Automação de Processos Industriais: do Pneumático à Indústria 4.0

Andréa P. Parente, Andrea Valdman, Rossana O. M. Folly, Maurício B. Souza Jr. & Isabella C. S. Nascimento

Este trabalho apresenta uma revisão da literatura acerca dos níveis de automação da indústria de processos dos anos 1940 até os dias de hoje. Sua motivação é destacar o papel da automação de processos para fins de confiabilidade, segurança e eficiência das operações por meio de uma perspectiva histórica. Ele também contempla a definição das novas tecnologias digitais que operam sob a Indústria 4.0. Essas novas tecnologias incluem, sensores sem fio, análises do tipo Big Data, computação em nuvem, e internet das coisas. Aqui estão incluídos o estado da arte das tecnologias de automação vigentes e suas projeções de mercado.

Palavras-chave: automação; instrumentação; estado da arte.

This paper presents a literature review of the evolution of the levels of automation in process industry from the 1940s up until now. The motivation of this study is to evidence the role of process automation for reliability, safety and efficiency of operations from a historical perspective. It also includes technologies definitions that operate under Industry 4.0. Such new technologies include wireless sensors, Big Data analysis, cloud computation, and the internet of things. Here, the state of the art of the current automation technologies and its market projections are exposed.

Keywords: *automation; instrumentation; state of the art.*

Jul / Dez de 2018 Revista Processos Químicos 101

Introdução

O sistema de automação é crítico para a operação das plantas de processo. Nos dias de hoje, ele executa funções de controle e outras funções avançadas que incluem, mas não se limitam, a otimização, o agendamento e o planejamento das operações industriais. A automação dos processos garante a medição de parâmetros apropriados, a análise das situações operacionais, a exploração de oportunidades mais lucrativas, o cálculo e a tomada de ações de controle. Além disso, os sistemas de automação mantêm o pessoal da planta informado permitindo que seus conhecimentos e habilidades sejam explorados, que as situações anormais sejam identificadas e abordadas e que os processos e os negócios sejam integrados ¹.

Portanto, a confiabilidade, a segurança e a eficiência do processo produtivo como um todo depende do correto funcionamento de todos os elementos do sistema de automação industrial e, em particular, de todos os componentes das malhas de controle.

PERSPECTIVA HISTÓRICA: DO SÉCULO XX AOS DIAS DE HOJE

Entre os fatores determinantes para a evolução natural do estado da arte da automação industrial destacam-se: a crescente demanda no desempenho do processo e na qualidade do produto, a definição de processos operacionais independentes do operador humano e a substituição de tarefas monótonas e repetitivas executadas pelo operador por tarefas mais especializadas ².

Além disso, uma análise do desenvolvimento histórico do setor de automação evidencia que desde o final do século XIX havia uma preocupação em diagnosticar falhas em grandes máquinas com a intenção de reduzir riscos humanos, sociais e ambientais. Nesse sentido, a solução adotada era baseada na possibilidade de interromper o processo ao ultrapassar limites operacionais ².

Até a década de 40, as plantas de processo eram atuadas manualmente por um grande número de operadores, com poucos instrumentos mecânicos elementares que realizavam controle local. A evolução natural da indústria com o desenvolvimento de equipamentos maiores e processos mais complexos impactou diretamente nas atividades de

comissionamento, operação e manutenção, demandando formas de controle mais precisas. Surgiram, então, os instrumentos pneumáticos, permitindo a transmissão de informações sobre as variáveis do processo através de tubulações específicas até certa distância. Assim, os controladores puderam ficar reunidos em uma mesma sala: a sala de controle do processo ².

A introdução da eletrônica analógica ocorreu durante as décadas de 50 e 60 e possibilitou a ampliação das distâncias entre os elementos de campo e a sala de controle, simplificando a transmissão de informações e contribuindo para a disseminação de sistemas de controle automático ².

Em 1970, surgiram os primeiros CLPs (controlador lógico-programável), criados para substituir sistemas automáticos que utilizavam relés, temporizadores e sequenciadores mecânicos ³. Esses equipamentos ganharam força a partir de 1980 e, ainda hoje, existe um grande número de processos industriais, principalmente, processos de fabricação de automóveis e de manufatura, baseados em informações discretas ³.

