Gradus Vol 12, No 2 (2025)
ISSN 2064-8014

DEVELOPMENT OF IOT-BASED GROUND MONITORING SYSTEM

Andras NAGY [1,2] *

[1] Institute of Engineering, University of Dunaújváros, Hungary, https://orcid.org/0000-0002-5665-4324
[2] Insitute of Mechatronics and Vehicle Engineering, Óbuda University, Hungary
https://doi.org/10.47833/2025.2.ENG.012

Keywords:
ESD protection
Raspberry CM5
IoT
MQTT JSON

Article history:
Received 19 November 2025
Revised 09 December 2025
Accepted 12 December 2025

Abstract
This paper focuses on the server module of a newly developed system. This system has been designed to continuously monitor the grounding resistance of Electrostatic Discharge (ESD) protection equipment - an essential factor in ensuring reliability in modern electronics manufacturing where ESD-sensitive components are handled. The system's real-time monitoring and logging capabilities enable early detection of grounding issues, thereby minimizing the risk of ESD-related failures. The complete system consists of several workbench modules and a central server module. Communication between these modules is implemented using MQTT and JSON technologies. The server module runs on a Raspberry Pi with a Linux-based operating system; both its hardware and software components are briefly presented in this paper. The paper begins with an overview of ESD protection and its importance in electronics manufacturing and concludes with practical examples demonstrating how the technologies employed in this system can be applied in real-world production environments.

1 Introduction

Electrostatic discharge (ESD) poses a significant risk to sensitive electronic components, particularly complex semiconductors [1]. Uncontrolled ESD events can result in serious damage, leading to functional failures in electronic devices and decreased reliability in both products and production processes. The international standard IEC 61340 Parts 1 to 6 outlines the general requirements and measurement methods for ESD, as well as standardized procedures for testing ESD protection equipment, tools, and environments [2].

Typical ESD test protocols recommend daily testing of commonly used protective devices, such as wrist straps. However, if continuous ESD monitoring is implemented, daily testing may be unnecessary [3] in certain conditions. To address these requirements, this paper proposes a continuous ESD ground monitoring system, focusing on the server module (see Figure 2), designed to automate the verification of grounding integrity and reduce dependence on manual checks. Effective ESD protection begins with a fundamental goal: equalizing the electric potential across all conductive elements in a workspace to prevent static charge accumulation [4]. This is achieved by employing materials that dissipate electrical charges, while also ensuring that all components and personnel are properly grounded. The materials used for this purpose are classified based on their electrical resistance properties.

Conductive materials, as defined in IEC 61340-2-3, have resistance values below 10 kΩ [5], making it possible for them to rapidly transfer electrical charges. Dissipative materials, in contrast, have resistance values ranging from 10^4 to 10^{10} Ω [6], allowing for controlled discharge of static

* Corresponding author. E-mail address: andras.nagy@bgk.uni-obuda.hu

electricity without inducing high current flow. Materials with resistance above this range are considered insulators and are unsuitable for ESD protection most of the time.

While conductive materials allow for fast charge dissipation, this can also lead to fast current surges that may damage sensitive electronic components. To decrease the rate of dissipation, the industry commonly incorporates 1 MΩ resistors in grounding paths when connecting equipment or personnel to a common ground potential [7]. This resistance value limits current peaks while still allowing charge equalization. Proper selection and configuration of grounding materials are therefore essential not only for effective ESD control but also for ensuring the safety and longevity of delicate semiconductor devices.

