

MOŽNOSTI INTELIGENTNÉHO RIEŠENIA VÝROBNÉHO PROCESU

POSSIBILITIES OF INTELLIGENT SOLUTION OF PRODUCTION PROCESS

Ing. Peter Malega, PhD.

Bc. Monika Matalíková

Technická univerzita v Košiciach

Strojnícka fakulta

Ústav manažmentu, priemyselného a digitálneho
inžinierstva

Park Komenského 9, 042 00 Košice,

e-mail: peter.malega@tuke.sk

Abstract: The aim of this paper is to describe possibilities of intelligent solution of production process. The individual parts of the paper describe new trends in production process innovation. In these days, there are many possibilities how to innovate the production process. We described five options – cyber security, cyber physical system, predictive maintenance, deep learning, automation.

Key words: production process innovation, cyber security, cyber physical system, predictive maintenance, deep learning, automation

Úvod

Inovovanie výrobného procesu je stále potrebné, preto sa táto téma stáva nadčasovou a je potrebné o nej neustále diskutovať. [8] V súčasnosti je možné inovovať výrobný proces zavedením inteligentného riešenia do daného procesu, čím sa zabezpečí lepšia flexibilita výroby. [11]

Postup inovácií výrobného procesu sa skladá z dvoch fáz, a to z fázy tvorby a fázy realizácie. [7] Pri inovovaní výrobných procesov sa odporúča postupné inovovanie, čo znižuje riziká a zvyšuje pružnosť prevádzky. Súčasťou inovácie pracovného procesu je aj identifikácia nedostatkov procesu, ktoré budú danou inováciou odstránené. [12]

Možnosti inovácie výrobného procesu

V súčasnosti disponujeme širokou paletou možností inovovania výrobného procesu. Dôsledkom toho sa zvyšuje celkový komfort spoločnosti. Spoločnosť žije konzumnejším životným štýlom, čo vedie k väčšiemu množstvu spotreby materiálov. Na to nadväzuje zvýšenie výroby, a taktiež sa zvýšený komfort ľudského života odráža na zlepšovaní pracovných podmienok pracovníkov. [4]

Možnosti inovácie výrobného procesu špecifikujeme v oblastiach, ktoré sú popísané nižšie.

Kybernetická bezpečnosť

Inovácie sa vo veľkej miere realizujú digitalizáciou výrobného procesu. Veľkým rizikom intenzívnej digitalizácie výrobného odvetvia je nárast náchylnosti na kybernetické útoky. Zavedením IoT (z anglického Internet of things, Internet vecí), cloudcomputing a umelej inteligencie vzniklo okrem nepredstaviteľnej hnacej sily inovácií vo výrobnom sektore, aj častejšie vystavovanie výrobcov kybernetickým útokom. [10]

Kybernetické hrozby sú dôsledkom pri zavádzaní počítačov, sietí a smartfónov do výrobného sektora bez dostatočného investovania do kybernetickej bezpečnosti. Veľký počet hackerských útokov je do značnej miery spôsobený pripojením strojov na internet, resp. využívaním zdieľania snímacích a riadiacich systémov založených na cloude. Cieľom je zvyšovanie kybernetickej bezpečnosti.

Pod kyber-bezpečnosťou rozumieme ochranu dôverných údajov, zachovanie integrity dát a dostupnosti údajov. Národný inštitút pre normy a technológie v Amerike (NIST, z anglického National Institute of Standards and Technology, Národný inštitút pre štandardy a technológie) vytvoril metodiku posudzovania rizika z charakterizácie systému, identifikácie hrozby a zraniteľnosti, kontrolnej analýzy, určenia pravdepodobnosti, analýzy dopadu, stanovenia rizika a kontrolných odporúčaní.

Príručka NIST pre riadenie rizík pre systémy informačných technológií hovorí, že sa hrozba týka „potenciálu konkrétneho zdroja hrozby úspešne uplatniť určitú zraniteľnosť“. Ako zdroj hrozby si predstavme akúkoľvek okolnosť alebo udalosť, ktorá umožňuje poškodiť systém informačných technológií.

Pod pojmom útok rozumieme pokus o získanie neoprávneného prístupu k systémovým službám, zdrojom alebo informáciám a taktiež pokus o narušenie integrity systému. Pritom môže ísť o útok heslom, zneužitím dôvery alebo presmerovaním portov.

V Tab. 1 môžeme vidieť zoznam hrozieb a v Tab. 2 zoznam možných útokov a ich dôsledkov.

