www.dergipark.gov.tr
ISSN:2148-3736
El-Cezerî Fen ve Mühendislik Dergisi
Cilt: 7, No: 1, 2020 (149-159)

El-Cezerî Journal of Science and Engineering
Vol: 7, No: 1, 2020 (149-159)

DOI: 10.31202/ecjse.599325

ECJSE

Research Paper / Makale

Cyber Security in Material Manufacturing

Tuba YENER[1], Şuayb Çağrı YENER[2*], Reşat MUTLU[3]

[a]Department of Materials and Metallurgy Engineering Sakarya University, Sakarya, Turkey
[b]Department of Electrical and Electronics Engineering, Sakarya University, Sakarya, Turkey,
[c]Department of Electronics and Telecommunication Engineering Namık Kemal University Çorlu, Tekirdağ, Turkey
syener@sakarya.edu.tr

Received/Geliş: 31.07.2019 **Accepted/Kabul:** 10.10.2019

Abstract: Industry 4.0, a new industry revolution, is happening now and several developed countries are leading the path. Internet of things (IoT) is also encompassed by Industry 4.0. In the future, more devices in factories are to be connected to Ethernet or Internet. However, this makes the companies, devices and researchers vulnerable to cyber-attacks. Recently, some cyber-attacks which have happened to some companies or countries verify the danger. Sintering systems and furnaces are used for research by universities and for series manufacturing by factories. Arc furnaces and induction furnaces are also commonly used devices in metal factories. A sintering system, an arc furnace or an induction furnace which is connected to Internet or Ethernet may also be under cyber-attack threat. The danger may be prevented by taking necessary precautions. In this study, these three-production systems are first briefly introduced and then inspected assuming that they have been connected to internet and examined with considering cyber-attack point of view. Some basic solutions against cyber-attacks to the aforementioned devices are suggested.

Keywords: Cyber-attack prevention, manufacturing systems, Electric Current Activated Sintering, arc furnaces, induction furnaces, Internet of Things, Industry 4.0

Malzeme Üretiminde Siber Güvenlik

Öz: Yeni bir endüstri devrimi olan Endüstri 4.0 günümüzde yaşanmakta ve özellikle bazı gelişmiş ülkeler bu alanda öncü çalışmalar ortaya koymaktadır. Nesnelerin İnterneti (IoT) Endüstri 4.0 tarafından kapsanan önemli bir altyapıdır. Gelecekte, fabrikalardaki daha fazla cihazın Ethernet veya İnternet üzerinden çalışmalarını sürdürmesi öngörülmektedir. Bunun kurum ve fabrika ortamındaki cihazları ve verileri siber saldırılara karşı savunmasız bırakabileceği açıktır. Son zamanlarda, farklı ülkelerden farklı kurumlarda yapılan bazı siber saldırılar tehlikeyi doğrulamaktadır. Çeşitli malzeme sinterleme sistemleri ve fırınlar üniversiteler tarafından araştırma yapmak ve fabrikalar tarafından seri imalat yapmak için kullanılırlar. Ark fırınları ve endüksiyon fırınları da metal fabrikalarında yaygın olarak kullanılan cihazlardır. Internet veya ethernet'e bağlı bir sinterleme sistemi, bir ark ocağı veya bir indüksiyon ocağı da siber saldırı tehdidi altında olabilir. Bu noktada gerekli önlemler alınarak tehlike önlenebilir. Bu çalışmada, bu üç üretim sistemi ilk öncelikle kısaca tanıtılmış ve daha sonra internete bağlı oldukları dikkate alınarak siber saldırı bakış açıları ile incelenmişlerdir. Çalışmada, belirtilen cihazlara karşı olası siber saldırılara yönelik çözümler önerilmektedir.

Anahtar Kelimeler: Siber saldırı, üretim sistemleri, sinterleme sistemleri, ark fırınları, indüksiyon fırınları, Nesnelerin İnterneti, Endüstri 4.0

1. Introduction

The concept of Industry 4.0 encourages automation across many industries. It globally influences companies to develop new technologies which incorporate features such as artificial intelligence, autonomous robotics, and system integration. Even though it is an inherent part of the Industry 4.0

How to cite this article
Yener, T., Yener, Ç.Ş., Mutlu, R., "*Cyber Security in Material Manufacturing*" El-Cezerî Journal of Science and Engineering, 2020, 7(1); 149-159.

