

# Folyamatalapú, szabványos irányítási rendszerek a biztonságos és rugalmas vállalati működésért

Michelberger Pál 

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, Magyarország  
E-mail: michelberger.pal@bgk.uni-obuda.hu

Beérkezett: 2023. február 3.; Elfogadva: 2023. február 16.; Online megjelent: 2023. május 25.

## Összefoglalás

Háborús helyzet, pandémia, nem mindig rendelkezésre álló energiahordozók és alapanyagok, infláció, szakképzett munkaerő hiánya és ingadozó rendelésállomány határozza meg a termelő vállalatok külső és belső környezetét. A változások sokszor szinte lehetetlenné teszik a nyereségességet és likviditást elváró vállalati tervezést. Válsághelyzetben, korlátozottan rendelkezésre álló és gyorsan változó árú erőforrások esetén előtérbe kerül a működőképesség fenntartása és az üzleti partnerek túlélése. A tanulmány néhány menedzsmenteszközt és trendet vesz számba, amelyek segíthetnek a nehéz helyzetbe került gazdálkodó szervezeteknek.

**Kulcsszavak:** folyamatbiztonság, ipar 4.0, szabványos irányítási rendszer, kockázat, üzletmenet-folytonosság

## Process-based, standardized management systems for secure and resilient corporate operations

Pál Michelberger

Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary

## Summary

War situations, pandemics, limited availability of energy and raw materials, inflation, shortage of skilled labor, and fluctuating stock order, all determine the external and internal environment of manufacturing companies. Hectic changes often make classical corporate planning, which is based on meeting economic objectives (profit, liquidity), almost impossible. In a crisis situation, with limited resources and rapidly changing prices, the focus is on maintaining functionality, taking into account the survival of business and technological partners. The paper will take stock of some industrial management tools and trends that can bail out seemingly hopelessly distressed business organizations. In addition to articles and textbooks on enterprise and process security, a number of management standards and recommendations for resilience and control business and technology processes have been included in the bibliography. Managers have a triple challenge in this area; to select, integrate and implement management systems that meet the expectations of business partners and help optimize and flexibly transform internal value-creating and service-providing processes on demand. Process management that has been developing in recent decades is not a miracle set in crisis situation. The application of management methods, standards, and the recognition of business and technological trends do not guarantee that substitute resources will be sufficient in the right place and time, and that profitable operations will remain sustainable. However, process-oriented companies with controlled resource allocation and business continuity in mind are more likely to survive times of crisis. Their built-in process control systems bring faster reactions to disadvantageous changes.

Complex production systems are moving towards error-free production. Failures, production and logistical disruptions can be detected more quickly and the root causes localized. Industry 4.0 has several technological components, the integration of which is exploited by these modern industrial production systems. Industry 5.0 focuses on human-machine collaboration and relies on the tools of Industry 4.0. Skilled workers with robots create unique products in the division of labor. Industry 5.0 does not mean the automatic, immediate replacement of old technologies. Previous equipment and production systems can also be integrated into a network using sensors. The coordination of standardised management systems with the technological shift of Industry 4.0 is not a bypass.

**Keywords:** process security, industry 4.0, standardised management system, risk, business continuity

## Bevezetés

A múlt század nyolcvanas éveitől kezdve előtérbe került a folyamatorientált vállalati működés. A korábbi nyereség- és/vagy árbevétel-centrikusság mellett a hatékonyság, a minőség, az üzleti és technológiai folyamatok kontrollált végrehajtása ugyanolyan fontos lett.

A vállalati célok zavartalan külső környezet esetén is többféleképpen differenciálódnak:

- Általában az egyik legfontosabb stratégiai cél a hosszú távú profitmaximalizálás.
- A marketingtevékenységekkel megbízott szervezeti egységek a fogyasztói igények meghatározására és minél teljesebb kielégítésére törekszenek.
- A folyamatos termék- és technológiai innováció biztosíthatja a termelő és/vagy szolgáltató vállalat hosszabb távú túlélését.
- A szervezet „napi”, operatív irányítása (termelés-szervezés, tárgyi eszköz-, munkaerő- és forgóeszköz-gazdálkodás) alapozza meg a folyamatos működést.
- A jogszabályi környezet (pl. környezetvédelem), annak betartása is befolyásolhatja a vállalati célokat.
- Az „önként vállalt” lean szemlélet a takarékoság jegyében és a pazarlás megszüntetése érdekében módosíthatja a tradicionális üzleti, logisztikai és technológiai folyamatokat (*Kilpatrick 2003*).

## Folyamatcentrikus vállalati működés

A folyamatcentrikus vállalatok biztonságos működését számos elméleti megalapozás, eszköz, módszer, szabvány és ajánlás támogatja. A gazdálkodó szervezetek feladata, hogy ebből a széles kínálatból olyan szabályozott működést alakítsanak ki, amelyek a turbulens környezeti változások között is növelik a vállalatok ellenálló képességét, és biztonságot mutatnak az üzleti, kormányzati partnerek felé.

„A folyamatbiztonság olyan állapotnak tekinthető, ahol az előírt bemenetek (erőforrások) biztosítása után a folyamat tevékenységeit végrehajtó szervezeti egységek az előírt időben megfelelő mennyiségű és minőségű kimenetet nyújtanak és zavar esetén a folyamat normál működése a lehető legkisebb erőforrás ráfordítással és a legrövidebb idő alatt helyreállítható.” (*Michelberger 2014: 402*)

A folyamatbiztonság kialakítását segítő komponensek megjelenése időrendben (a teljesség igénye nélkül):

- Porter-féle értéklánc modell (*Porter 1985*),
- Business Process Reengineering – BPR (*Hammer-Champy 1993; Tenner-DeToro 1997*),
- Tranzakciókezelő információs rendszerek (*Wallace-Kremzar 2001*),
- Kontrolling rendszerek (*Malina-Selto 2001*),
- Szabványos irányítási rendszerek és integrált bevezetésük (*Labodova 2004*),
- Folyamat menedzsmentet támogató információs rendszerek (*Rob 2008*),

