level [9].

External complexity of a manufacturing system is defined by its inter-connected supply chain. Cost effective supply chains come with a hidden cost incurred by disruptions. Supply chain disruptions can have a long-standing negative effect on manufacturing systems. In the recent past, global electronic manufacturers like Ericsson have lost over 400 million € owing to a fire in one of their supplier’s semiconductor plants in 2000 [9]. Recent incidents like the COVID-19 pandemic have slowed down the supply chains due to factory closures, staff absences in turn affecting the global economy. In India, supply chain shortages led to a drop in product availability of foods and vegetables by 8 % and vegetable oils by 14 % [10]. Disruptions under the effect of such complexities make production planning and control a highly non-trivial task. Consequently, resilience which is traditionally classified by a high level of dynamics and time variance becomes a highly complex attribute for modern manufacturing systems.

Various attributes of a manufacturing system can be studied to get an estimate of resilience like energy, materials, components, physical assets and processes, supply chain logistics, workforce societal values [11, 12]. Performance related indicators like Production-loss, Throughput-settling-time, Time-to-recover can be considered when attaching resilience to possible disruptions. Fig. 1 gives the curve of performance against time in regards of production quantity. The curve in the figure signifies the dip in production after a disruption starts. Production-loss as seen in Fig. 1 signifies the maximum dip in the production of the system after the disruption starts, Throughput-settling-time is the time elapsed from the end of disruption, for the manufacturing system, to resume its normal operations and Time-to-recover is the total time elapsed from the start of the disruption to get the throughput of the manufacturing system back to normalcy. The curve in Fig. 1 can also be extended to other performance measures like the quality of production, and the cost of production in terms of ROI. Quantitatively, resilience can be classified as a multi-dimensional attribute highly dependent on the disruption posed to the manufacturing system.

The production loss suffered due to events like the pandemic have spurred a lot of research regarding resilience of manufacturing systems. Stochastic as well as quantitative and qualitative approaches have been used to measure resilience. [11] takes a quantitative approach towards incorporating resilience in production control by defining Penalty-of-Change (POC) as the measure of probabilistic changes coming due to pandemic related scenarios. Understanding resilience using manufacturing design has also been attempted in [13]. [2] uses socio-technical aspects and deterministic interactions between
the tasks of production control to design robust production processes. [1] uses supervised learning to predict turbulence from order data and reinforcement learning for devising approaches to mitigate turbulence thus adding on to the resilience in production control. Given one of the most important factors in determining the productivity of a manufacturing system, many approaches have been studied to increase the supply chain resilience [15].

While addressing a largely different subject, the field of ML also dedicates a fair amount of literature to study resilience. Many ML models suffer from security issues like adversarial examples. An adversarial example is one created by modifying a correctly predicted sample. The modification is carefully designed such that it is imperceptible and cause the model to predict incorrectly. This phenomenon is known as an adversarial attack. As several methods have been developed to prevent negative effects of such attacks, investigating possible methods from ML robustness for manufacturing systems seems promising.

2.2 Robustness using ML

ML aims at modeling a given task by utilizing data collected from previous successful attempts of that task (e.g., an ML model can learn to recognize images from a dataset of pairs of images and their corresponding labels). Algorithms and models used in ML have been utilized in making smart decisions in many aspects of manufacturing systems, for example, quality management [16], conceptual layout planning [17], and smart production planning and control [18]. Recently, it has been shown that many ML models trained with standard algorithms suffer from resilience issues. For a model with high accuracy and an example that it classifies correctly, another example, called adversarial example can be created, such that it is close to the original example (in some sense), but the model classifies it incorrectly. This phenomenon is known in the literature as adversarial examples [27]. Stop signs with graffiti have been found to be misclassified, thus posing a threat for autonomous driving applications [19].

The literature on adversarial attacks falls into three categories. The first category aims to evaluate the resilience of models by developing attacks that generate adversarial examples under different knowledge assumptions about the model. White-box attacks [20] refer to the case in which the adversary has a full knowledge of the model and its parameters while in black-box attacks [20], the adversary does not have knowledge about the model but rather can query it. The evaluation of resilience in ML is non-trivial; a model trained with many attacks can still be susceptible to future attacks [28]. To remedy this, some researchers propose provable evaluation (second category), that is, algorithms designed to mathematically evaluate resilience rather than empirically [29, 28].