Em 1975, os primeiros SDCDs (Sistemas Digitais de Controle Distribuído) foram lançados, um sistema integrado no qual um nível supervisório de controle monitora múltiplos subsistemas integrados. Inicialmente, essa tecnologia foi lançada para substituir a tecnologia anterior, baseada em CLPs ⁴. No entanto, devido às limitações de cada uma das tecnologias citadas, em 1985 começaram a ser utilizados padrões de TI (tecnologia da informação), com a consequente integração de CLPs e SDCDs.

Entre os anos 70 e 80, surgiu a instrumentação eletrônica digital e com ela o grau de automação das instalações industriais foi ampliado. A partir dos anos 80, o computador digital se popularizou, agregando funções de troca de informação em rede, integrando muitas das funções que eram antes dispersas pelos vários elementos de um sistema de automação ^{5,6}. Os sistemas supervisórios tornaram-se uma ferramenta importante, ampliando suas funções de armazenamento de dados históricos. Nessa época, foram desenvolvidos os primeiros sistemas de Supervisão e Aquisição de Dados (SCADA - Supervisory Control and Data Acquisition)

incorporando uma interface homem-máquina (IHM) mais amigável com o usuário ³.

O surgimento da plataforma Windows da Microsoft® no final dos anos 80 e pressões do mercado, principalmente o boom da utilização de equipamentos de informática em todos os setores de desenvolvimento da automação industrial, conduziram os fabricantes a também adotar plataformas operacionais como parte inerente aos seus equipamentos ³. Os fabricantes de produtos de automação industrial rapidamente aderiram à era de comunicação em redes, propondo a padronização do barramento de campo. No final dos anos 90, surgem os equipamentos de instrumentação baseados em redes industriais, incorporando protocolos de comunicação em tecnologia digital. Destacam-se o padrão Fieldbus Foundation (FF), proposto pelos fabricantes dos Estados Unidos e o padrão Profibus (PF), proposto pelos fabricantes europeus ³.

O aumento da capacidade de processamento dos computadores e componentes microeletrônicos expandiu as

aplicações de sistemas de controle de processos automáticos, que passaram a incorporar também o conhecimento de especialistas sobre os processos por meio de técnicas de inteligência artificial. Esse salto tecnológico se reflete na miniaturização dos dispositivos e no aumento da sua sensibilidade e precisão além da diminuição do seu tempo de resposta ².

Nos dias de hoje, observa-se uma tendência à padronização de elementos e de protocolos de comunicação, reduzindo os custos associados à implantação dos sistemas de controle e aumentando a interoperabilidade entre diferentes fabricantes. Além disso, há uma convergência tecnológica com origens na utilização da tecnologia digital que resulta na interligação dos sistemas de monitoramento e controle de processos com os sistemas de gestão integrada das empresas e o acesso a informações e relatórios de controle pela internet e terminais portáteis². médicos e automação doméstica, para citar alguns.

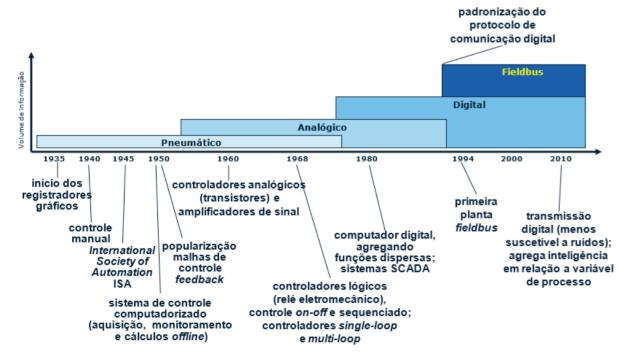


Figura 1. Evolução tecnológica da automação industrial.

Jul / Dez de 2018 Revista Processos Químicos 103

A instrumentação atual oferecida pelo mercado de automação para atender às demandas específicas de processos industriais contínuos utiliza, principalmente, a tecnologia de redes industriais³. Os novos parques industriais químicos e petroquímicos já exigem essa tecnologia como sendo padrão para seus projetos de instrumentação e, tendo em vista o salto na quantidade de informação e de inteligência em relação às tecnologias anteriores, as indústrias que foram instaladas sem esse padrão estão gradativamente migrando e adaptando a instrumentação de suas plantas, dando origem às plantas de instrumentação híbrida. A Figura 2 resume a evolução tecnológica da automação industrial do século XX ao século XXI.