Bu makaleye atıf yapmak için
Yener, T., Yener, Ç.Ş., Mutlu, R., *"Malzeme Üretiminde Siber Güvenlik"* El-Cezerî Fen ve Mühendislik Dergisi 2020, 7(1); 124-134.

model, the complexity of cyber security has led to its being overlooked by many industrial sectors [1], [2]. Such analysis has already been made for textile engineering [3], [4]. This study aims to provide useful analysis of cyber security in material/metallurgical manufacturing environments and addresses the presence of threats and vulnerabilities in material/metallurgical manufacturing systems. It also focuses on these cyber threats in action and analyses how best to achieve successful cyber security in material/metallurgical manufacturing. Sintering systems, arc furnace and induction furnace systems are commonly used in metallurgical or material engineering and in factories [5], [6], [15]–[24], [7], [25]–[31], [8]–[14].

Resistive sintering systems using electric current as the source of the heat energy, provides a technique that allows sintering of composite, ceramics, metal, intermetallic materials at very low temperatures and very short production times. It has remarkable features compared to other conventional methods. In this technique, which is a way to obtain perfect combination of electric current and mechanical pressure, the material to be sintered may be dust or compacted. The primary purpose of the using electric current is to ensure the energy needed for resistance-based heating in the container [5], [7], [9], [32].

Electric arc furnaces (EAF) are systems used for heating materials with electric arc. Arc furnaces which are also high power metallurgical devices like resistive sintering systems are commonly used in industrial settings to heat and mold metal and their power system harmonics and power requirements have been examined in literature [10], [12], [13], [18]–[21], [23], [28]. Arc furnaces range in size from only a few dozen grams (used in research laboratories for some specific purposes) to about hundreds ton units (used for high volume industrial applications). They can typically be heated up to 1800 °C in industrial applications while their temperature can exceed 3000 °C for some special applications.

An Induction Furnace (ICF) is an electrical furnace in which the heat is applied by induction heating of metal to be melted. Induction furnace capacities range from less than one kilogram to one hundred tons, and are used to melt copper, aluminum, iron, steel, and precious metals [33]–[35]. The advantage of the induction furnace is being a clean, energy-efficient and well-controllable melting process compared to most other means of metal melting. Most of the modern foundries use this type of furnace, and nowadays more iron foundries are replacing cupolas with induction furnaces to melt cast iron, as the former vent out lots of dust and other pollutants [36]. Since no arc or no combustion are needed, the temperature of the material is no higher than required to melt it; this highly prevents loss of valuable alloying elements [37].

Internet of Things (IoT), which allows devices and systems to communicate with each other, is becoming increasingly important nowadays. A survey on Internet of Things (IoT) Technologies can be found in A survey on Internet of Things Technologies are found in [38]. Several IoT applications are available in the literature: Such as intelligent laboratory management systems based on IoT [39], [40]. a remote laboratory based on IoT for performing remote experiments [41], [42], IoT to turn a house into a remote-controlled laboratory [43], laboratory equipment managed using IoT [38]. IoT to build smart cities [44]. In the future, the factories are going to have more devices or manufacturing utilities connected to internet or ethernet. This makes them vulnerable to cyber-attacks. The attackers are classified in [2] as Nation-state, Terrorist Groups, Rival organizations, Cybercriminal, Hacker Hobbyists, Hacktivists, Insiders. In this study, electric current assisted sintering and Arc furnace systems which are connected to Internet of Things are to be examined considering cyber security. Considering their electrical circuits, it is shown how they can be attacked and how they can be protected.

The paper is arranged as follows. In the second section, the factory electrical system considered is given. In the third section, the material production systems are briefly explained. In the fourth

section, its vulnerabilities to cyber-attacks are inspected. In the fifth section, the possible cyber-attack protection methods are given/suggested. The paper is concluded with the last section.

2. Factory Electrical Circuit

The Residential Electric circuit given in Fig. 1 is considered in this study. Point of common coupling (PCC), neighbor factories, and other internal factory loads are shown in Fig. 1. Due to PCC, an electrical load can affect other loads with voltage swells, voltage lags, and electromagnetic interference (EMI). In the next sections, it is to be told how the high-power material production systems may affect other loads. Figures are only used to explain the electric current assisted sintering system since the other two are better-known by electrical engineers.