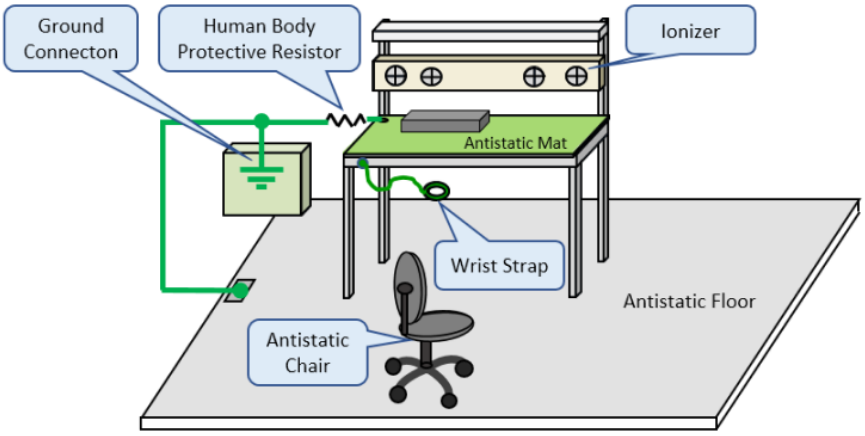

Figure1. Typical ESD safe workbench (Example) [8]

The most accepted upper resistance limit for ESD wrist straps is 35MΩ [9], therefore the resistance range from 1MΩ to 35MΩ is the best for dissipating static electricity. A typical ESD safe workbench can be seen in Figure 1.

Most common equipment that may require constant monitoring includes wrist straps, antistatic mats and, fixed tools such as soldering station or test instruments. The common grounding point is usually connected to the equipotential bonding system (EPB) of the building. When implementing ESD protection in a manufacturing facility, it may be necessary to customize the standard program for the specific workplace. One way to achieve such customization is by designing ESD protective measures based on ESD risk analysis, which takes into account possible sources of risks and their consequences regarding the type of workplace [10].

The optimization brings positive impacts in both technical and economic aspects. Reference [11] indicates that without established process control, actions targeting only the environment do not provide adequate ESD protection. The use of grounding as a means of reducing the accumulation of static charge and the presence of electric fields in the manufacturing environment is an effective and essential part of damage control [12]. ESD events can be detected by specialized high-speed electronics, such as the one described in [13], which detects high-frequency transient signals up to 450 MHz.

Wrist straps are used to safely dissipate static voltage build-up on a person and are considered an important static control product [14]. The level of static voltage that can build up on a person depends on several factors, including the material of clothes, the intensity of movement and the air humidity. The human body can generate static voltage by walking on a carpet as high as 2.5kV at 70% relative humidity, or 30kV at 20% relative humidity [4]. This amount of static voltage can easily damage sensitive electronics, highlighting the importance of personal grounding using a wrist strap.

2 Monitoring system design

The ground monitoring system presented in this paper consists of two parts: (i) several workbench modules to continuously monitor ESD ground resistance, and (ii) a central server module to collect, store and present measured data. This paper focuses on the central (server) module. The system architecture can be seen in Figure 2. The workbench modules are connected to the server module using WiFi technology, which may use either an existing or dedicated WiFi network for this application.

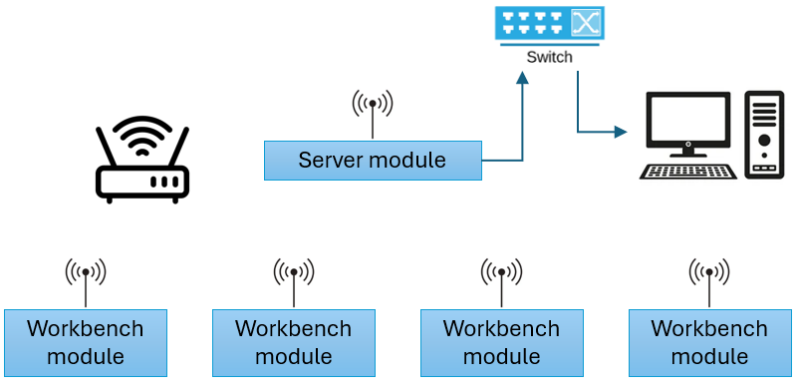

Figure 2. ESD ground monitoring system architecture

The server module is equipped with a wired network connection for integration with the user's local network. This enables the separation of the factory local network from the IoT network. By utilizing the LAN connection, the system can be monitored remotely from a PC or tablet. The workbench module is described in detail in another paper [15]. Its main functions are to measure the ESD grounding resistance, raise an alarm if the resistance exceeds a preset limit, and send the resistance values to the server.