Tab. 1 Hrozby spojené s kybernetikou [10]

Terč	Zraniteľnosť	Zdroj hrozby
Software	Overenie vstupu, eskalácie privilégii, zraniteľnosť miesta pri kódovaní softvéru	Hacker, cracker, počítačový zločinec, terorista, priemyselná špionáž, zamestnanec, vláda
Hardware	Škodlivá logika, otvorené ladiace porty	Zamestnanec
Operačný systém alebo firmvér	Neodoslané systémy, zraniteľné súčasti systému	Hacker, cracker, počítačový zločinec, terorista, priemyselná špionáž, zamestnanec, vláda
Sieť	Obmedzená šírka pásma na rušenie, nešifrovaná komunikácia, slabé protokoly zabezpečenia siete (napr. autentifikácia)	Hacker, cracker, počítačový zločinec, terorista, priemyselná špionáž, zamestnanec, vláda
Údaje	Obyčajný text šifrovania, bez kódu integrity správy (MAC)	Hacker, cracker, počítačový zločinec, terorista, priemyselná špionáž, zamestnanec, vláda

Tab. 2 Zoznam možných útokov na digitálne výrobné systémy [10]

Útok	Metóda	Dôsledok
Snaha o neoprávnený prístup (napr. útoky heslom, zneužitie dôveryhodnosti, kontrola portov)	Získanie neoprávneného prístupu k sieti, systému, aplikačnému softvéru alebo iným zdrojom	Strata dôverných informácií
Denial-of-Service (DoS) a oneskorenie	Pokus o znemožnenie legítimného prístupu k hardvéru alebo softvéru,	Porucha prevádzky, strata produktivity

	znefunkčnení m danej služby	
Man-in-the-Middle (MTM)	Snaha o útočníka o odpočúvanie prenosu a zmenu správ medzi strojom a systémom	Fyzické poškodenie, zníženie kvality produktu, zranenie alebo smrť, strata dôverných informácií
Škodlivý softvér (napr. trójske kone, vírusy a červy)	Zničenie výrobného systému vložením programov so škodlivým úmyslom do výrobného systému	Prerušenie prevádzky, strata produktivity, fyzické poškodenie, znížená kvalita produktu, zranenie alebo smrť
Manipulácia s údajmi	Prístup a zmena citlivých údajov, ako sú kľúčové parametre digitálnych modelov a dokumentov	Fyzické poškodenie, zlá kvalita, zranenie alebo smrť

Po identifikácii hrozieb a zraniteľnosti nasleduje analýza ovládacích prvkov, ktorých implementácia sa snaží vylúčiť alebo minimalizovať pravdepodobnosť uplatnenia zraniteľného miesta. Bezpečnostné kontroly slúžia na zistenie, zníženie alebo minimalizovanie bezpečnostných rizík. Poznáme viacero metód kontroly. Jednou z nich je riadený prístup. Ide o selektívne obmedzenie k zdrojom a infraštruktúre. Ďalšou metódou je šifrovanie. Pri šifrovaní dochádza k procesu kódovania správ spôsobom, ktorý umožňuje prístup k správe iba oprávneným osobám. Známu metódou je aj overovanie, kde sa jedná o proces, v ktorom dochádza k porovnávaniu poskytnutých poverení a súborov uvedených v databáze. Poslednou zo spomenutých metód je dedukcia nepovolených vstupov. Táto metóda pozostáva z monitorovania aktivít v sieti alebo počítačovom systéme so zreteľom na možné bezpečnostné problémy.

Kyber-fyzické systémy (CPS)

Ďalšou z možností inteligentného riešenia výrobného procesu sú kyber-fyzické systémy (CPSz anglického cyberphysical system, kyber-fyzický systém). Ide o systém, ktorý umožňuje komunikáciu robotov a počítačov s reálnym svetom a to vďaka sieťovému prepojeniu. Tento systém je jedným z

hlavných znakov Industry 4.0. Rozvoj komunikačných a informačných technológií prispel k výskumu systémov kyber-fyzickej výroby (CPPS, z anglického cyber physical production system, kyber-fyzický systém výroby) a taktiež k podpore výrobných systémov s podporou Interentu vecí (IoT) a integrácie cloudov. I keď ide o rozdielne námety, všetky tieto myšlienky sa snažia o rozvoj stratégií výrobných systémov. [3]