Provable evaluation has the advantage of providing strong guarantees that applies for any attack even the ones designed in the future. Finally, the third category of research is developing algorithms for building robust models. The most common way is adversarial training [21], in which a given attack is used to generate adversarial examples for the training set and augment the training set with those examples with correct labels. One other approach is the regularization approach. In this approach, some quantity derived from the trained model (e.g., the spectral norm of the weights) is controlled to increase its robustness. This approach has the advantage that robustness is controlled via specific properties of the model and hence provide better theoretical and practical understanding compared to the adversarial training approach. For instance [14] controls robustness via the second-order derivatives of classifiers with respect to its input [14, 30, 31]. This led to the design of a regularization technique that increased the practical resilience of neural network models.

2.3 Summary of State Of The Art  

The nature of current disruptions leveraged by the complexity of modern-day manufacturing systems have made studies regarding manufacturing system resilience extremely crucial. Literature regarding resilience mainly focuses on improving resilience either studying the manufacturing system operation or the design. [11] tries to quantify resilience using probabilistic formulations of possible disruptions and their effects on the system, but mainly considers scenarios related to the current pandemic, therefore localizing the possible disruptions to the pandemic situation. [2] tries to define robust processes by an empirical consideration of possible disruptions.
and incorporating them in the production control whereas [1] tries to predict disruptions depending on historical order data and use reinforcement learning to learn and thus include measures in manufacturing control. The uncertainty and complexity characterizing the manufacturing systems poses questions on the efficiency of predictive models based on historical data. [13] focuses only on the manufacturing design to increase the resilience of the manufacturing systems but considers hindrances or disruptions only due to internal factors like machine unavailability. Approaches like [15] focus on optimizing supply chain resilience using various strategies, but do not involve other factors related to the manufacturing system. The current approaches mostly focus either on changing the design or the operation of the manufacturing system or solely rely on increasing the supply chain resilience.

The method proposed in the remainder of this paper considers both the operation and design of the manufacturing system to create a ML model. It also takes under consideration both the internal and the external causes of disruptions that can affect a manufacturing system including the supply chain strategies. Disruptions are modeled in the form of adversarial attacks on the ML model of the manufacturing system. The model is then analyzed under the impact of the generated adversarial attacks to find out the most robust design parameters under various operational conditions.

### 3. Resilience using adversarial attacks

The approach proposed in this paper considers the cross-domain application of ML resilience in the manufacturing system. The physical manufacturing system can be modeled using ML algorithms which take as input the manufacturing system design and operations and outputs performance related indicators like throughput. The manufacturing system operations can be simulated using design decisions subjected to various operational policies. This simulation is used for data generation by creating conditions mimicking the operational conditions under actual disruptions. The data generated is then used to train the machine learning model. Adversarial attacks pertaining to simulated disruptions inspired by actual disruptions caused due to incidents like pandemic, wars and further adversities can then be generated to highlight the vulnerabilities of a given design. These examples can then be used to generate more resilient manufacturing systems. The following section discusses this approach in further details by breaking it down into a pipeline as given in Fig. 2. An illustrative example is formulated in the form of a use case of a chair manufacturing factory in Section 4 to discuss the pipeline described in the following sections.

### 3.1 Description of Manufacturing System

A manufacturing system can be formally described by its operation and design. Manufacturing system design can be conceptualized as a function mapping the required performance measures to the decision variables which describe its design [7]. The operation of a manufacturing system is defined by the parameters or decision variables that are used in production planning and control (PPC). It is established in three main layers: strategic planning, operations planning and detailed planning [7, 22]. A favorable set of design, strategic planning and operational planning variables are being referred broadly to as the design of the system in this article. Operation is represented by the variables and the policies that affect the day-to-day operations of the manufacturing system. A list of possible design and operations variables that can be considered broadly for any production system is given below in Table 1.

| Type             | Design Parameters                  | Operational Parameters      |
|------------------|------------------------------------|-----------------------------|
| Resources        | Resource requirements              | Resource availabilities     |
| Automation       | Planned degree of automation       | Achievable degree of automation |
| Material flow    | Planned material flow              | Operational material flow   |
| Customer Orders  | Estimated demand / Original customer order | Customer Demand            |
| Supply strategy  | Supplier strategy                  | Supplier availability       |
| Inventory        | Planned buffer capacities          | Available buffer capacities  |

### 3.2 Data Generation from Simulation

Typically, manufacturing systems can be modelled as Discrete Event Models based on the processes and the flow of material [23]. Design and operations defined in the previous section are used to get the planned throughput from the simulation. Operational parameters are modified to simulate disruption and the performance measures generated from the simulation are used as the target variable of the data set along with the corresponding design and operation as input.