The server module is based on Raspberry Compute Module 5 (CM5), which is a compact, high-performance system-on-module (SoM) designed for industrial and embedded applications. It has a quad-core 64-bit ARM Cortex-A76 processor, 4GB RAM and 32GB eMMC flash memory and wired and wireless connection including WiFi and Bluetooth 5.0. The main connector is two 100 pin high-density board-to-board mezzanine connector with 0.4 mm pitch from the Hirose DF40 series.

Raspberry module is widely used in industry and in scientific research also. It is successfully used in applications like CNC machine control [16], remote-controlled vehicle [17] or human detection [18]. The main factors why it is so popular are the low price, flexible and feature-rich hardware, Linux based open software, built-in wireless connectivity, and massive global community [19].

3 Hardware development

The main functions of the Raspberry Pi–based server module are (i) collect measurement data from workbenches via WiFi connection, (ii) process and store the data for statistical analysis and (iii) host the user interface. Since Raspberry CM5 runs Linux operation system, a sudden power loss may lead to data loss or file system corruption. To mitigate this risk, a dedicated uninterruptible power supply (UPS) is implemented to ensure a safe shutdown of the Raspberry Pi in the event of power loss. The operating system requires approximately 30 seconds to shut down safely, therefore the UPS must be capable of supplying power for at least 45 seconds. A supervisory microcontroller (MCU) monitors the status of the UPS circuit and issues a shutdown signal to the Raspberry Pi when a power failure is detected. At startup, the MCU also blocks the Raspberry Pi from booting until the UPS has enough stored energy to support a future safe shutdown. The UPS is based on supercapacitors, which are ideal for applications where frequent, short-duration backup is needed. It charges within tens of seconds, supports millions of cycles before degradation, and is more

environmentally friendly and compact than battery-based solutions. The block diagram of the UPS can be seen in Figure 3.

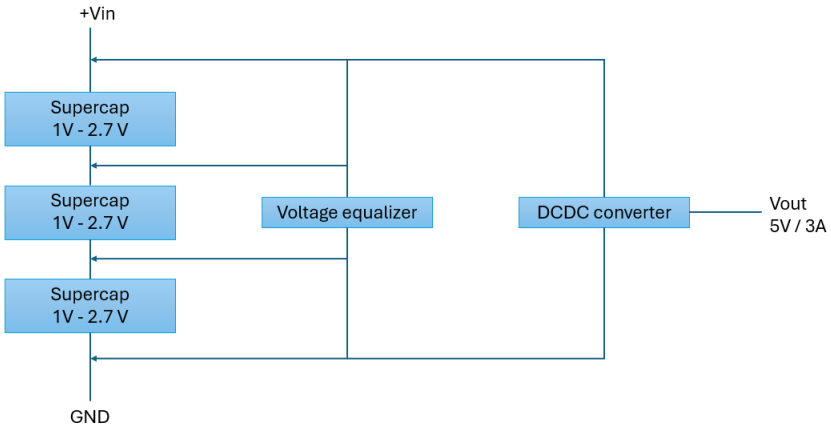

Figure 3. Block diagram of the UPS designed to protect Raspberry from power loss

The three supercapacitors are connected in series to provide a higher voltage for the DC-DC converter. A typical supercapacitor has a 2.7V voltage rating, in this design, the BCAP0025-P270-S12 is selected from Maxwell Technologies. It is a 25F / 2.7V component, with continuous discharge current rating of up to 3.7A [20], ideal for this application. In a series configuration, variations in capacitance or insulation resistance caused by manufacturing tolerances or aging can lead to uneven voltage distribution across the capacitors, potentially exceeding their voltage rating. Therefore, a balancing circuit (voltage equalizer) is required to prevent accelerated aging or damage of the capacitor cell [21]. The literature [22] categorizes balancing strategies by different properties like:

- energy dissipative behaviour
- balancing speed
- the type of technology that is used or
- pricing

Active balancing involves the use of actively controlled switches or amplifying systems, whereas passive balancing relies on shunts or self-regulating resistors to mitigate overvoltage. Compared to passive balancing, active balancing is faster and more energy-efficient, but also more expensive. In this paper, an active balancing circuit is implemented, the circuit schematic is shown in Figure 4.

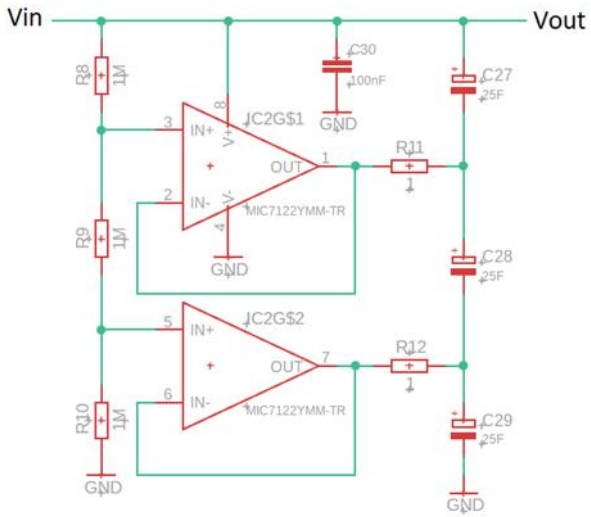

Figure 4. Schematic of supercapacitor balancing circuit

It can be seen, that a three-resistor voltage divider is used to evenly divide the input voltage to the required voltage level. This voltage signal is then fed into a buffer circuit composed of an operational amplifier. The primary requirement for the op-amp is to have high output current, so the MIC7122YMM from Microchip Technology is selected.

The output of the supercapacitor bank is connected to a DC-DC converter that provides a stable 5V supply for the RPi CM5. The maximum output current is set to 3 A. The DC-DC controller used is the LM3488 from Texas Instruments, a versatile low-side N-FET, high performance controller for switching regulators. The LM3488 includes thermal shutdown, short-circuit protection, and overvoltage protection, making it a robust solution for embedded applications. The circuit diagram of the DC-DC converter is shown in Figure 6.