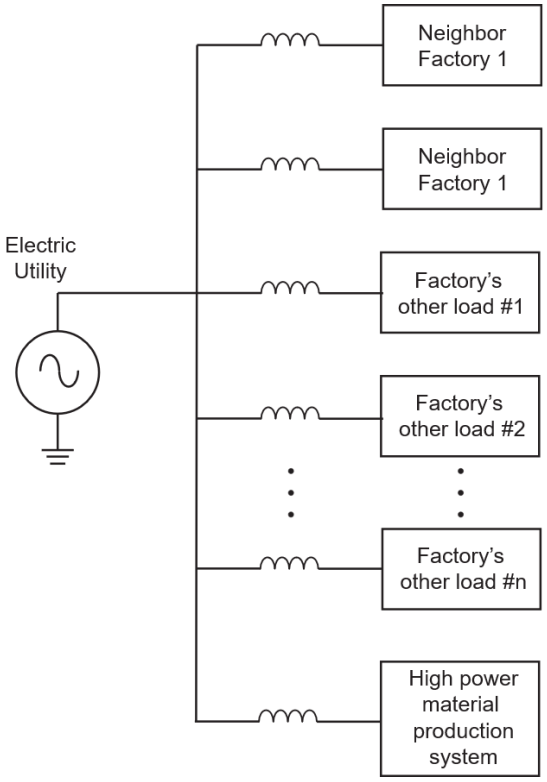

Figure. 1. Residential Electric Circuit

3. Material Manufacturing Systems

In this section, all three material production systems are to be briefly explained.

3.1 Pulse DC Sintering System

Pulse DC electric current assisted sintering system is a newer sintering system which has superior features compared to other traditional methods. Mechanical structure of such sintering system is illustrated in Fig. 1. Pulsed DC current is used in the system to provide the heat needed to produce the sample during the process. Electrical Schematic of the power unit is illustrated in Fig. 2.

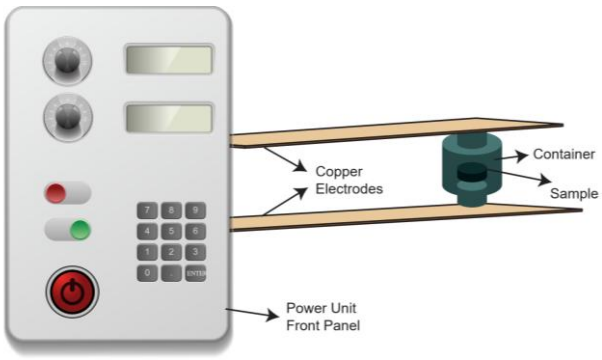

Figure 2. Principle mechanical structure representation of the pulse DC electric current assisted sintering system

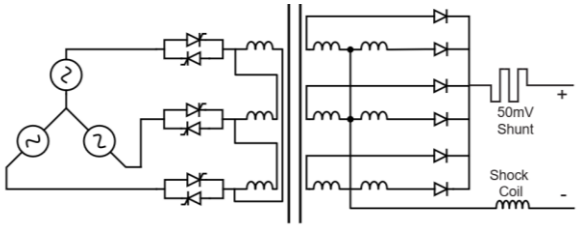

Figure 3. Detailed electronics circuit schematic of the power unit

In order to adjust the rms voltage value of the phase voltages, an AC chopper is used at the input of the delta connected primary windings of the transformer rated at 60 kVA. Two center-tapped windings present for each phase of the secondary part. The output is rectified and a DC pulsed current is used to feed the sample container to melt the sample. The operator set the required DC current flowing through the sample. After measuring the resistor current connected in series with the sample, thyristors are triggered by the system.

Current and voltage of one phase are measured and shown in Fig. 4. The phase current shows that the rectifier operates in discontinues conduction mode.