### 3.3 ML Model of a manufacturing system

The data generated from the simulation is used to train the ML model representing the manufacturing system. A function
is learned to predict the functionality of a given design. It utilizes the dataset generated from the simulation discussed in section 3.2. Formally, a manufacturing system design can be represented by design parameter \( D \in \mathcal{D} \) and operational parameters \( O \in \mathcal{O} \) where \( \mathcal{D} \) and \( \mathcal{O} \) are the space of all possible design and operational parameter. Formally, a functionality predictor is a map \( \hat{Q} : \mathcal{D} \times \mathcal{O} \rightarrow [0, 1] \) which can be learned to estimate the functionality \( \hat{Q}(D, O) \) of a design \( D \) under an operational parameter \( O \). Let \( S := \{(D_i, O_i, q_i)\}_{i=1}^n \) be a dataset of \( n \) examples, where \( D_i \in \mathcal{D}, O_i \in \mathcal{O} \) and \( q_i \in [0, 1] \). The objective is to select a function \( \tilde{Q} \) that can minimize the empirical squared error on \( S \), that is

\[
\tilde{Q} = \arg\min_{\hat{Q} \in Q} \frac{1}{n} \sum_{i=1}^{n} (Q(D_i, O_i) - q_i)^2 ,
\]

(1)

Where \( Q \) is represented by the set of deep neural networks. The set of the operational parameters is chosen to be \( \mathcal{O} \subset \mathbb{R}^d \) as they can be represented by real numbers. Graphs can be considered as a possible format for representing the design \( D \).

Fig. 3 ML architecture for learning functionality

A graph is defined as the tuple \( G := (V, E) \) where \( V \) is a set of nodes–each node representing a given manufacturing element (e.g., machine)–while \( E \) is the set of edges connecting such elements (e.g., conveyor belts). Graphs are flexible to represent the different manufacturing situations, amenable to learning through Graph Neural Networks (GNN) [24], and there exist techniques to optimize them using guiding signals from the GNNs [25]. The design graph is fed into a GNN that outputs a real-valued vector while the operation parameters are fed into a multi-layer perceptron that also outputs a real-valued vector (Fig. 3). The outputs are fused by concatenating them and feeding the resultant vector into a fusion network.

3.4 Design Adversarial attacks

A manufacturing system realized from a given design \( D \) is resilient if, by changing the operation parameters \( O \) slightly, its functionality does not suffer a large decline. To formally quantify the changes in an operational parameter a distance function \( d: \mathcal{O} \times \mathcal{O} \rightarrow \mathbb{R}_+ \) is defined which maps two operational parameters into a positive real number that quantifies the difference between them. This can thus help in designing adversarial attacks for the above defined ML model \( \hat{Q} \). Any operation parameter \( \hat{O} \) within \( \varepsilon \) \( d \) distance of an operation parameter \( O \) that causes the maximum difference in functionality can be called as an adversarial example pertaining to \( O \) as shown in Equation 2.

\[
\hat{O} = \arg\max_{O \in \mathcal{O}, d(O, \hat{O}) \leq \varepsilon} (\hat{Q}(O, D) - \hat{Q}(O, D))^2
\]

(2)

Proximal gradient descent is a good candidate to solve the optimization problem in Equation 2 given that the distance metric is efficiently evaluated and there is an efficient algorithm to project any \( \hat{O} \in \mathcal{O} \) into the ball \( \{ O : O \in \mathcal{O}, d(O, O) \leq \varepsilon \} \). Assuming \( \mathcal{O} \subset \mathbb{R}^d \), Euclidean distance can be used as a metric.

3.5 Adversarial training to find out a robust design

Robust design parameters should have the least deviation in their functionality when subjected to the adversarial examples designed in the last section. This can help in finding out a manufacturing system design that can stay resilient under the face of disruptions caused by factors intrinsic as well as extrinsic to the manufacturing system. This is achieved by solving a mini max problem given by Equation 3.

\[
D^* = \arg\min_{D \in \mathcal{D}} \max_{O \in \mathcal{O}, d(O,D) \leq \varepsilon} (\hat{Q}(O, D) - \hat{Q}(O, D))^2
\]

(3)

The objective function in Equation 3 is non-trivial since the objectives are not concave/convex functions and the design parameter \( D \) can exhibit a rich structure. This can be solved using an alternative approach breaking down Equation 3 into two separate optimization problems and solving them iteratively over the dataset \( S \) generated from the simulation.