PERSPECTIVA FUTURA: PROJEÇÕES E TENDÊNCIAS

Uma tendência tecnológica sugerida pela Honeywell® ¹ é a de que em um futuro não muito distante um novo dispositivo possa ser fisicamente ligado à uma rede e ser automaticamente descoberto pelo sistema e autoconfigurado, com mínima supervisão humana.

Um estudo setorial acerca da automação de processos industriais relatado pelo BNDES² sugere que novas tecnologias vêm sendo alvo de investimentos, como, por exemplo, a comunicação sem fio (*wireless*) e a adoção de instrumentos baseados em ultrassom, expandindo ainda mais a área de atuação do controle, indo além dos processos industriais e das plantas de infraestrutura para abranger também sistemas prediais e de logística, procedimentos médicos e automação doméstica, para citar alguns.

A tecnologia wireless é agora amplamente vista como um agente de mudança em automação industrial, especialmente valioso para atualizações em plantas já existentes em que o custo para adicionar fiação é proibitivo ¹. Computadores em plantas agora estão conectados à internet e em algumas aplicações via wireless. Os dispositivos conectados à rede agora também apresentam servidores web incorporados. Através de qualquer conexão com a internet, os dispositivos de campo podem servir páginas da web com valores de variáveis de processo, parâmetros e telas de configuração de maneira que tais dispositivos podem ser configurados e

monitorados por um navegador em qualquer lugar por meio de uma conexão segura.

Outra tendência emergente se reflete em uma mudança estrutural da arquitetura de automação. Muitas funcionalidades são entregues por meio de softwares na forma de aplicações do tipo *stand-alone*: monitoramento, estimações, controle, otimização, visualização de tendências, pontes de integração com outras bases de dados, para citar algumas. Há um surgimento, entretanto, de arquiteturas orientadas para serviço. Nesta nova abordagem, as funcionalidades ficam localizadas em um servidor remoto e são acessadas via internet ¹.

Nesse contexto, *cybersegurança* é um tópico in voga. Embora não se tenha notícia de acidentes graves causados por invasão cibernética à rede de automação, há reportes de ocorrência de brincadeiras localizadas ⁷⁻¹⁶.

TECNOLOGIA DIGITAL E REDES INDUSTRIAIS

Apesar de sua ampla aceitação e aplicação nas indústrias de processos os transmissores de sinal 4-20 mA ou analógicos já não satisfazem os requisitos necessários aos modernos sistemas de automação. O sinal analógico é apenas um carreador de informação em um fluxo unidirecional do sensor para o sistema de automação ou para o atuador.

A tecnologia de transmissão em redes digitais viabiliza um meio de interconexão de dispositivos de campo a custos baixos ao substituir a conexão ponto a ponto pela conexão multiponto. Assim, os instrumentos para controle se comunicam por meio de protocolos digitais puros, tornando possível a transmissão de informações processadas auxiliares. Ao contrário da transmissão analógica, em que a informação é transmitida através da modulação de uma corrente elétrica, a informação passa a ser transmitida através de uma sequência de pulsos elétricos de mesma largura, representando dígitos binários de 0 ou 1 ⁷. Este formato oferece informações mais robustas e de maior qualidade de sinal uma vez que a amplitude da onda elétrica responsável pelo ruído é muito menor do que a amplitude da onda elétrica responsável pelo pulso contendo a informação de interesse 8,17-30.

Segundo Fieldbus⁷ é o termo genérico utilizado para designar os protocolos de alta velocidade, baseado em redes de transmissão digital, que suportam a comunicação bidirecional de informação entre um determinado número de equipamentos inteligentes em uma rede local. Atualmente, as redes industriais mais amplamente disponíveis podem ser classificadas em três categorias principais: fieldbus tradicionais, redes baseadas em Ethernet e redes sem fio ⁷.

Uma comparação das principais propriedades das redes atualmente mais amplamente disponíveis no mercado em cada uma das três categorias principais é dada na Tabela 1.