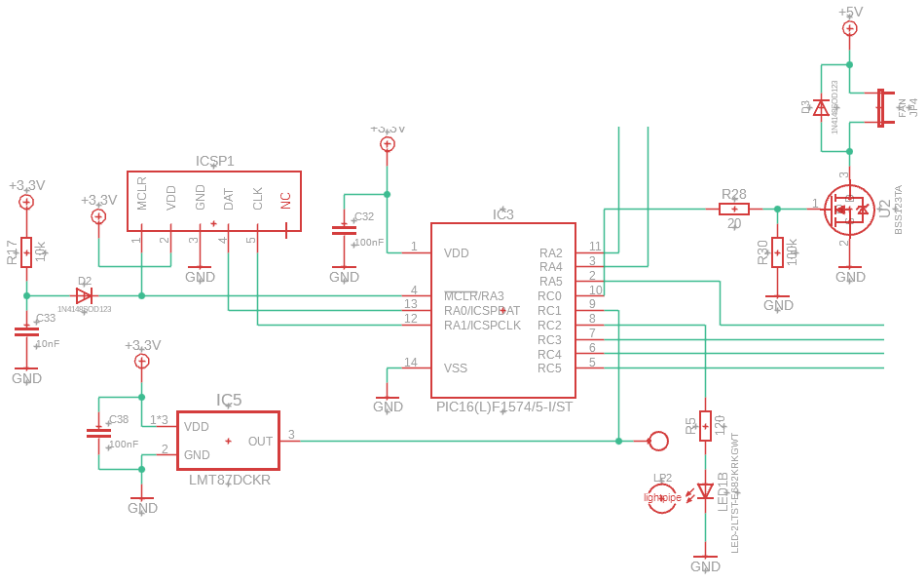

Figure 5. UPS supervisor microcontroller circuit

The external voltage is constantly monitored by a microcontroller (MCU), which can start/stop the RPi CM5 through its PWR_BUTTON input pin, as Figure 5 shows.

A UART serial communication is also implemented between RPi and MCU to make it possible to display diagnostic information about the UPS sub-circuit.

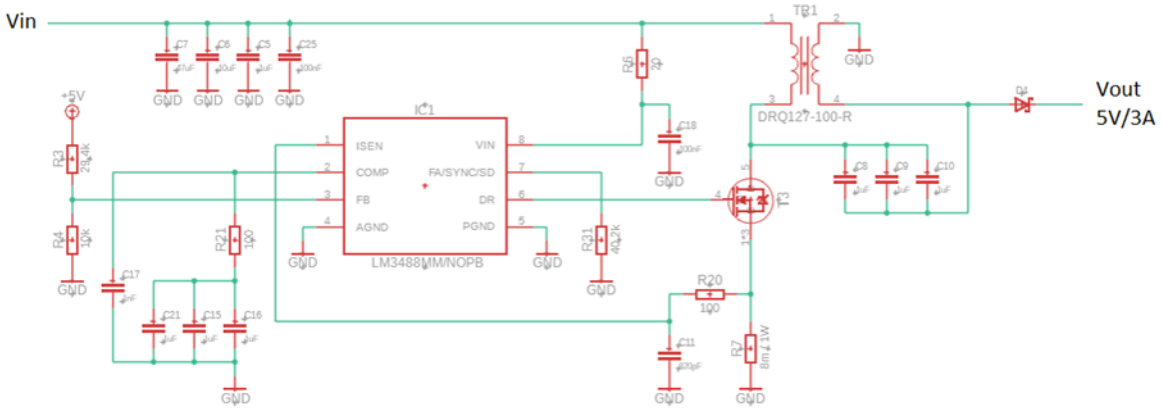

Figure 6. Schematic of the DC-DC converter of UPS

The RPi CM5 itself has an on-board u.FL RF connector for wireless antenna connection. The wired LAN connection is also designed using ARJM11D7-009-AB-EW2 MagJack as described in the datasheet of the RPi CM5 [23]. A coin cell battery holder is also added to support the on-board real-time clock (RTC).

Once the schematic was finalized, the PCB was designed on standard two-layer FR4 board. The 3D model of the hardware is shown in Figure 7. The PCB fits into a Hammond 1455J602 aluminium enclosure, which is equipped with a 20x20mm FAN in order to keep the internal temperature on a moderate level. Since the RPi CM5 can dissipate significant heat—reaching 50–60°C even under light load—overheating is mitigated by monitoring the internal temperature via an LMT87 sensor. The MCU controls the fan based on this sensor data.