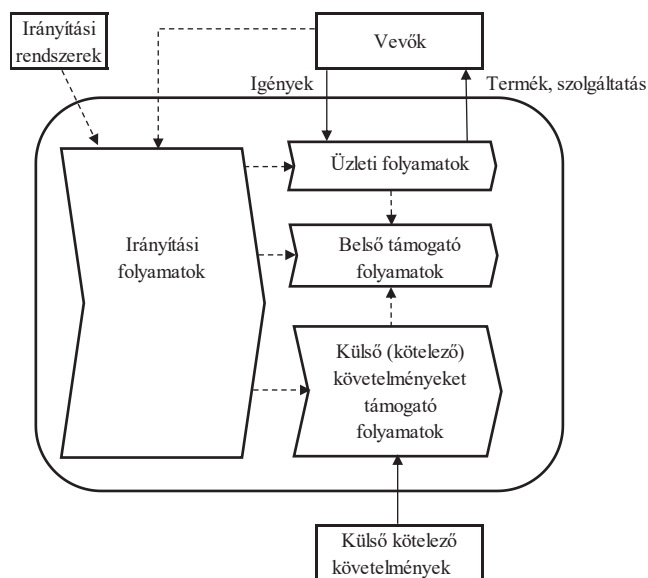
- VUCA környezeti kockázat-elemzés (*Bennett-Lemoine 2014*),
- Teljesítménymutatók (KPI-ok) előírása és monitorozása (*van der Aalst-La Rosa-Santoro 2016*),
- Üzletmenetfolytonosság-menedzsment és vállalati rugalmasság (rugalmas ellenálló képesség – resilience) (*Corrales-Estrada et al. 2021*).

A vállalati folyamatok állandó ellenőrzésére, értékelésére és fejlesztésére jó eszköz lehet az ISO/IEC 33000-es szabványcsomag, amely az üzleti és technológiai folyamatokat hatos skálán értékeli és hozzárendeli a lehetséges (ALACSONY, KÖZEPES és MAGAS) kockázati szinteket:

0. szint – hiányos folyamat (a folyamat céljának teljesülése bizonytalan – MAGAS KOCKÁZAT)
1. szint – végrehajtott folyamat (a folyamatnak biztosan lesz valamilyen értékelhető eredménye – MAGAS v. KÖZEPES KOCKÁZAT)
2. szint – irányított folyamat (a folyamat és annak eredménye is megfelelően kezelt – MAGAS v. KÖZEPES KOCKÁZAT)
3. szint – kialakított folyamat (a folyamat valamilyen belső szabvány alapján megtervezett és végrehajtott – KÖZEPES v. ALACSONY KOCKÁZAT)
4. szint – kiszámítható folyamat (a folyamat mérhető és ellenőrizhető – KÖZEPES v. ALACSONY KOCKÁZAT)
5. szint – optimalizáló folyamat (a folyamat céljai teljesülnek, megjelenik a „visszacsatolás” – ALACSONY KOCKÁZAT)

Ma az üzleti folyamatok tervezése, dokumentálása és követése is olyan mennyiségű adattal jár, amit informatikai háttér – „Business Process Management” (BPM) rendszerek – nélkül nagyon nehéz kézben tartani. A folyamatleírások alapjait nagyon sokszor a korábban megírt szabályzatok adják, amelyek gyakran nem a teljes folyamatra vonatkoznak, hanem egy-egy szervezeti egység összegyűjtött feladataira. Ez pedig felesleges redundanciákat jelent mind a folyamatokban, mind a végrehajtásukhoz szükséges erőforrásokban, és nem optimalizált folyamatmodelleket eredményez. A BPM rendszerek ebben is segítséget nyújthatnak. Támogatják a folyamatok átláthatóságát, eredményességük mérhetővé tételét, a folyamatok állandó fejlesztését és a változó körülményekhez való alkalmazkodását (*Ányos 2017a*).

Az üzleti folyamatok külső ügyfél igényeinek kielégítését végzik, a vevőnek értéket teremtenek. A belső támogató folyamatok a szervezet többi folyamata számára széleskörűen értelmezett erőforrásokat biztosítják. A külső követelményeket támogató folyamatok a jogszabályi megfelelést szolgálják. Az irányítási folyamatok a szervezet belső követelményeit határozzák meg (stratégia, üzleti tervezés) és a teljesítménymérést is megalapozzák, valamint a „Plan-Do-Check-Act” (tervezés-végrehajtás-ellenőrzés-beavatkozás) ciklus alapján folyamatok állandó fejlesztését is biztosítják (*1. ábra*). A követelmények lehetnek kötelezőek vagy önként vállaltak. Egy



1. ábra | Vevői igények, külső követelmények és folyamatok  
Forrás: Ányos (2017b) alapján.

követelmény vonatkozhat folyamat outputjára (termékre és/vagy szolgáltatásra), de akár egy (technológiai) belső támogató folyamatra is. A követelmény az előre definiált folyamat végrehajtása által teljesül (Ányos 2017b).

## Vállalati erőforrás-tervezés

A gyártási erőforrás-tervezés (Manufacturing Resource Planning – MRP) a termeléshez szükséges erőforrások előzetes meghatározásán és biztosításán alapszik (Chikán–Demeter 2001). A piaci igények és kibocsátási lehetőségek összehangolásával működik, alapja az erőforrás-termék mátrix, ami egy egyszerűsített statikus modell és a lineáris programozást kihasználva segítheti a gazdálkodó szervezetek számára az optimális termékszerkezet kialakítását (Starr 1976). Változó feltételrendszer esetén ennek a mátrixnak és módszernek a dinamizálása mindenképpen szükséges. A termékportfólió (mennyiségek) és a rendelkezésre álló erőforrások változhatnak. Különösen igaz ez pandémiás vagy háborús helyzetekben, ahol a logisztika nehezen birkózik meg a bizonytalansággal (alapanyag-, energia-, munkaerőhiánnyal és azok beszerzési költségeinek hektikus változásaival stb.). A megrendelők piaci helyzete is bizonytalan. Gyakran ők is módosítanak a megrendeléseken. Ilyenkor a termelő vállalatok több, opcionális erőforrás-termék kapcsolati mátrixot is lefektetnek és az erőforrás rendelkezésre állásának (kapacitások) változása függvényében a termék kibocsátás ideje és mennyisége változhat. A rugalmasság és az állandó kommunikáció az ellátási és értékesítési lánc minden szereplőjével szemben alapkövetelmény lesz. A hosszabb távú üzleti, logisztikai kapcsolatok már nem rögzített áron és jó előre lekött mennyiségekkel operálnak, hanem javasolt a változó erőforrásköltségeket

is figyelembe vevő (minimum és maximum értékeket megadó) „ársávok” és naprakész mennyiségi egyeztetések alkalmazása. Ez szinte csak a vállalati erőforrás-tervező rendszerek (Enterprise Resource Planning System) szabályozott adatcseréjével, kommunikációjával lehetséges. A termelési és technológiai folyamatoknál kiemelkedő szerepet kap a naprakész önköltséget és értékesítési árat meghatározó elő-, együtt futó- és utókalkuláció.