Um levantamento das tendências no mercado de automação industrial realizado pela Intech e divulgado pelo BNDES ² revela que os protocolos Profibus e Foundation Fieldbus são os mais abrangentes e que 80% das empresas entrevistadas usam instrumentos que utilizam protocolos de comunicação baseados em redes industriais afirmando uma tendência de mercado consolidada.

De um ponto de vista de arquitetura, a tecnologia Fieldbus tornou o sistema de controle ainda mais distribuído ao incorporar dispositivos cada vez mais sofisticados em que os transmissores podem ter algoritmos de compressão e escalonamento internos e os atuadores podem incluir processadores nos quais os cálculos de controle podem ser executados ¹.

Além disso, os equipamentos de campo com comunicação microprocessada são capazes de indicar falha em tempo real e disponibilizar diagnóstico preventivo baseado em dados de operação do equipamento e avaliação estatística desses. As capacidades de autovalidação, inerentes aos próprios equipamentos, tornam esta tecnologia de instrumentação atraente para ser usada em associação a ferramentas de detecção e diagnóstico de falhas e de controle tolerante a falha em um framework para gerenciamento de situações anormais.

NOVAS TECNOLOGIAS DIGITAIS

As três primeiras revoluções industriais resultaram em mudanças radicais nos processos de produção, introduzindo mecanização, eletricidade e tecnologia de informação. Desde as máquinas a vapor até a produção automatizada elétrica e digital, estas mudanças levaram ao aumento

da eficiência e da produtividade. Não obstante, o atual paradigma do modo de produção em que vivemos está se tornando insustentável ⁸.

O impacto da produção industrial sobre o meio ambiente em termos de aquecimento global e poluição ambiental é grave. O consumo de recursos não-renováveis, como petróleo e carvão, aumenta. A indústria sofre de uma oferta cada vez menor de força de trabalho em razão do envelhecimento da população ⁹. Nesse contexto, é indispensável que os processos industriais alcancem alta flexibilidade e eficiência associados ao baixo consumo de energia e redução de custos.

Consequentemente, uma iniciativa estratégica denominada "Industrie 4.0" (Indústria 4.0) foi proposta e adotada pelo governo alemão como parte do *High-Tech Strategy 2020 Action Plan*¹⁰. Estratégias similares também foram propostas por outros países industrializados, por exemplo, "Internet Industrial" pelos Estados Unidos e "Internet +" pela China ⁹.

Uma série de publicações se preocupa em conceituar os requerimentos que caracterizam a indústria 4.0, como (24) e (25), mas ainda não há um consenso padrão entre os autores.

Sob a Indústria 4.0, o processo de produção consistirá em troca de informações, máquinas controladas e unidades de operação atuando de forma autônoma e inteligente (11).

Segundo o plano de ações proposto pelo governo alemão, a fábrica inteligente é a característica mais importante da Indústria 4.0. Nela, os itens relevantes para a indústria, como materiais, sensores, máquinas, produtos, cadeia de suprimentos e clientes, podem ser conectados. Isso significa que estes objetos vão trocar informações e ações de controle uns com os outros de forma independente e emancipada ¹¹. Uma tendência atual é a preocupação em estabelecer uma abordagem organizacional para a arquitetura das Fábricas Inteligentes através de metodologias ⁹ e frameworks ¹¹.

Do ponto de vista do engenheiro de controle, a fábrica inteligente pode ser vista como um sistema de malha fechada dupla, como mostrado na Figura 3. Um laço consiste em recursos físicos e nuvem, enquanto o outro laço consiste em terminais de controle de supervisão e nuvem ⁹.

Tabela 1. Rede Digitais Disponíveis no Mercado e Propriedades.