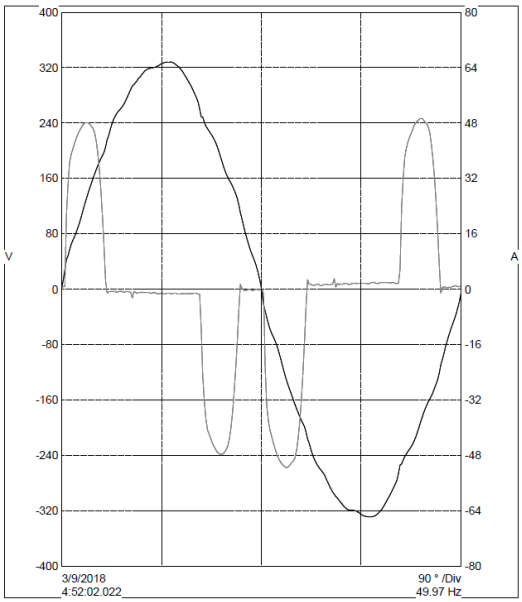

Figure 4. Voltage and current waveforms of the pulse DC electric current assisted sintering system measured for one phase

As seen from the figure that the phase current has more distortion than the phase voltage has. This means this system is a big harmonic source and have a low power factor and can affect other loads by mans of interaction at PCC.

3.2 Arc Furnace and Its Electrical Power Circuit

Electric arc furnaces (EAFs) are one of the common technology used in steel industries and widely used to produce steel by melting recycled scrap steel [23], [24], [31], [45]. The EAF contributes to steelmaking by providing more than 25% of the world's total crude steel production [14]. The melting of the required steel scrap results in a high energy intensive process, which requires efficient operation [24], [45], [46]. In this furnace, while multiple electrodes are used to transfer electrical power to the furnace, natural gas and oxygen injected from the burners provide chemical combustion after combustion [30]. It produces about 400 kilowatt-hours/ton of steel in its extremely intensive operation. Electric power is transferred to solid scrap by multiple electrodes. As the batch (heat) progresses, the scrap steel melts to form a flat molten steel bath at the bottom of the furnace. The metal also reacts with the oxygen present to give metal oxides floating on the molten metal such as slag. Reactions in the slag during heat are controlled by oxygen and carbon, and sometimes directly by the addition of lime, carbon and dolomite [14].

3.3 Induction Furnace and Its Electrical Power Circuit

In the steel industry, induction crucible furnaces (ICF) are widely used. ICF provides non-contact electromagnetic mixing, which enables the chemical homogeneity of the melt and mixing. In such furnaces, the time harmonic current I in a coil creates an oscillating magnetic field for heating the metal in the ICF. The magnetic field is controlled due to the harmonic nature of the so-called skin effect. This effect indicates that the magnetic field is mainly concentrated in a skin layer near the surfaces of the melt [27].

Modern metallurgy, melting technology on metals and alloys are widely applied. The typical side is this system is very good purity of the end product and its ability to shed refractory metals. In order to control the melting and thinning process, it is more convenient to do this in the pot. Therefore, induction melting furnaces are widely used in the production of materials for the latest technologies such as turbine blades used in aviation or implants and prostheses in biotechnology [26].

4. Possible Attack Scenarios

In this section, the attack types are classified, and some attack scenarios are given.

4.1 Attack Types

We separate the attack types into two categories: The harmful and the curious ones. The harmful ones result in physical harm. The curious ones do not result in any physical harm however it may let some technique information useful for making money stolen by the competitors. That’s why it is important to be protected from both types.

4.2 The curious attacks

If an example to a curious attack is to be given: Let’s assume the computer which are connected to an arc furnace or an electric current assisted sintering system has the information about what it is produced for which customer. If a hacker steals the information, it may harm the company financially or customer wise although no physical damage has occurred.

4.3 The harmful attacks

The harmful attacks can be categorized into three categories: Direct harmful ones, Indirect harmful ones and a Full attack. Direct harmful ones may damage the device, the product, the process costwise, timewise, and energywise. Indirect harmful ones may damage the neighboring device(s), the neighboring product(s), the neighboring process(es) costwise, timewise, and energywise. A full attack is the combination of both of the attacks occurring at the same time.

If an example to a direct harmful attack is to be given: Let's assume the computer which are connected to an arc furnace or an induction furnace or an electric current assisted sintering system has the control of the system(s).