Az utóbbi évtizedek divatos LEAN filozófiája (karcsúsított termelés) átértékelődik. A vállalatok a bizonytalan beszerzési háttérű erőforrásoknál inkább választják a saját készletezést, mintsem a napjainkban kevésbé megbízható „just in time” beszállítói szolgáltatást. A nagyobb tárolási költségek még mindig kisebbek, mint a szállítási késésekből adódó kötbér, a gyorsan emelkedő beszerzési árak és a hiány „költsége”. A gyártókapacitások túlterhelése és működési zavarai esetén a klasszikus termelésirányítói kockázatkezelés a technológiai opciók összegyűjtését és ráfordítás szerinti rangsorolását jelenti:

1. belső, alternatív technológiai lehetőségek kihasználása, technológiai áttervezés (lehet, hogy drágább és/vagy lassúbb stb.),
2. időalapok növelése a kieső erőforrás rekonstrukciója után (túlóra, további műszakok elrendelése),
3. gyártás (ideiglenes) kihelyezés, külső erőforrások (kooperációs partner) igénybevételével,
4. konstrukciós változtatás, a termék áttervezése,
5. kapacitásbővítés (termelőeszköz beszerzése és/vagy munkaerő-felvétel).

## Szabványos irányítási rendszerek

A vállalati célrendszer zavartalan külső körülmények között is többszörösen differenciált. Az egyik stratégiai cél mindenképpen a hosszú távú nyereségmaximalizálás. A fogyasztói igények kielégítése jelenti a marketingcélokat. A folyamatos termék- és technológiai innováció biztosíthatja a vállalat hosszú távú fennmaradását, míg a napi operatív gazdálkodási feladatok (termelésmenedzsment, tárgyieszköz-, munkaerő- és forgóeszköz-gazdálkodás) megoldása hozhatja a napi „túlélést”. Erre rakódik rá a jogszabályi követelményeknek való megfelelés, a környezetvédelem és általában a külső partnerek által elvárt menedzsmentrendszerek üzemeltetése.

A nemzetközi szabványügyi testület (International Organization for Standardization) az elmúlt években, évtizedekben sok auditálható és tanúsítható menedzsment-, magyarul irányítási rendszert alakított ki és fejlesztett folyamatosan tovább a minőség-, a környezet-, az információbiztonság-, az élelmiszer-biztonság-, az ellátási láncok működtetése és az üzletmenet-folytonosság, valamint a munkahelyi egészségvédelem területén. Az irányítási rendszerek folyamatközpontúak. Hasonló felépítésük miatt integrálhatók, elkerülhetővé téve a többszörös folyamatszabályozást és túl gyakori háromévenkénti irányítási rendszerenként megszerzett külső auditokat. A tanúsított szervezetek/vállalatok száma fo-

1. táblázat | Szabványos tanúsított irányítási rendszerek a világban és Magyarországon 2021-ben

Jelzet	Szabványos irányítási rendszerek 2021-ben	Összes érvényes tanúsítvány, világszinten	%	Magyarországi, érvényes tanúsítvány	%
ISO 9001	Minőségirányítási rendszer	1 077 884	55,06%	7 856	56,16%
ISO 14001	Környezetközpontú irányítási rendszer	420 433	21,48%	3 279	23,44%
ISO 45001	Munkahelyi egészségvédelem és biztonságirányítási rendszere	294 420	15,04%	1 263	9,03%
ISO/IEC 27001	Információbiztonság-irányítási rendszer	58 687	3,00%	661	4,73%
ISO 22000	Élelmiszer-biztonsági irányítási rendszer	36 124	1,85%	128	0,92%
ISO 13485	Orvostechikai eszközök. Minőségirányítási rendszer	27 229	1,39%	108	0,77%
ISO 50001	Energiairányítási rendszer	22 575	1,15%	626	4,47%
ISO/IEC 20000-1	Informatika. Szolgáltatásmenedzsment	11 769	0,60%	27	0,19%
ISO 37001	Antikorrupciós irányítási rendszer	2 896	0,15%	23	0,16%
ISO 22301	Üzletmenet-folytonossági irányítási rendszer	2 559	0,13%	11	0,08%
ISO 39001	Közúti közlekedésbiztonsági irányítási rendszer	1 285	0,07%	0	0,00%
ISO 28000	Biztonság és ellenálló képesség – biztonságirányítási rendszer	584	0,03%	1	0,01%
ISO 55001	Vagyongazdálkodás – irányítási rendszer	488	0,02%	4	0,03%
ISO 20121	Fenntartható eseménymenedzsment – irányítási rendszer	253	0,01%	0	0,00%
ISO 29001	Kőolaj-, petrokémiai és földgázipar – minőségirányítási rendszer	157	0,01%	2	0,01%
ISO 44001	Együttműködési irányítási rendszer az üzleti kapcsolatokhoz	136	0,01%	0	0,00%
Összesen		1 957 479	100,00%	13 989	100,00%

Forrás: The ISO Survey of Management System Standard Certifications, 2021

lyamatosan növekszik világszerte (*The ISO Survey of Management System Standard Certifications, 2021*). A külső, független tanúsító szervek által adott igazolások bizonyítják a rendezett és ellenőrizhető vállalati működést, valamint erősíthetik az üzleti bizalmat (*1. táblázat*). Sokszor az üzleti kapcsolat létrejöttének feltétele egy-egy irányítási rendszer megléte. Az irodalomjegyzékben megtalálhatók a jelenleg is érvényes, nemzetközi szabványügyi testület által jegyzett irányítási rendszereket leíró jelentősebb szabványok angol és – ahol a honosítás megtörtént – magyar nyelvű jelzetei.