Тіро	Rede Digital	Fabricante	Velocidade de Transmissão	Número de Equipamentos	Aplicações
Field bus Tradicional	CAN	Bosch	10 kb/s–1 Mb/s, 31,25 kb/s, 1Mb/s, 2,5 Mb/s (5Mb/s fibra óptica)	Máx 32	Controle Automotivo e Industrial, Sistemas Embutidos
	WorldFIP(1158-2)	Schneider		Máx 256 (64/s)	Manufatura, Distribuído em Tempo Real
	Profibus - DP	Siemens	9,6kb/s-12Mb/s	Máx 126	Automação de Manufatura, Ambiente Genérico
	Profibus - PA	Siemens	31,25kb/s	Más 32/s	Controle de Processo, Ambiente Perigoso
		Rock well Auto	5Mb/s	Máx 99	Manufatura
	Control Net Interbus	Phoenix contact	500kb/s	Máx 512	Manufatura, IO remoto, Tecnologia de Manufatura
	Asi	Siemens	167kb/s	Máx 62	Barramento de Sensor
	Foundation Fieldbus HI	Fieldbus Foundation	31,25kb/s	Máx 32	Processo
Ethernet	Ethernet/IP	Rockwell Auto	10, 100 Mb/s, 1Gb/s	-	Manufatura, Tecnologia de Sistemas de Manufatura
	Foundation Fieldbus HSE	Fieldbus Foundation	100 Mb/s	-	Manufatura
	Ether CAT	Beckhoof	100 Mb/s	Até 65.535 devices	IO Descentralizado, Controle de Movimento
	Powerlink	B&R	100 Mb/s	=	Controle de Movimento
	Profinet	Siemens	100 Mb/s	-	Manufatura, Objetos de Automação Distribuídos, Comunicação entre Sistemas, Tecnologia de Manufatura
	Sercos III	Bosch Rexroth	100 Mb/s	Máx 254	Controle de Movimento Rápido
	ModbusTCP	Schneider	10, 100 Mb/s, 1Gb/s	-	Comunicação etre Sistemas
Wireless	IEEE 802.11(a/b/g)	-	11 Mb/s, 54 Mb/s	-	SOHO
	Bluetooth, EEE 802.15.1	-	1 Mb/s	Até 7 escravos/piconet	WPAN, Tecnologia de Substituição de Cabos
	IEEE 802.15.4/ZigBee	-	20, 40, 250 kb/s	Suporte redes grandes	WPAN, Para Sensores e Dispositivos de Controle, Rede de Sensores Sem Fio
	Ethernet (IEEE 802.3	=	10, 100 Mb/s, 1 Gb/s	Quase illimitado	_

Fonte: Jämsa-Jounela, 2007 - modificada.

Esse sistema será possível com o auxílio de tecnologias de ponta emergentes na última década orientadas para os sistemas Cyber-Físicos (CPS) como os sensores sem fio, a computação em nuvem, a análise de Big Data ¹², a internet móvel e, sobretudo, a Internet das Coisas (IoT) ⁹.

A Internet das Coisas (IoT) derruba as barreiras entre o mundo real e o mundo virtual ao transformar todos os objetos físicos em objetos inteligentes ¹³. Os autores de ¹⁶ apresentam a evolução da Internet das Coisas desde suas ideias raízes até a geração tecnológica atual. Mas, em uma

abordagem mais ampla que perpassa pelos objetos do diaa-dia, nossas roupas, móveis, carros, luzes de casa ou até mesmo potes de café terão sua própria conta nas mídias sociais, interagirão com outras redes, enviarão dados para a nuvem e permitirão a agregação de dados de diferentes fontes e aspectos da nossa vida. Os medidores inteligentes deduzirão quando tomamos banho, os carros saberão quando não estamos indo para o trabalho, os dispositivos médicos saberão nosso peso, e os celulares saberão como estamos nos sentindo ¹³. Se esta realidade soa desconfortável do

ponto de vista de privacidade e segurança para as pessoas, quando se trata da segurança dos processos industriais o controle de acesso é condição sine qua non e vem sendo estudado nas pesquisas recentemente divulgadas acerca de cybersegurança. (16) e (15) são alguns exemplos.

A empresa especializada em segurança cibernética Symantec estima que as perdas financeiras das empresas, que incluem reparos e tempo de recuperação, causadas pelos crimes virtuais chegam a US\$385 bilhões anuais ¹⁴. A invasão dos sistemas com intenções nocivas de violação de dados é tipicamente carreada pkor meio de malware, que é, por definição, qualquer código computacional capaz de causar danos ao sistema ¹⁵. As vítimas de malware não se limitam aos usuários finais, mas incluem servidores, equipamentos em redes digitais e sistemas SCADA ¹⁵. As ameaças atuais incluem, além do roubo de dados econômicos e de propriedade intelectual ¹⁶, sequestro do sistema inteiro or meio de uma modalidade denominada ransomware, em que o acesso é completamente bloqueado e devolvido mediante pagamento de resgate ¹⁷.