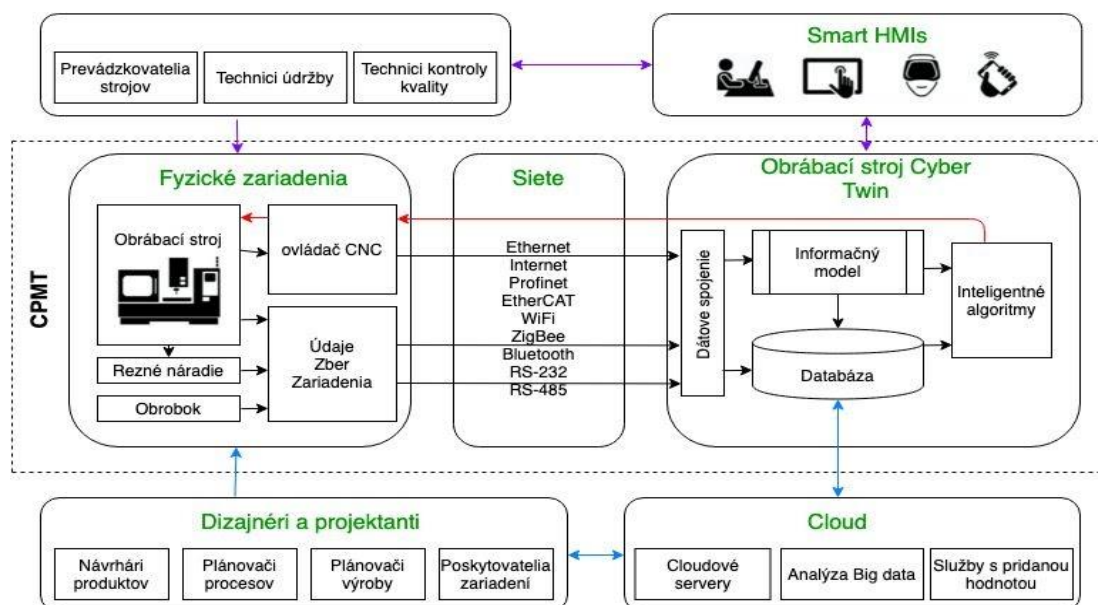
Tento systém je základom pre kyber-fyzické počítačovo riadené stroje. Tieto stroje poznáme aj pod názvom MachineTool 4.0 alebo Cyber-Physical MachineTools (CPMT, z anglického Cyber-Physical Machine Tools, kyber-fyzické obrábacie stroje) a reprezentujú novú generáciu obrábacích strojov. Ich základnými vlastnosťami sú dobrá konektivita, široká dostupnosť, pričom integráciou do systému dokážeme tvoriť inteligentné a autonómne riešenia.

Na Obr. 1 môžeme vidieť všeobecnú architektúru systému CPMT, ktorá umožňuje rozvoj existujúceho CNC obrábacieho stroja na CPMT. Farebné šípky znázorňujú väzby medzi fyzickým svetom, počítačovým priestorom a ľuďmi. Tieto väzby slúžia na zvýšenie výkonnosti a efektívnosti obrábacích strojov.

aplikáciách z dôvodu prerušenia výroby, nákladov na údržbu náhradných dielov a nedostatkov kvality.

Prediktívna údržba alebo podmienená údržba (CBM, z anglického Condition-Based Maintenance, Údržba založená na stave) sa líšia od preventívnej. Zakladá sa na potrebe údržby namiesto skutočného plánu. Preventívna údržba je časovo závislá na činnosti, ako je výmena maziva. Táto výmena je závislá na čase a to napríklad kalendárny čas alebo doba prevádzky zariadenia. Príkladom nám môže byť výmena motorového oleja v aute, kde väčšina ľudí ju uskutočňuje každých 3000 až 5000 km. Táto metodika by bola analogická úlohe preventívnej údržby. Ak na druhej strane, prevádzkovateľ vozidla znížil čas jazdy a mal olej analyzovaný v určitej periodicite, aby sa určil jeho skutočný stav a mazacie vlastnosti, môže byť schopný predĺžiť výmenu oleja, až kým vozidlo neprešlo 10 000 km. Toto je zásadný rozdiel medzi prediktívnou údržbou a preventívnou údržbou, pričom prediktívna údržba sa používa na definovanie potrebnej úlohy údržby na základe kvantifikovaného stavu materiálu, resp. zariadenia. [4]

CBM je založená na použití údajov prognostiky, manažmentu životnosti prístrojov v reálnom čase, na stanovenie priorít a optimalizáciu údržby zdrojov.