A gazdálkodó szervezetek olykor sajátos folyamataikra képesek lehetnek speciális és egyedi irányítási rendszerek kialakítására és üzemeltetésére. A közismert, esetenként auditálható és független fél által tanúsítható szabványok és ajánlások az üzleti partnerek számára azonban nagyobb bizalmi tényezőt jelentenek és jobban is ellenőrizhetőek. A nemzetközi szabványügyi testület (ISO) a szabványok folyamatos fejlesztésével, harmonizációjával serkenti is az ilyen irányítási rendszerek alkalmazását.

A különböző menedzsmentrendszerek alkalmazása és kialakítása országonként, földrészenként és iparáganként nagyon eltérő. (Nem csak az ISO ajánl szabványos menedzsmentrendszereket, folyamat alapú vállalati működést támogató módszertanokat.) Számos esetben kialakításuk és működtetésük a külvilág számára nem látható. Új belépők, tanúsítványt elvesztők folyamatosan alakítják ezeket a számsorokat. Az ISO-felmérésben szereplő

számok vélhetően nem az összes irányítási rendszert tartalmazzák. (Pl. vannak olyan cégek, amelyek nem kérkednek a meglévő információbiztonsági irányítási rendszerükkel, hiszen az védendő információk jelenlétére utal, amelyek mások számára is értékesek/érdekesek lehetnek...)

Az irányítási rendszer kialakítása és fenntartása többletmunkát jelent a szervezet számára. Fontos a környezeti (piaci) elvárások és a belső szervezeti kultúrának is megfelelő szabványcsomagok kiválasztása. Túlszabályozás és a tulajdonosok/menedzsment által támasztott túlzott elvárások (pl. irracionális nyereség vagy forgalom, piaci terjeszkedés, technológiaváltás) összeroppanthatják a céget.

## Üzletmenet-folytonosság

Az ISO 22301-es brit eredetű üzletmenet-folytonossági irányítási rendszer kialakítását lehetővé tevő szabvány. A hagyományos PDCA ciklus alapján 21 lépésben és ezen belül 101 tevékenységben adja meg az üzletmenet-folytonosság tervezésének követelményeit. Minden szervezetre alkalmazható. A potenciális veszélyek, fenyegetések és kockázati tényezők feltárása az alapja a folyamatosan fejlesztett és ellenőrzött, ún. üzletmenet-folytonossági tervnek (Business Continuity Plan – BCP). Az üzleti hatáselemzés (Business Impact Analysis – BIA) során vizsgálják a cég fontos termékeit, annak előállítás lépéseit és a belső szolgáltatásokat támogató folyamato-

kat. Elemzik az üzleti, termelési, illetve szolgáltatási tevékenységek fennakadásának lehetőségeit, a leállás várható időtartamát és a külső partnerektől való függőséget. Váratlan események (pl. katasztrófahelyzet, erőforráshiány, közművek működési zavarai, technológiai berendezések meghibásodása, IT-problémák, vevői reklamációk) sem okozhatnak gondot, hiszen a BCP-ben megfelelő, ideiglenes helyettesítő megoldások vannak megnevezve (Godányi 2004). A BCP világos és értelmezhető leírás üzletmenetet befolyásoló esemény bekövetkezése utáni tennivalókról a korábban megnevezett felelősök számára. Minden olyan információt tartalmaz, ami a normál működés helyreállításához szükséges (erőforrások, időadatok, szolgáltatási szintek).

## Külső és belső kockázatok integrált elemzése és kezelése

Számos vállalati területnek (pl. információbiztonság, minőségmenedzsment, környezetirányítás, munkahelyi egészségvédelem, karbantartás, pénzügy, termelés) sajátos kockázatkezelési gyakorlata van, ami sok esetben egymástól független és a gazdálkodó szervezet működését többszörösen megterheli. A kockázatmenedzsment a vállalat (szervezet) külső és belső környezetére egyaránt vonatkozik. Indokolt tehát a kockázatok kezelésének holisztikus és integrált megközelítése (Iványos 2014). A kockázati kategóriák azonban gyakran összefüggnek egymással, szétválasztásuk nem is mindig indokolt vagy lehetséges (pl. egy magasán képzett, értékes munkaerő elvesztése). A legfontosabb az, hogy minden, a szervezetet és annak működését érintő lényeges kockázatot azonosítsunk (Erazo-Chamorro et al. 2022). Ugyanannak a kockázatnak a különböző funkcionális területeken más és más lehet az értékelése és kezelése. Javasolt egy szervezetnek egységes kockázatmenedzsment módszertant alkalmazni. A különböző kockázattípusoknál összemérhető módon, azonos skálán kell a kockázatokot értékelni. Ugyanannak a fenyegetettségnek a bekövetkezési valószínűségeit szinkronizálni és a különböző területekre vonatkozó hatásokat egyeztetni szükséges. Korábban be nem következett kockázati események valószínűségét és káragságát pontosan mérni vagy kiszámolni nem lehetséges, ezért javasolt az elemzés során ezeket inkább

kockázati osztályokba sorolni. Az osztályozási rendszerrel közismert szakmai dokumentum vagy szabvány előírásainak alkalmazását tartom célszerűnek az üzleti, technológiai és logisztikai partnerek kockázatmenedzsmentbe történő bevonása miatt.

A jól ismert ISO 31000-es általános szabvány mellett egy nyilvánosan elérhető amerikai katonai szabvány (MIL-STD-882E) egyszerű kockázati esemény besorolást javasol (2. táblázat).

A kockázati esemény bekövetkezési valószínűsége lehet: lehetetlen (eliminated), valószínűtlen (improbable), csekély (remote), alkalmi (occasional) és valószínű (probable), valamint gyakori (frequent).

A következmények súlyosságát négy csoportba sorolja a szabvány; elhanyagolható (negligible), nem jelentős (marginal), kritikus (critical) és katasztrófális (catastrophic).