- By turning on or turning off the device(s), the production process might be harmed or delayed.
- By turning off the process early, the desired sample cannot be produced by the electric current assisted sintering system since it is not reached to the desired temperature.
- By turning off the process early, the desired production cannot be made by the arc furnace or induction furnace system since it is not reached to the desired temperature. The metal parts can come out half-melted or unmelted and may have to be put into the furnace again.
- By increasing the control current, a hacker may cause a load voltage drop and this may harm devices which are sensitive to operation voltage.
- Tempering with temperature control by a hacker may result in sample destruction or produced not the way we wanted, i.e. the process is terminated with the product being half-baked.
- If the sample is destructed by a hacker, overall production would dissipate more electrical power be costlier, it would increase entropy more and be more harmful to environment.

If an example to an indirect harmful attack is to be given: Let's assume the computer which are connected to an arc furnace or an electric current assisted sintering system has the control of the system(s).

- By turning on or turning off the device(s), the voltage across the neighboring devices can be disrupted momentary: a voltage swell or a voltage lag occurs as shown in Fig. 5 and this may result in overvoltage or under voltage protection circuits of the neighboring devices be turned on and these may result in early termination of their production processes. These may turn out quite costly depending on what is produced and how much it is harmed. When such a voltage swell or a voltage lag occurs, in a moment, tens of thousands of dollars become wasted in pulp or plastic factories.
- By turning on or turning off the device(s), sometimes the attacker may harm the neighboring factories in the previously mentioned way.
- Both sintering devices, induction furnaces and arc furnaces are heavy harmonic sources. The harmonic examination of the arc furnaces has already been done in literature well-known [10], [12], [13], [18]–[21], [23], [28]. The harmonics of an electric current assisted sintering system is to be examined in the near future by the present authors. By turning on or turning off the device(s), harmonics or subharmonics can be produced and these may harm the neighboring devices or their production processes in a similar way a voltage swell or a voltage lag does. Subharmonics may result in ferromagnetic resonances in the power transformers.

- Also, the radiated electromagnetic interference (EMI) by the attacked devices may harm the devices resulting again damages in the previously mentioned ways.
- The harmed neighbors may take legal actions and this may result in economic losses if the factory attacked cannot prove its case.

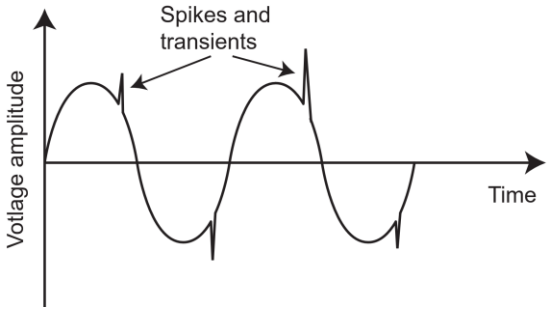

Figure 5. The voltage swell or voltage sag at the point of common coupling with the neighboring loads

5. Attack Prevention

If an attack happens, an effective recovery strategy should also be present in the electric current assisted sintering and Arc furnace manufacturing facility, which has been tried and tested by a multifunctional team, perhaps consisting of a software, a hardware and an electrical engineer, who understand the structured countermeasures needed. It can be said that developing awareness of cyber security across an automatized manufacturing company is also imperative for technique personnel such as workers, technicians, engineers etc. at all levels.

Material or metallurgical manufacturers should utilize developments in technology such as blockchain and full immune systems, which may be the future of cyber security in the fourth industrial revolution, to gain advantage in developing their processes, control systems and security.

Some solutions we suggest for manufacturing companies with electric current assisted sintering systems and Arc furnaces are the follows.

- In the first instance, as material manufacturing is centered around process control, understanding the difference between operational technology and information technology by the factory workers is very crucial for effective cyber security.
- The simplest solution for a manufacturing company is not to connect the manufacturing devices to Internet and only connect them to Ethernet.
- If they are connected to Internet, do not use operating systems with open doors or vulnerabilities.
- Use Linux-based operating systems which are less vulnerable to cyber-attacks
- Use encrypted programs for communication throughout Internet.
- Use fire-wall programs.
- Employ a cyber-security attack expert with an expertise in factory electrical system.
- If an attack happens, an effective recovery strategy should also be present in the material manufacturing facility, which has been tried and tested by a multifunctional team who understand the structured countermeasures needed.