Obr. 1 Všeobecná architektúra systému CPMT [3]

Prediktívna údržba

Inovatívnym prvkom, ktorý predlžuje životnosť strojov a znižuje náklady na prevádzku, je prediktívna údržba. V súčasnosti sa väčšina údržbárskych prác vykonáva preventívnym alebo nápravným prístupom. Preventívny prístup má pevné intervaly údržby, aby sa zabránilo degradácii komponentov, subsystémov alebo systémov. Nápravná údržba sa vykonáva po zjavení poruchy. Oba prístupy sa ukázali ako nákladné v mnohých

Sledovaním systému vieme určiť jeho stav a konať iba vtedy, keď je nevyhnutná údržba. Pomocou CBM sa pracovníci údržby môžu rozhodnúť, kedy je správny čas na jej vykonanie. V ideálnom prípade CBM umožní personálu údržby robiť iba nevyhnutné úkony, z dôvodov minimalizovania nákladov na náhradné diely, prestojov systému a času stráveného údržbou. Oblasť inteligentných údržbárskych, diagnostických a prognostických mechanizmov CBM strojov je

životne dôležitá pre súčasné komplexné systémy v priemysle, kozmických vozidlách, vojenských a obchodných lodí, automobilovom priemysle a inde. Priemyselné a vojenské komunity sa zaujímajú o spoľahlivosť a dostupnosť kritického systému a komponentov. Cieľom je maximalizovať vybavenie a minimalizovať náklady na údržbu a prevádzku.

Deeplearning a strojové učenie

Deeplearning umožňuje automatické spracovanie údajov smerom k vysoko nelineárnej a komplexnej abstrakcii prvkov prostredníctvom kaskády viacerých vrstiev, namiesto ručného vytvárania optimálnej reprezentácie údajov pomocou znalosti domény. Vďaka funkcii automatického učenia funkcií a veľkoobjemového modelovania, poskytuje hlbkové vzdelávanie pokročilý analytický nástroj na inteligentnú výrobu v ére veľkých dát. Používa kaskádu vrstiev nelineárneho spracovania, aby sa naučil znázornenie údajov zodpovedajúcich rôznym úrovňam abstrakcie. Skryté vzory pod sebou sa potom identifikujú a predpovedajú pomocou optimalizácie end-to-end. Hlboké vzdelávanie ponúka veľký potenciál na podporu výrobných aplikácií založených na údajoch, najmä v období veľkých údajov. [9]

V deeplearning sa s rozširovaním výrobných údajov inteligencia založená na údajoch s pokročilou analýzou premieňa bezprecedentné objemy údajov na akčné a dômyselné informácie pre inteligentnú výrobu, ako je znázornené na Obr. 2.

nich podobnosti a tiež sa učí zužitkovať výsledky na ich zovšeobecnenie. Strojové učenie je systém, ktorý by mal dosiahnuť cieľ na základe vstupov vďaka vlastným rozhodnutiam. Táto časť umelej inteligencie sa používa vo viacerých oblastiach obchodu, zábavy a čoraz väčšmi v priemyselnom prostredí. Strojové učenie umožnilo počítaču nielen vykonávať vopred naprogramované úlohy, ale vie získavať vedomosti zo skúseností. [6]

Automatizácia

Jedným z možností inovácie je aj automatizácia. Tento pojem je zadaný ako technológia, ktorá súvisí s použitím elektrických, mechanických a počítačových systémov. Automatizácia sa rozdeľuje takto [1]:

- Tvrdá/fixná – ide o automatizáciu využívajúcu tradičné prepravné linky. Používa sa vo výrobe, kde výrobky dosahujú veľkú výrobnú rýchlosť. Počiatkové náklady tejto automatizácie sú vysoké, preto je ich možné rozdeliť na značne veľký počet jednotiek. Charakteristické pre túto výrobu je pevne stanovený návrh výrobného zariadenia, ktorý jasne definuje postupnosť výrobných operácií. Tvrdá automatizácia využíva pneumatikové, hydraulické, elektropneumatikové, elektrohydraulické zariadenia, aby tieto zariadenia zabezpečili čiastočnú automatizáciu, ktorá zabezpečila zníženie nákladov. Tieto náklady však nie sú dostatočne pružné, kvôli zložitosti zmeny postupu.



Obr. 2 Znázornenie Deeplearning [9]

Strojové učenie (ML, z anglického Machine learning, strojové učenie) je časť umelej inteligencie (AI, z anglického Artificial intelligence umelá inteligencia), ktorá sa zaoberá autonómnym získavaním počítačových znalostí. Vďaka tomuto učeniu vie počítač porozumieť dátam a získavať z

- Programovateľná – hovoríme o nej v tom prípade, ak je výrobné zariadenie vytvorené s možnosťou výroby podobných výrobkov. Ide o výrobnú postupnosť, ktorá je riadená uloženým programom, no na zmenenie produktu je potrebné výrazné

preprogramovanie a zmenu nástrojov. Ide o automatizáciu väčšiny výrobných procesov.