A kockázati szint – az előző két tényező függvényeként – lehet elhanyagolható (eliminated), alacsony (low), közepes (medium) és súlyos (serious), valamint magas (high).

## Ellátási és értékesítési láncok

Az ellátási lánc kockázata olyan potenciális események, zavarok bekövetkezése az ellátási láncon belül és annak környezetében, amelynek veszélybe kerül a vevői igény kielégítése vagy a vevő biztonsága is. A hagyományos kockázati megfontolás (a bekövetkező kockázati tényezőből származó kár nagysága és a kockázati esemény valószínűsége) mellett használják a „sebezhetőség” fogalmát is.

A kockázatokot, illetve az ellátási láncok sebezhetőségét eredetük alapján öt csoportba lehet sorolni (Christopher–Peck 2004):

1. értékteremtő folyamatok zavarai (gyártás, beszerzés, raktározás, szállítás, ütemezés),
2. ellenőrzés (annak hiánya, illetve hibája),
3. piaci igények (információhiány, kiszámíthatatlanság, váratlan események),
4. beszállítók (megbízhatatlanság, kapacitáshiány, vis maior),
5. környezet (gazdasági, politikai események, balesetek, természeti katasztrófák).

2. táblázat | Kockázatértékelési mátrix

Valószínűség	1 – Katasztrófális	2 – Kritikus	3 – Nem jelentős	4 – Elhanyagolható
A – Gyakori	Magas	Magas	Súlyos	Közepes
B – Valószínű	Magas	Magas	Súlyos	Közepes
C – Alkalmi	Magas	Súlyos	Közepes	Alacsony
D – Csekély	Súlyos	Közepes	Közepes	Alacsony
E – Valószínűtlen	Közepes	Közepes	Közepes	Alacsony
F – Lehetetlen	Elhanyagolható	Elhanyagolható	Elhanyagolható	Elhanyagolható

Forrás: MIL-STD-882E szabvány.

Ezt további két kockázat „forrás” egészíti ki. A belső vállalati szervezet szintén sebezhető, ha az nem felel meg a kialakított értékteremtő folyamatoknak, és nem jól használja az információs rendszereket. Az ellátási lánc tagjai között is előfordulhatnak együttműködési zavarok mind az információ-, mind az anyagáramlásban. A több, önálló vállalatból álló hálózat is kockázati tényezőt jelent

Az amerikai Supply Chain Council (Supply-Chain-Operations-Reference-Modell) által megfogalmazott definíció alapján az ellátási lánc minden olyan tevékenységet magában foglal, amely a termék előállításával és kiszállításával kapcsolatos, a beszállító beszállítójától kezdve a végső fogyasztóig bezárólag. Az öt fő folyamat, amely meghatározza az ellátási láncot (APICS 2017):

1. tervezés (a kereslet-kínálat elemzése és a termékek, illetve szolgáltatások előállításának minőségi, mennyiségi és időrendi meghatározása),
2. beszerzés (alapanyag, alkatrész és kooperációs szolgáltatások),
3. gyártás (alkatrészgyártás és szerelés),
4. kiszállítás (készletezés, rendelésfeldolgozás, elosztás, valamint a végső fogyasztó kiszolgálása),
5. visszazállítás (hibás, felesleges és karbantartandó termékek kezelése, illetve vevőszolgálati tevékenység).

Az ellátási láncot alkotó szervezetek eredményei nem egyszerűen összeadódnak, hanem az erőforrás-allokációból adódóan a gazdálkodás különböző területein egymást felerősítő szinergikus hatások alakulnak ki. Ez azonban a kockázatokra is igaz. Az ellátási lánc menedzsentje a vállalatok tudatos együttműködését jelenti. Elfogadják, hogy annak léte versenyelőzést eredményez. A lánc tagjai hajlandók lemondani rövid távú előnyöket hozó egyéni érdekeik érvényesítéséről a teljes lánc optimális működésének érdekében. Ez közös kockázatkezelést és komplex „ellátás” biztonságot eredményező védelmi tevékenységet is feltételez. Ennek szabályozásában nyújthat segítséget az ISO 28001-es szabvány, amely az ellátási láncok biztonságirányítási rendszerére vonatkozó követelményeket is tartalmazza.

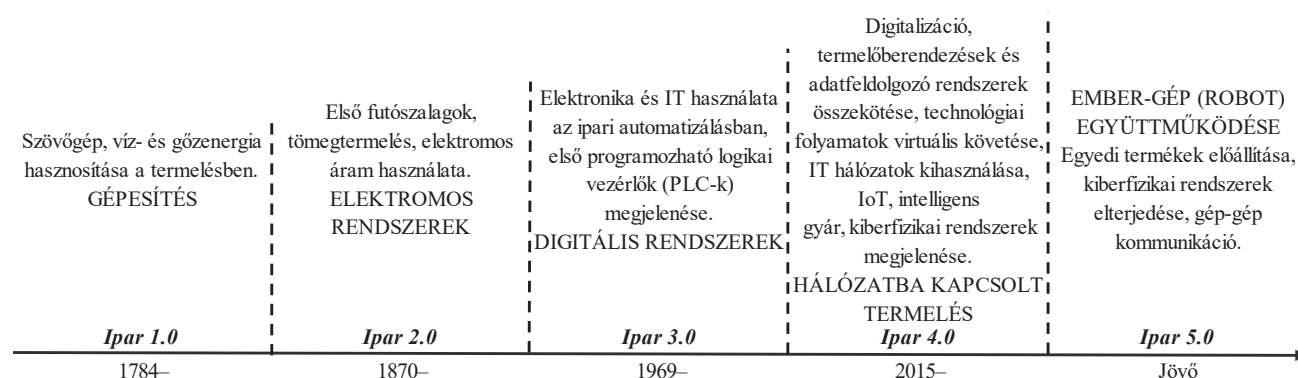
Az ellátási láncokban fontosabb a teljes hálózat hatékony működése, mint a tagvállalatok egyéni erőforrás felhasználási optimuma. Ez bevált CPFR (Collaborative Planning, Forecasting and Replenishment) folyamatmodell alapján arra készíti a vállalatokat, hogy együttműködjenek. A szükséglettervezés alapja a végső fogyasztói igény. A modell alkalmazása egy konszenzuson alapuló előrejelzést eredményez, amely azután meghatározza a disztribúció, a termelés és a beszerzés tagokra is lebontott terveit. Az ellátási lánc tagjai törekednek arra, hogy az előrejelzés alapját szolgáló adatok minél pontosabbak legyenek. Ez az ellátásbiztonságot is javítja (Hollmann-Scavarda-Thomé 2015).