- Learn to understand how to apply successful cyber security for the devices. The information supporting this includes the importance of an effective intrusion detection system (IDS) with examples of different types of IDS. It should also include a practiced and fluid recovery strategy.
- Forbid installing access programs in factory and have it diagnosed periodically like General Electric does.
- Have also manual control as a choice instead of just automatic control or controlling from Internet in case the system gets damaged.
- Let only monitoring of the electric current assisted sintering sample production and system variables such as voltage, current, temperature, etc. and do not allow the system operated through Internet or do not allow the system operated without encryption.
- Have an electronic record system or a data-logger for the devices or for the control programs of them to report anomalies with a program not effectible with internet connection.
- Need a security suite that helps protect all your devices– your Windows PC, Mac, ..., latest software releases and updates which installs security patches and fixes bugs.
- When updating old technology, differences in systems can lead to opportunities for intrusion, as can technology incompatibility. Therefore, a risk analysis should be on the agenda, to identify any areas of vulnerability prior to opportunities for internal or external attack being generated.
- Because of the very dynamic quality of the arc furnace load or the induction furnace or the electric current assisted sintering systems, power systems may require technical measures to maintain the quality of power for other customers; flicker and harmonic distortion are common side-effects of arc furnace operation on a power system. For this reason, the power station should be located as close to the EA furnaces as possible.
- In material manufacturing companies, regulatory compliance and clear governance objectives are crucial to minimizing risk.
- Understand the various types of industrial control systems; different types of systems pose different types of vulnerabilities when used for the sintering systems and Induction furnace devices.
- Improve the awareness of organizational vulnerability, technological threats, human influence, and external influence by educating the workers.
- It must be the company strategy to educate the new coming workers about cyber security of the devices by the experienced workers.
- The recovery plans should be backed up and easily reachable by the operators in case of a successful cyber-attack to the devices.

The material manufacturing devices are not required connect to the internet. However, it the future, they are most probably going to be, maybe just for monitoring and recording, maybe just for comfort and control, maybe for all of them, since the IoT become more common in each passing day. From this perspective, we wanted to provide possible cyber-attack scenarios and prevention strategies if they are connected to the internet through IoT or the computer connected to Internet.

6. Conclusion

A factory may be vulnerable to cyber-attacks if the production systems such as electric current assisted sintering systems, Induction furnaces and Arc furnaces are connected to internet. In this paper, it is shown how a sintering system or Induction furnace or an Arc furnace process may be damaged or cancelled with a Cyber-attack. The best way to prevent such an attack is to isolate its controls from internet or built-in codes to prevent early turn-off or turning off before manufacturing the product. A code should be written or exist to allow such a device to turn off only after once the production process is finished.

We have realized another danger: turning on and off a machine with a high power may danger other devices in factory or harm the production in neighbor factories due to voltage swells, voltage sags, and conducted EMI. Again, preventing early turn on or turn off may prevent such phenomenon.

We suggest prevention scenarios if such an attack happens. The likelihood level of such an attack is not our concern. In our opinion, it is best if an attack never happens or due to the attack prevention strategies given in this paper, such an attack is prevented or not resulted in no harm to the devices or company or neighbors. The solutions suggested in this paper can also be used for other manufacturing systems.

Any system connected to Internet can be hacked using proper attack programs which we are not expert on. We just implied the importance of cyber security in these manufacturing systems and, with which electrical methods, they can be attacked and how they can be prevented. Software wise, some other researcher can fill the gaps remaining. In 21st century, factories should be aware of such cyber-attacks and take the necessary precautions to keep their competitive edge.

References

[1] Ani, U. P. D., He, H. (Mary), and Tiwari, A., Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, J. Cyber Secur. Technol., 2017, 1, (1), 32–74.

[2] Tuptuk, N. and Hailes, S., Security of smart manufacturing systems, J. Manuf. Syst., 2018, 47, 93–106.

[3] Bullón Pérez, J., González Arrieta, A., HernándezEncinas, A., and Queiruga-Dios, A., Industrial Cyber-Physical Systems in Textile Engineering, Springer, Cham, 2017, 126–135.

[4] Cyber Security in Textile Manufacturing - Research and Markets, 2018.

[5] Yener, T. and Zeytin, S., Production and Characterization of Niobium Toughened Ti-TiAl3 Metallic-Intermetallic Composite, Acta Phys. Pol. A., 2017, 132, (3–II), 941–943.