4. Case Study: Office-Chair Manufacturing

This section provides a very basic use case of office chair manufacturing factory to illustrate the pipeline mentioned in Section 3. Chair manufacturers mainly use plastic, wood, foam, cloth, steel as raw materials performing a host of molding, bending, cutting operations followed by a manual or semi-automatic assembly, and then shipping. The design of a chair manufacturing factory in this analysis is represented by decisions taken for a time range of between 1 month - 2 years like the location, the supplier strategy, number of variants of chairs to be produced, number of induction molding machines (for producing plastic parts), number of bending machines (for producing the metallic chassis), number of personnel needed to man the shop floor. Operations on the other hand can be signified by the availabilities of the same resources during the period, the machine conditions, the current customer orders. The values of these variable are used to simulate the factory operations where the design variables can represent the factory planning and the operations represent the running conditions. Disruptions are simulated by changing the operational conditions of the factory. Data obtained from simulation is used to train a ML model representing the chair factory.

The material flow, the structure of the factory along with the position and quantity of buffers and resources can be encoded in a graph. The operational conditions like the availabilities of resources, buffers, and suppliers along with the actual machine running times can be encoded using a vector of real numbers and thus represented using an MLP. An ensemble of these networks can be trained as per the network architecture given in Fig. 3 considering a vector of performance measures like the throughput, inventory levels, work in process as the functionality.

This is a resupply of March 2023 as the template used in the publication of the original article contained errors. The content of the article has remained unaffected.
An adversarial example can be considered as the set of the same parameters within an ε Euclidian distance of the original parameters (encountered in the dataset) that lead to a significant change in the performance indicators. For a given design of the chair manufacturing system reducing the number of available injection molding machines (for creating the plastic parts) and increasing the plastic supply delivery time can signify machine down time due to supply disruptions. Such disruption can be used as adversarial examples if they significantly change the functionality of the ML model above a given limit. A design for mass-production supporting inventory-based operations proves to be more robust than a design intended for JIT operation under such circumstances which works on temporary customer demand, consequently giving a lower change in the performance measures as per Equation 3.

5. Summary and Outlook

Resilience of a manufacturing system is defined by its ability to spring back from disruptions under acceptable time and performance limits. The functionality of a given manufacturing system design can be predicted by training a ML model to represent its parametric design. Such a model can then be studied under the influence of white-box adversarial attacks to find out parameters that can increase the resilience of manufacturing system. The conceptual pipeline and the example described in sections 3 and 4 above will be followed by actual investigation throwing more light on the parameters representing the design and operation and designs that stay resilient under possible operational disruptions.

Acknowledgement

This research was funded by the State of Rhineland-Palatinate within the Special fund „Nachhaltige Bewältigung der Corona-Pandemie“ – Program to strengthen Digitization at Universities. Program line 3: Digital Profile Development in Research Project: „KI-Nachwuchsförderung in Zeiten von Corona“.