A gyakorlatban a vállalatok „bizonytalan” beszállítói háttér esetén ugyanazt az alapanyagot vagy alkatrészt több (2-4) szállítótól is megrendelhetik. Sok esetben kevertrendeléseket alkalmazva, amelyekben kapacitástartalék biztosítását is kikötik. Zavar vagy hibás teljesítés (mennyiség, minőség, szállítási határidő) esetén a megbízható beszállítók rávehetőek a hibázó „konkurens” feladatainak átvételére.

### Ipar 4.0 és 5.0

A tanulmánynak nem célja az Ipar 4.0 új definíciójának megalkotása. Elfogadom Kovács Olivér – nem csak technológiai szempontokat figyelembe vevő – komplex, korábbi tudományos munkákat és szakmai/politikai szervezetek meghatározásait is magába integráló megfogalmazását.

„Az Ipar 4.0 szintetizáló jellegű definíciója: a dolgok és szolgáltatások internetére (IoT) építő új gyártási filozófia és működési mód, amely során okos gyárak (smart factories) jönnek létre azáltal, hogy az erőforrásokat, a gépeket és még a logisztikai rendszereket is online integrált rendszerré, egyfajta kibernetikai rendszerré kötik össze. Ily módon pedig független és optimalizáló helyi termelési folyamatokat hozunk létre. A helyi azt jelenti, hogy különböző technológiák révén maguk az egyes gyártóegységek is okosakká válnak, és központi helyett helyi – azaz decentralizált – ellenőrzés valósul meg.” (Kovács 2017a: 825)



2. ábra Ipari forradalmak  
 Forrás: saját szerkesztés, Oláh-Popp-Erdei, 2019 alapján

A folyamatbiztonságot szolgálja az állandó, decentralizált, szinte minden gyártási paraméterre kiterjedő ellenőrzés és a termelési tevékenységeket leíró adatok visszakereshetősége. A komplex termelőrendszerek elindulnak a hibamentes gyártás felé. A hibák, termelési és logisztikai zavarok gyorsabban felderíthetők és a kiváltó okok lokalizálhatók. A kibernetikai rendszerek (Cyber Physical System – CPS) esetében a termékek beépített szenzorok alkalmazásával tudnak információkat közölni pillanatnyi állapotukról és helyzetükről valamint kommunikálni egymással és a gyártó rendszerekkel.

Az Ipar 4.0-nak több technológiai komponense van, amelyek integrációját ezek a korszerű ipari termelőrendszerek kihasználják:

- Big Data és az ott szereplő (termelési) adatok gyors elemzése döntés-előkészítéshez,
- szenzorokkal felszerelt autonóm termelő robotok, gépek,
- logisztikai és termelési szimulációk (pl. termelés-tervezés ellenőrzésére),
- horizontális integráció (ellátási és értékesítési láncok szereplőinek „bekapcsolása” a gyártásba),
- vertikális rendszerek (ember-gép-egyéb belső erőforrások) integrációja,
- Dolgok Internete (Internet of Things – IoT),
- információbiztonság (bizalmasság, sértetlenség és rendelkezésre állás),
- felhőtechnológiák alkalmazása,
- 3D-s nyomtatás (ún. additív technológiák) alkalmazása,
- virtuális elemek beillesztése valós környezetbe (kiterjesztett valóság).

Vannak olyan iparágak, amelyek tradíciójuk (igény a tömegtermelés fenntartására) és költségesnek ígérkező technológiaváltásuk miatt nem tudnak (vagy mernek) maradéktalanul átállni Ipar 4.0-ra. A termelés rugalmasabbá tétele nem mindig lehetséges az elvárt mértékben. Ez részben a gyártó- és logisztikai rendszerek heterogén, nehezen összeépíthető elemeivel és a bizonytalan, gyorsan változó környezettel, valamint a kevésbé rugalmas humán erőforrással is magyarázható. A „VUCA” betűszó négy angol kifejezés kezdőbetűjéből ered (Volatility – változékonyság; Uncertainty – bizonytalanság; Complexity – komplexitás; Ambiguity – kétértelműség). A fogalmat az amerikai hadseregben kezdték el használni a 20. század végén, elsősorban a kiszámíthatatlan, gyorsan változó környezetre (harcászati helyzetre) vonatkoztatva. Azóta már megjelent a vállalati logisztikában és az ellátási láncok működésében is (Packowski 2014). Olyan gazdasági és természeti környezetben élünk, ahol a változás, bizonytalanság és a kiszámíthatatlanság állandó csak (Çiçeklioğlu 2020). A VUCA környezet megnehezíti a vezetői előrelátást (Pató Gáborné Szűcs-Kovács-Aboonyi 2021). A beérkező, gyorsan feldolgozott és továbbadott információk mindenképpen szükségesek a környezeti változásokra történő megfelelő reagáláshoz.