[6] Yener, Ş. Ç. and Kuntman, H. H., Fully CMOS memristor based chaotic circuit, Radioengineering, 2014, 23, (4).

[7] Orrù, R., Licheri, R., Locci, A. M., Cincotti, A., and Cao, G., Consolidation/synthesis of materials by electric current activated/assisted sintering, Mater. Sci. Eng. R Reports, 2009, 63, (4–6), 127–287.

[8] Yener, S. C., Yener, T., and Mutlu, R., A process control method for the electric current-activated/assisted sintering system based on the container-consumed power and temperature estimation, J. Therm. Anal. Calorim., 2018, 1–10.

[9] Weintraub, G. and Rush, H., Process and apparatus for sintering refractory materials, 1913.

[10] Park, B., Lee, H., Jang, G., and Han, B., A fault analysis of DC electric arc furnaces with SVC harmonic filters in a mini-mill plant, Electr. Power Syst. Res., 2010, 80, (7), 807–814.

[11] Zimmermann, L., Avice, G., Blard, P.-H., Marty, B., Füri, E., and Burnard, P. G., A new all-metal induction furnace for noble gas extraction, Chem. Geol., 2018, 480, 86–92.

[12] Wu Ting, A new frequency domain method for the harmonic analysis of power systems with arc furnace, in *APSCOM-97. International Conference on Advances in Power System Control, Operation and Management*, 1997, 1997, 552–555.

[13] Alonso, M. A. P. and Perez Donsion, M., An Improved Time Domain Arc Furnace Model for Harmonic Analysis, IEEE Trans. Power Deliv., 2004, 19, (1), 367–373.
[14] Shyamal, S. and Swartz, C. L. E., Real-time energy management for electric arc furnace operation, J. Process Control, 2018.
[15] Silva, A. P., Segadães, A. M., and Lopes, R. A., Castable systems designed with powders reclaimed from dismantled steel induction furnace refractory linings, Ceram. Int., 2017, 43, 5020–5031.
[16] Lanzerstorfer, C., Electric arc furnace (EAF) dust: Application of air classification for improved zinc enrichment in in-plant recycling, J. Clean. Prod., 2018, 174, 1–6.
[17] Khodabandeh, E., Rahbari, A., Rosen, M. A., Najafian Ashrafi, Z., Akbari, O. A., and Anvari, A. M., Experimental and numerical investigations on heat transfer of a water-cooled lance for blowing oxidizing gas in an electrical arc furnace, Energy Convers. Manag., 2017, 148, 43–56.
[18] Chang, G. W., Liu, Y. J., Huang, H. M., and Chu, S. Y., Harmonic analysis of the industrial power system with an AC electric arc furnace, in *2006 IEEE Power Engineering Society General Meeting*, 2006, 4 pp.
[19] Mendis, S. R. and Gonzalez, D. A., Harmonic and transient overvoltage analyses in arc furnace power systems, IEEE Trans. Ind. Appl., 1992, 28, (2), 336–342.
[20] Vatankulu, Y. E., Senturk, Z., and Salor, O., Harmonics and Interharmonics Analysis of Electrical Arc Furnaces Based on Spectral Model Optimization With High-Resolution Windowing, IEEE Trans. Ind. Appl., 2017, 53, (3), 2587–2595.
[21] Donsion, M. P., Guemes, J. A., and Oliveira, F., Influence of a SVC on AC Arc furnaces harmonics, flicker and unbalance measurement and analysis, in *Melecon 2010 - 2010 15th IEEE Mediterranean Electrotechnical Conference*, 2010, 1423–1428.
[22] Gajic, D., Savic-Gajic, I., Savic, I., Georgieva, O., and Di Gennaro, S., Modelling of electrical energy consumption in an electric arc furnace using artificial neural networks, Energy, 2016, 108, 132–139.
[23] Teklić, A. T., Filipović-Grčić, B., and Pavić, I., Modelling of three-phase electric arc furnace for estimation of voltage flicker in power transmission network, Electr. Power Syst. Res., 2017, 146, 218–227.
[24] Rashid, M. M., Mhaskar, P., and Swartz, C. L. E., Multi-rate modeling and economic model predictive control of the electric arc furnace, J. Process Control, 2016, 40, 50–61.
[25] Buliński, P. *et al.*, Numerical and experimental investigation of heat transfer process in electromagnetically driven flow within a vacuum induction furnace, Appl. Therm. Eng., 2017, 124, 1003–1013.
[26] Bulin´ski, P. *et al.*, Numerical modelling of multiphase flow and heat transfer within an induction skull melting furnace, Int. J. Heat Mass Transf., 2018, 126, 980–992.
[27] Asad, A., Kratzsch, C., Dudczig, S., Aneziris, C. G., and Schwarze, R., Numerical study of particle filtration in an induction crucible furnace, Int. J. Heat Fluid Flow, 2016, 62, 299–312.
[28] Uz-Logoglu, E., Salor, O., and Ermis, M., Online Characterization of Interharmonics and Harmonics of AC Electric Arc Furnaces by Multiple Synchronous Reference Frame Analysis, IEEE Trans. Ind. Appl., 2016, 52, (3), 2673–2683.
[29] HOOSHMAND, R. A., Torabian Esfahani, M., and Torabian Esfahani, M., Optimal Design of TCR/FC in Electric Arc Furnaces for Power Quality Improvement in Power Systems, Leonardo Electron. J. Pract. Technol.
[30] Shyamal, S. and Swartz, C. L. E., Optimization-based Online Decision Support Tool for Electric Arc Furnace Operation, IFAC-PapersOnLine, 2017, 50, (1), 10784–10789.
[31] Khodabandeh, E., Ghaderi, M., Afzalabadi, A., Rouboa, A., and Salarifard, A., Parametric study of heat transfer in an electric arc furnace and cooling system, Appl. Therm. Eng., 2017, 123, 1190–1200.
[32] Yener, T., ECAS Yöntemiyle Üretilmiş Ti-Al Esaslı İntermetalik Kompozit Malzemelerin