De acordo com a empresa CISCO, especializada em tecnologia da informação, em 2020 haverá 50 bilhões de dispositivos conectados ¹⁸. Isso explica a insurgência de uma série de trabalhos dedicados a discutir as vulnerabilidades dos sistemas modernos, como em ¹⁷. Em ²¹ a segurança dos sistemas de controle em redes foi abordada por meio da teoria de jogos, em que cada equipamento inteligente é considerado um jogador. Já em ²² uma pesquisa sobre invasores que afetam a disponibilidade, confiabilidade e integridade dos recursos e serviços em nuvem foi relatada e técnicas de identificação e prevenção contra estas ameaças foram discutidas.

Muitos outros estudos recentes focam na resiliência industrial dos sistemas de infraestrutura crítica, como as plantas de energia e os sistemas de distribuição da rede elétrica, diante de ataques cibernéticos. Referências (21), (22) e (23) são alguns exemplos. Um obstáculo para a evolução das ferramentas de segurança cibernética para processos industriais reside no fato de que testar as soluções de segurança em fábricas reais é quase impossível; porque isto significa desacelerar ou mesmo desligar operações.

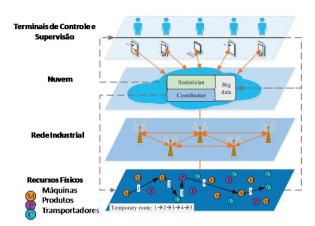


Figura 3. Representação esquemática de uma fábrica inteligente da indústria 4.0.

Conclusão

Este trabalho mostrou uma revisão da literatura sobre o grau de automação da indústria de processos e as características dos sistemas de automação dos anos 1940 até os dias de hoje. Por meio de uma perspectiva histórica, destacou-se o papel da automação de processos para fins de confiabilidade, segurança e eficiência das operações.

Abordou-se, também, o estado da arte das tecnologias de automação vigentes expondo tendências de mercado e pesquisas in voga. Em particular, as novas tecnologias digitais apresentam características de processamento e transmissão de informação superiores às tecnologias pneumáticas e analógicas e parecem se consolidar cada vez mais no parque industrial. A princípio, com o espalhamento das indústrias híbridas e, no futuro próximo, com sistemas de automação completamente digitais. As novas tecnologias digitais como sensores sem fio, análises do tipo Big Data, computação em nuvem, e internet das coisas encontram suporte nas Fábricas Inteligentes, oriundas da revolução 4.0 cuja finalidade estratégica é levar a processos produtivos cada vez mais otimizados e sustentáveis.

Referências

 Samad, T.; Mclaughlin, P.; LU, J. System architecture for process automation: Review and trends. Journal of Process Control, v. 17, p. 191-201, 2007.