Az Ipar 5.0 – az ipar 4.0 eszközparkjának kihasználásával – az ember és a gép együttműködésére helyezi a hangsúlyt. Szakképzett munkavállalók robotokkal munkamegosztásban egyedi termékeket hoznak létre és szolgáltatásokat végeznek. A fogyasztói igények egyre inkább az egyedi, vevőre szabott termékek irányába mozdulnak el, és ehhez szükséges az emberek és robotok kreatív együttműködése (Oláh-Popp-Erdei 2019). Az Ipar 5.0 nem jelenti a régi technológiák automatikus, azonnali leváltását. A korábbi berendezések, gyártó rendszerek is hálózatba integrálhatók szenzorok alkalmazása mellett. A robotok a termelési rendszerekben fontos szerepet kapnak, mivel intelligens rendszerek révén képesek hibákat azonosítani és kezelni. Az Ipar 4.0 és 5.0 elemeinek alkalmazása elvileg mindenképpen javítja a termelékenységet, a rugalmasságot és a minőséget, valamint a vevőkiszolgálás sebességét is. A gyártási folyamatok a termék tervezésétől és technologizálásától kezdve a gyártás automatizálásán át a beszállító és kooperációs partnerek bevonásán keresztül egészen az értékesítés lezárásáig egy letesztelt virtuális folyamat keretein belül történik meg. Mesterséges intelligencia révén a tanulásra és optimalizálásra képes komponensek akár „maguktól” is továbbfejlesztik a gyártási folyamatokat. A rendelkezésre álló erőforrások és az ismert piaci mozgástér alapján alakítják ki a legyártandó termékportfóliót és határozzák meg az egyes termékek gyártási mennyiségét.

Az Ipar 4.0 és 5.0 talán legnagyobb kockázatát a tágabb értelemben vett információbiztonsági események jelentik komplex, heterogén elemekből álló gyártó rendszerek esetében (Kovács 2017b). A felügyelet rövid ideig tartó elvesztése is kritikus mennyiségű javítható (a technológiai idő növekszik, speciális javítási feladatok jelentkeznek) és nem javítható selejtet eredményezhet.

## Következtetések

Az elmúlt évtizedekben folyamatosan fejlődő folyamatmenedzsment sem csodaszer válsághelyzetekben. A menedzsment módszerek, szabványok alkalmazása és az üzleti és technológiai trendek felismerése sem garantálja, hogy a helyettesítő erőforrások megfelelő helyen és időben elégségesek lesznek és a nyereséges működés fenn tartható marad.

A kontrollált erőforrás-allokációt végző és üzletmenet-folytonosságot szem előtt tartó, folyamatcentrikus vállalatok nagyobb eséllyel élik túl a válságos időszakokat. Beépített folyamat-ellenőrző rendszereik gyorsabb reakciókat hoznak a kedvezőtlen változásokra. Az irányítási rendszerek és az Ipar 4.0-ból következő technológiai váltás összehangolása ma már nem megkerülhető lépés. További kutatási irány lehet a termelő és logisztikai rendszerek régi és új komponenseinek Ipar 4.0 és 5.0 szerinti integrálása, illetve az ezeket bemutató jó gyakorlatok elemzése és bemutatása.