- Flexibilná – nazýva sa taktiež pružná a využíva sa v procesoch vyžadujúcich zmenu. Veľkou výhodou pružnej automatizácie je schopnosť rýchlejšie a pri menších nákladoch reagovať na požiadavky. Táto výhoda pružnej automatizácie pramení z využívania počítačov, procesorov, počítačovo riadených strojov a zariadení, ktoré sú programovateľné. Ide o číslicovo riadené stroje, súradnicové meracie stroje a roboty.

Záver

Správne inovovanie výrobného procesu je dôležité pre udržateľnosť postavenia spoločnosti na trhu. Pri inovovaní výrobného procesu musíme dbať na čo najefektívnejšie zlepšenie výrobného procesu pri čo možno najmenšej investícii. [6] Tým nemyslíme, že do inovovania netreba venovať výraznú investíciu, ale táto investícia musí byť hodná danej inovácie a jej návratnosť splniteľná. [2]

Zavádzaním inovácií vo výrobnom procese dochádza k zefektívneniu výroby a k zvyšovaniu kvality výrobkov. [9] Zabezpečuje to zvyšovanie technologickej a inovačnej úrovne v podniku. Môže ísť o inováciu existujúcej výrobnéj technológie alebo kúpu novej. Možnosti inovovania výrobných procesov je mnoho, ako napr. robotizácia a automatizácia výrobného procesu. Zavádzaním týchto prvkov sú vytvárané inteligentne riadené, vzájomné prepojené, autonómne systémy. [5]

Príspevok bol riešený v rámci projektu 009TUKÉ-4/2020 Transfer digitalizácie do vzdelávania v študijnom programe Riadenie a ekonomika podniku.

Literatúra

- [1] Black, J. T., Hunter, S. L.: *Lean Manufacturing Systems and Cell Design*. Society of Manufacturing Engineers: 336 p. ISBN 978-0872636477. 2003.
- [2] Fusko, M., Rakyta, M., Krajcovic, M., Dulina, L., Gaso, M., Grznar, P.: *Basics of designing maintenance processes in industry 4.0*. MM science journal, pp. 2252-2259. 2018. ISSN 1803-1269
- [3] Liu, C., Vengayil, H., Zhong, R.Y. and Xu, X.: A systematic development method for cyber-physical machine tools. *Journal of Manufacturing Systems*, 48, pp.13–24. ISSN 0278-6125. 2018.
- [4] Matalíková, M.: *Inteligentné riešenia výrobného procesu*. Bakalárska práca. TU SJF v Košiciach. 52 s. 2020.
- [5] Radhakrishnan, P.: *Computer Numerical Control Machines and Computer Aided Manufacturing*, New Academic Science, 454 p, ISBN 978-1781830154, 2014.
- [6] Sharp, M., Ak, R. and Hedberg, T.: A survey of the advancing use and development of machine learning in smart manufacturing. *Journal of Manufacturing Systems*, 48, pp.170–179. 2018. ISSN 0278-6125
- [7] Straka, L.: *New Trends in Technology System Operation*. Proceedings of the 7th conference with international participation, Presov, pp. 385, 2005.
- [8] Šutaj-Eštok, A., Liberko, I., Sirková, M.: *Process management in relation to the systems thinking*. In: *Management 2012 : research management and business in the light of practical needs*. - Prešov : Bookman, 2012. p. 214-218. ISBN 978-80-89568-38-3.
- [9] Wang, J., Ma, Y., Zhang, L., Gao, R.X. and Wu, D.: *Deep learning for smart manufacturing: Methods and applications*. *Journal of Manufacturing Systems*, 48, pp.144–156. ISSN 0278-6125. 2018.
- [10] Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X. and Terpenney, J.: *Cybersecurity for digital manufacturing*. *Journal of Manufacturing Systems*, 48, pp.3–12, ISSN 0278-6125. 2018.
- [11] Xu, X.: *Machine Tool 4.0 for the new era of manufacturing*. *Int J Adv Manuf Technol* 92, 1893–1900, 2017. <https://doi.org/10.1007/s00170-017-0300-7>.
- [12] Zhang, J., Wang, P., Yan, R. and Gao, R.X.: *Long short-term memory for machine remaining life prediction*. *Journal of Manufacturing Systems*, 48, pp.78–86. 2018.