Jul / Dez de 2018 Revista Processos Químicos 107

Artigo Geral 9

- Isermann, R. Fault Diagnosis Systems: an introduction from fault detection to fault tolerance. [S.l.]: Springer-Verlag Berlin Heidelberg, 2006. 8-10 p.
- Gutierrez, R. M. V.; PAN, S. S. K. Complexo Eletrônico: Automação do Controle. BNDES Setorial, Rio de Janeiro, v. 28, p. 189-232, Setembro 2008
- Valdman, A. Estrutura Unificada Baseada em Sensor Virtual e Tecnologia Fieldbus para Monitoramento, Diagnóstico e Controle de Caldeiras. Universidade Federal do Rio de Janeiro. Rio de Janeiro, p. 224. 2013.
- Abdi. Panorama setorial de eletrônica para automação. Agência Brasileira de Desenvolvimento Industrial - Centro de Gestão de Estudos Estratégicos. Brasília. 2009.
- Seborg, D. E.; Edgar, T. F.; Mellichamp, D. A. Process Dynamics and Control. 4ª Edição. ed. [S.l.]: John Wiley & Sons, Inc., 2016.
- 7. Byres, E. Can't happen at your site? In Tech Magazine, Fevereiro 2002.
- Morris, A. S. Measurement and Instrumentation Principles. 3^a. ed. Oxford: Butterworth-Heinemann, 2001.
- Geron, L. C. A Utilização de Fieldbus para Controle de Caldeiras. IBP. Rio de Janeiro. Outubro 1998.
- Jämsä-Jounela, S.-L. Future trends in process automation. Annual Reviews in Control, v. 31, p. 211-220, 2007.
- Alkaya, E. et al. Adaptationto climate change in industry: improving resource efficiency through sustainable production applications. Water Environment Research, v. 87, p. 14-25, 2015.
- Wang, S. et al. Towards smart factory for industry 4.0: a selforganized multi-agent system with big data based feedback and coordination. ComputerNetworks, v. 10, p. 158-168, 2016.
- "Recommendations for implementing the strategic initiative INDUSTRIE 4.0", 2013. Disponivel em: <a href="http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report_Industrie_4.0/Enal_report_Acesso em: 28 Janeiro 2017.
- Qin, J.; Liu, Y.; Grosvenor, R. A Categorical Framework of Manufacturing for Industry 4.0 and Beyond. Changeable, Agile, Reconfigurable & Virtual Production, v. 52, p. 173-178, 2016.
- Flouris, I. et al. Issues in complexeventprocessing: Statusandprospe ctsin the Big Dataera. The Journal of Systems and Software, p. 1-20, 2016.
- Ouaddah, A. et al. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, v. 112, p. 237-262, 2017.
- Atzori, L.; Iera, A.; Morabito, G. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, v. 56, 2017.
- LI, F.; HAN, Y.; JIN, C. Practical access control for sensor networks in the context of the Internet of Things. Computer Communications, v. 89-90, p. 154-164, 2016.
- Symantec. Internet Security Threats Report. Symantec. Disponivel em: http://www.symantec.com/threatreport/. Acesso em: 02 Março 2017.
- Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, v. 80, p. 973 – 993, 2014.

- 21. Parent, M.; Cusack, B. Cybersecurity in 2016: People, technology, and processes. Business Horizon, v. 59, p. 567 569, 2016.
- Mansfield-Devine, S. Ransomware: taking businesses hostage. Network Security, v. 10, p. 8-17, 2016.
- 23. Evans, D. How the Next Evolution of the Internet Is Changing Everything. CISCO White Paper, 2011. Disponivel em: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/loT_IBSG_0411FINAL.pdf Acesso em: 02 marco 2017.
- Amin, S.; Schwartz, G. A.; Sastry, S. S. Security of interdependent and identical networked control systems. Automatica, v. 49, p. 186-192. 2013.
- Modi, C. et al. A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, v. 36, p. 42–57, 2013
- Yusta, J. M.; Correa, G. J.; Lacal-Arántegui, O. Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy, v. 39, p. 6100-6119, 2011.
- Bekara, C. Security Issues and Challenges for the IoT-based Smart Grid. Procedia Computer Science: International Workshop on Communicating Objects and Machine to Machine for Mission Critical Applications (COMMCA-2104). [S.I.]: [s.n.]. 2014. p. 532-537.
- Langer, L. et al. From old to new: Assessing cybersecurity risks for an evolving smart grid. Conputers abd Security, v. 62, p. 165-176, 2016
- Oesterreich, T. D.; Teuteberg, F. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. Computers in Industry, v. 83, p. 121-139, 2016.
- Stock, T.; Seliger, G. Opportunities of Sustainable Manufacturing in Industry 4.0. 13th Global Conference on Sustainable Manufacturing - Decoupling Growth from Resource Use. [S.l.]: [s.n.]. 2016. p. 536 - 541

Andréa P. Parente^{1*}, Andrea Valdman², Rossana O. M. Folly², Maurício B. Souza Jr.² & Isabella C. S. Nascimento²

¹Sc., Centro de Tecnologia da Indústria Química e Têxtil, Curso de Engenharia Química

²Universidade Federal do Rio de Janeiro, Escola de Química, Departamento de Engenharia Química.

*E-mail: aparente@cetiqt.senai.br