Geliştirilmesi, Fen Bilimleri Enstitüsü, 2015.
[33] Laughton, M. A. and Warne, D. F., Electrical engineer's reference book. Newnes, 2003.
[34] Campbell, F. C., Metals fabrication : understanding the basics. .
[35] Bauccio, M. and American Society for Metals., ASM metals reference book. ASM International, 1993.
[36] Ostwald, P. F. and Muñoz, J., Manufacturing processes and systems. John Wiley & Sons, 1997.
[37] Robiette, A. G., V: Coreless Induction Furnaces, Electr. Melting Pract. Charles Griffin Co, 1935, 153–252.
[38] Fujii, N. and Koike, N., IoT Remote Group Experiments in the Cyber Laboratory: A FPGA-based Remote Laboratory in the Hybrid Cloud, in *2017 International Conference on Cyberworlds (CW)*, 2017, 162–165.
[39] Xu, L. Da, He, W., and Li, S., Internet of Things in Industries: A Survey, IEEE Trans. Ind. Informatics, 2014, 10, (4), 2233–2243.
[40] Ganti, R., Ye, F., and Lei, H., Mobile crowdsensing: current state and future challenges, IEEE Commun. Mag., 2011, 49, (11), 32–39.
[41] Stankovic, J. A., Research Directions for the Internet of Things, IEEE Internet Things J., 2014, 1, (1), 3–9.
[42] Torres, A., Santos, M., Balula, S., Fortunato, J., and Fernandes, H., Turning the internet of (my) things into a remote controlled laboratory, in *2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV)*, 2016, 371–374.
[43] Kortuem, G., Bandara, A. K., Smith, N., Richards, M., and Petre, M., Educating the Internet-of-Things Generation, Computer (Long. Beach. Calif)., 2013, 46, (2), 53–61.
[44] Bin, H., The Design and Implementation of Laboratory Equipments Management System in University Based on Internet of Things, in *2012 International Conference on Industrial Control and Electronics Engineering*, 2012, 1565–1567.
[45] Gajic, D., Savic-Gajic, I., Savic, I., Georgieva, O., and Di Gennaro, S., Modelling of electrical energy consumption in an electric arc furnace using artificial neural networks, Energy, 2016, 108, 132–139.
[46] Kirschen, M., Badr, K., and Pfeifer, H., Influence of direct reduced iron on the energy balance of the electric arc furnace in steel industry, Energy, 2011, 36, 6146–6155.