## Irodalomjegyzék

- van der Aalst, W. M. P., La Rosa, M. & Santoro, F. M., (2016) Business Process Management - Don't Forget to Improve the Process! Business & Information Systems Engineering, Vol. 58. No. 1. pp. 1–6. <https://doi.org/10.1007/s12599-015-0409-x>
- Ányos É. (2017a) Amit a folyamatok modellezéséről tudni érdemes. Magyar Minőség, Vol. XXVI. No. 2. pp. 4–12.
- Ányos É. (2017b) Amit a folyamatok modellezéséről tudni érdemes II. Magyar Minőség, Vol. XXVI. No. 3. pp. 5–15.
- Bennett, N., & Lemoine, G. J. (2014) What a difference a word makes: Understanding threats to performance in a VUCA world. Business Horizons, Vol. 57. Issue 3. pp. 311–317, <https://doi.org/10.1016/j.bushor.2014.01.001>
- Chikán A., & Demeter K. (szerk.) (2001) Az értékteremtő folyamatok menedzsmentje (Termelés, szolgáltatás, logisztika). Budapest: Aula Kiadó
- Christopher, M., & Peck, H. (2004) Building the resilient supply chain. International Journal of Logistics Management, Vol. 15. No. 2. pp. 1–13.
- Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodríguez-López, J. E. (2021) Sustainability and Resilience Organizational Capabilities to Enhance Business Continuity Management: A Literature Review. Sustainability, Vol. 13. No. 15. 8196. <https://doi.org/10.3390/su13158196>
- Çiçeklioğlu, H. (2020) VUCA Concept and Leadership. In: Mert, G. (ed.) Management & Strategy. Artikel Akademi, Chapter 13, pp. 229–244.
- Erazo-Chamorro, V. C., Arciniega-Rocha, R. P., Nagy, R., Babos, T., & Szabó, Gy. (2022) Safety Workplace: The Prevention of Industrial Security Risk Factors. Applied Sciences, Vol. 12. No. 21. 10726. <https://doi.org/10.3390/app122110726>
- Godányi G. (2004) Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában (A DR/BC tervezés alapjai). Híradástechnika, Vol. LIX No. 4. pp. 47–52.
- Hammer, M., & Champy, J. (1993) Reengineering the Corporation: A Manifesto for Business Revolution. New York: Harper Business
- Hollmann, R. L., Scavarda, L. F., & Thomé, A. M. T. (2015) Collaborative planning, forecasting and replenishment: a literature review. International Journal of Productivity and Performance Management, Vol. 64. No. 7. pp. 971–993.
- Iványos J. (2014) Kockázatkezelési Kézikönyv (Irányítási forgatókönyvek alkalmazása az integrált vállalati kockázatkezelés megvalósítására). v. 2.1, Trusted Business Partners Kft.
- Kilpatrick, J. (2003) Lean Principles. Utah Manufacturing Extension Partnership, Vol. 68. No. 1. pp. 1–5.
- Kovács O. (2017a) Az ipar 4.0 komplexitása – I. Közgazdasági Szemle, Vol. 64. No. 7–8. pp. 823–854. <https://doi.org/10.18414/KSZ.2017.7-8.823>
- Kovács O. (2017b) Az ipar 4.0 komplexitása – II. Közgazdasági Szemle, Vol. 64. No. 9. pp. 970–987. <https://doi.org/10.18414/KSZ.2017.9.970>
- Labodová, A (2004) Implementing integrated management systems using a risk analysis based approach. Journal of Cleaner Production, Vol. 12. Issue 6. pp 571–580. <https://doi.org/10.1016/j.jclepro.2003.08.008>
- Malina, M. A., & Selto, F. H. (2001) Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard. <https://ssrn.com/abstract=278939>, <http://dx.doi.org/10.2139/ssrn.278939>
- Michelberger, P. (2014) Risk Management for Business Trust. In: Michelberger, Pál (ed.) MEB 2014 Management, Enterprise and Benchmarking in the 21st Century. Budapest: Óbuda University, pp. 401–413.
- O'Neill, P., & Sohal, A. S. (1999) Business Process Reengineering – A review of recent literature. Technovation, Vol. 19. Issue 9. pp. 571–581. [https://doi.org/10.1016/S0166-4972\(99\)00059-0](https://doi.org/10.1016/S0166-4972(99)00059-0)
- Oláh J., Popp J., & Erdei E. (2019) Az Ipar 5.0 megjelenése: ember és robot együttműködése. Logisztikai trendek és legjobb gyakorlatok, Vol. V. No. 1. pp. 12–19.
- Packowski, J. (2014) LEAN Supply Chain Planning. The New Supply Management Paradigm for Process Industries to Master Today's VUCA World. CRC Press
- Pató Gáborné Szűcs B., Kovács K., & Abonyi J. (2021) A Negyedik Ipari Forradalom hatása a kompetenciacserélődésre. Vezetéstudomány / Budapest Management Review, Vol. 52. No. 1. pp. 56–70. <https://doi.org/10.14267/VEZTUD.2021.1.05>
- Porter, M. E. (1985) Competitive Advantage: Creating and Sustaining Superior Performance. New York: Free Press
- Rob, D. (2008) Aris Design Platform (Advanced Process Modelling and Administration). Springer London Ltd.
- Starr, M. K. (1976) Rendszerszemléletű termelésvezetés, termelés-szervezés. Budapest: Közgazdasági és Jogi Könyvkiadó
- Tenner, A. R., & DeToro, I. J. (1997) Process Redesign: The Implementation Guide for Managers. Addison-Wesley
- Wallace, T. F., Kremzar, M. H. (2001) ERP – Making It Happen; The Implementers' Guide to Success with Enterprise Resource Planning. John Wiley & Sons
- The ISO Survey of Management System Standard Certifications (2021) <https://www.iso.org/the-iso-survey.html> (letöltés dátuma: 2023. 01. 27.)
- APICS: Supply Chain Operations Reference Model (SCOR) Version 12.0 (2017)
- CPFR Model: Collaborative Planning, Forecasting and Replenishment (CPFR) Overview, (2004) Voluntary Interindustry Commerce standards (VICS)
- ISO 9001:2015 Quality management systems – Requirements (MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények)
- ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes (MSZ EN ISO 13485:2016 Orvostechnikai eszközök. Minőségirányítási rendszerek. Szabályozási célú követelmények)
- ISO 14001:2015 Environmental management systems – Requirements with guidance for use (MSZ EN ISO 14001:2015 Környezetközpontú irányítási rendszerek. Követelmények alkalmazási útmutatóval)
- ISO 20121:2012 Event sustainability management systems – Requirements with guidance for use
- ISO 22000:2018 Food safety management systems – Requirements for any organization in the food chain (MSZ EN ISO 22000:2018 Élelmiszer-biztonsági irányítási rendszerek. Az élelmiszerláncban részt vevő szervezetekre vonatkozó követelmények)
- ISO 22301:2019 Security and resilience - Business continuity management systems – Requirements (MSZ EN ISO 22301:2020 Társadalmi biztonság. Üzletmenet-folytonossági irányítási rendszerek. Követelmények) (angol nyelvű)
- ISO 22313:2020 Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301
- ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes
- ISO 28000:2022 Security and resilience – Security management systems – Requirements
- ISO 28001:2007 Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
- ISO 29001:2020 Petroleum, petrochemical and natural gas industries – Sector-specific quality management systems – Requirements for product and service supply organizations (MSZ EN ISO 29001:2020 Kőolaj-, petrokémiai és földgázipar. Ágazatspecifikus minőségirányítási rendszerek. Terméket előállító és szolgáltatást nyújtó szervezetek követelményei)
- ISO 31000:2018 Risk management – Guidelines (MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek)



- ISO 37001:2016 Anti-bribery management systems – Requirements with guidance for use (MSZ ISO 37001:2019 Antikorrupciós irányítási rendszerek. Követelmények alkalmazási útmutatóval)
- ISO 39001:2012 Road traffic safety (RTS) management systems – Requirements with guidance for use
- ISO 44001:2017 Collaborative business relationship management systems – Requirements and framework
- ISO 45001:2018 Occupational health and safety management systems – Requirements with guidance for use (MSZ ISO 45001:2018 A munkahelyi egészségvédelem és biztonság irányítási rendszere. Követelmények alkalmazási útmutatóval)
- ISO 50001:2018 Energy management systems – Requirements with guidance for use (MSZ EN ISO 50001:2019 Energiagazdálkodási irányítási rendszerek. Követelmények alkalmazási útmutatóval)
- ISO 55001:2014 Asset management – Management systems – Requirements (MSZ ISO 55001:2015 Vagyongazdálkodás. Irányítási rendszerek. Követelmények)
- ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements (MSZ ISO/IEC 20000-1:2019 Informatika. Szolgáltatásmenedzsment. 1. rész: A szolgáltatásirányítási rendszer követelményei)
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (MSZ ISO/IEC 27001:2014 Informatika. Biztonságtchnika. Információbiztonság-irányítási rendszerek. Követelmények)
- ISO/IEC 33001:2015 Information technology – Process assessment – Concepts and terminology
- ISO/IEC 33002:2015 Information technology – Process assessment – Requirements for performing process assessment
- ISO/IEC 33003:2015 Information technology – Process assessment – Requirements for process measurement frameworks
- ISO/IEC 33004:2015 Information technology – Process assessment – Requirements for process reference, process assessment and maturity models
- ISO/TS 22318:2021 Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management
- MIL-STD-882E Department of Defence Standard Practice – System Safety, 2012

A cikk a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>) feltételei szerint publikált Open Access közlemény, melynek szellemében a cikk bármilyen médiumban szabadon felhasználható, megosztható és újraközölhető, feltéve, hogy az eredeti szerző és a közlés helye, illetve a CC License linkje és az esetlegesen végrehajtott módosítások feltüntetésre kerülnek. (SID\_1)