References

[1] Bauer, D., Böhm, M., Bauernhansl, T., Sauer, A., 2021. Increased resilience for manufacturing systems in supply networks through data-based turbulence mitigation. Prod. Eng. Res. Devel. 15, p. 385-395.
[2] Alexopoulos, K., Anagnostis, I., Nikolakis, N., Chryssohoulis, G., 2021. A quantitative approach to resilience in manufacturing systems. International Journal of Production Research, p. 1 - 16.
[3] Papacharakamposopoulos, A., Michail, C.K., Stavropoulos, P., 2021. Manufacturing resilience and agility through processes digital twin: design and testing applied in the LPBF case. Procedia CIRP 103, p. 164 – 169.
[4] Liu, Y., Chen, R., Zhou, F., Zhang, S., Wang, J., 2021. Analysis of the Influencing Factors of Organizational Resilience in the ISM Framework: An Exploratory Study Based on Multiple Cases. Sustainability 13, p. 13492.
[5] Buchanan, R.K., Goerger, S.R., Rainaud, C.H., Pamell, G., Ross, A., Sitterle, V., 2020. Resilience in engineered resilient systems. Journal of Defense Modeling & Simulation 17, p. 435-446.
[6] Haines, Y.Y., 2009. On the definition of resilience in systems. Risk Anal 29, p. 498-501.
[7] Chryssohoulis, G., 2013. Manufacturing systems: theory and practice. Springer Science & Business Media.
[8] Wiendahl, H.P., ElMaraghy, H.A., Nyhuis, P., Zäh, M.F., Wiendahl, H.H., Duffie, N., Brieke, M., 2017. Changeable Manufacturing - Classification, Design and Operation. CIRP Annals 56, p. 783-809.
[9] Tang, C.S., 2006. Robust strategies for mitigating supply chain disruptions. International Journal of Logistics Research and Applications 9, p. 33-45.
[10] Mahajan, K., Tomar, S., 2020. COVID-19 and Supply Chain Disruption: Evidence from Food Markets in India. Am J Agric Econ.
[11] Alexopoulos, K., Anagnostis, I., Nikolakis, N., Chryssohoulis, G., 2021. A quantitative approach to resilience in manufacturing systems. International Journal of Production Research, p. 1-16.
[12] Caputo, A.C., Pelagagge, P.M., Salini, P., 2019. A methodology to estimate resilience of manufacturing plants. IFAC-PapersOnLine 52, p. 808-813.
[13] Gu, X., Jin, X., Ni, J., Koren, Y., 2015. Manufacturing System Design for Resilience. Procedia CIRP 36, p. 135-140.
[14] Mustafa, W., Robert, A.V., Kloie, M., 2020. Input Hessian Regularization of Neural Networks. International Conference on Machine Learning 37.
[15] Belhadi, A., Kamble, S., Fosso Wamba S., Queiroz, M.M., 2021. Building supply-chain resilience: an artificial intelligence-based technique and decision-making framework. International Journal of Production Research, p. 1-21.
[16] Park, J.K., Kwon, B.K., Park, J.H., Kang, D.J., 2016. Machine learning-based imaging system for surface defect inspection. Int. J. of Precis. Eng. and Manuf.-Green Tech. (International Journal of Precision Engineering and Manufacturing-Green Technology) 3, p. 303-310.
[17] Klar, M., Glatt, M., Aurich, J.C., 2021. An implementation of a reinforcement learning based algorithm for factory layout planning. Manufacturing Letters 30, p. 1-4.
[18] Cadavid, J., Pablo, U., Lamouri, S., Grabot, B., Fortin, A., 2019. Machine Learning in Production Planning and Control: A Review of Empirical Literature, IFAC-PapersOnLine 52, p. 385-390.
[19] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., Song, D., 2018. Robust physical-world attacks on deep learning visual classification. Proceedings of the IEEE conference on computer vision and pattern recognition, p. 1625-1634.
[20] Balda, E.R., Belboudi, A., Mathar, R., 2020. Adversarial Examples in Deep Neural Networks: An Overview, in Deep Learning: Algorithms and Applications. Pedrycz, Chen (Hg.) 2020 – Deep Learning, p. 31-65.
[21] Madry, A., Makelov, A., Schmidt, L., Tsipras, D., Vladu, A., 2017. Towards deep learning models resistant to adversarial attacks, arXiv.
[22] Anthony, R.N., 1965. Planning and control systems: a framework for analysis. Division of Research, Graduate School of Business Administration, Harvard.
[23] New, S., 1994. Modeling and Analysis of Manufacturing Systems. Journal of the Operational Research Society 45, p. 725-726.
[24] Jaeckle, F., Kumar, M.P., 2021. Generating adversarial examples with graph neural networks, in Proceedings of the Thirty-Seventh Conference on Uncertainty in Artificial Intelligence. PMLR, p. 1556.
[25] Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., Sun, M., 2020. Graph neural networks: A review of methods and applications. AI Open 1, p. 57-81.
[26] Bayro-Corrochano, E., Hancock, E., 2014. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. Springer International Publishing.
[27] Goodfellow, I.J., Shlens, J., Szegedy, C., 2014. Explaining and harnessing adversarial examples. arXiv.
[28] Athalye, A., Carlini, N., Wagner, D., 2018. Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples, in Proceedings of the 35th International Conference on Machine Learning, PMLR, p. 274.
[29] Xiao, K.Y., Tjeng, V., Shafiullah, N.M., Madry, A., 2018. Training for Faster adversarial robustness verification via inducing relu stability. arXiv. PMLR, p. 274.
[30] Cisse, M., Bojanowski, P., Grave, E., Dauphin, Y., Usunier, N., 2017. Parseval networks: Improving robustness to adversarial examples, in Proceedings of the 35th International Conference on Machine Learning, PMLR, p. 808-813.