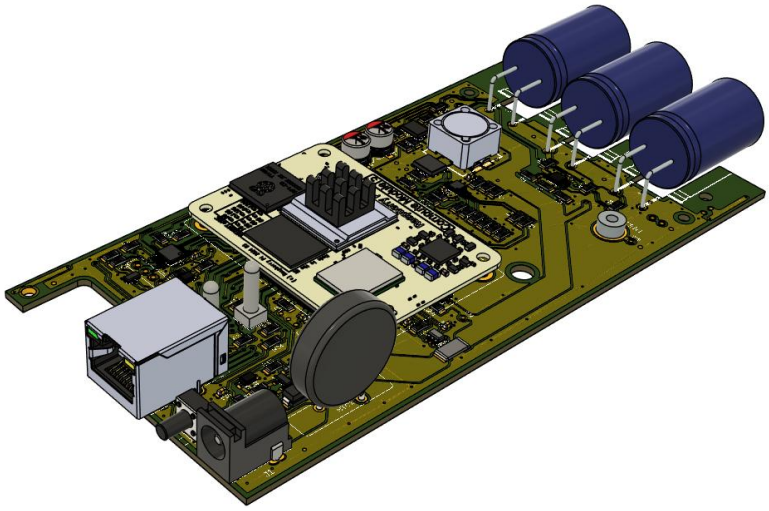

Figure 7. 3D model of the server module electronics

4 Software environment

The Raspberry Pi in the server module runs Raspberry Pi OS, a Debian Linux-based operating system and the official OS for RPi CM5. While Raspberry Pi OS is typically installed on an SD card, the RPi CM5 instead uses internal eMMC storage as its primary memory. The same imaging tool can be used with the RPi CM5, but the module must first be booted into upload mode. In this mode, it can be connected to a PC via USB and will appear as a mass storage device, allowing the OS image to be written directly to the eMMC. After the OS is uploaded and the RPi CM5 restarted in normal mode. Afterward, SSH can be used to access the device over a wired or wireless LAN.

The main tasks of the server module are (i) manage the MQTT connection with the workbench modules and (ii) host the user interface. The data received from the workbench modules is stored in a MySQL database, which is provided through the MariaDB package and is installed using the Advanced Package Tool (APT) library (apt-get) of the operating system. The Mosquitto Broker package, which provides the MQTT server, is installed in the same way.

Designed for Internet of Things (IoT) applications, MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol based on the publish–subscribe model. It is particularly well-suited for environments with limited resources and low-bandwidth connectivity. Instead of direct device-to-device communication, MQTT allows devices to publish messages to designated topics, while other devices subscribe to those topics to receive relevant information efficiently [24]. A key concern with MQTT is security, as the protocol does not include built-in encryption mechanism. Studies [e.g., 25] show that botnet and IoT-based attacks can overload MQTT servers through excessive connection attempts, disrupting system operation. The MQTT protocol is widely used in cloud integration of industrial IoT systems. [26] provides a comprehensive survey of cloud-based IoT architectures and security models, highlighting how the rapid adoption of cloud computing has improved industrial capabilities, while introducing significant security challenges across certain domains.

The Mosquitto MQTT broker receives data packages from the workbench modules, which are then stored in a MySQL database using a custom Python script. The script processes the MQTT

data, checks for errors, and inserts the valid entries into the database [see Figure 8]. It is configured to run as a background service, allowing the operating system to monitor it and automatically restart in case it is not running.

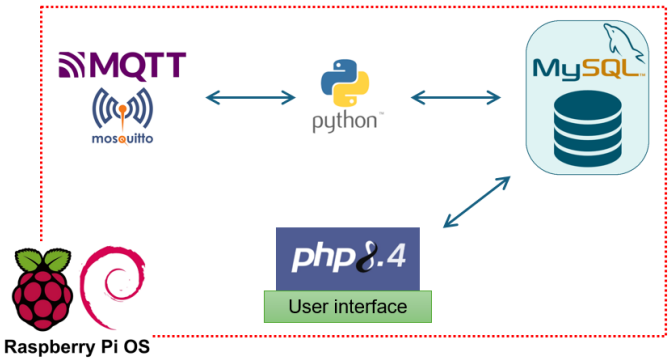

Figure 8. Software technologies used in server module

The MQTT messages use JSON (JavaScript Object Notation) objects, which helps standardize communication. JSON is a text-based format for representing structured data and is widely used in IoT systems for data exchange between devices and applications. To improve system security, the JSON payloads can be encrypted using AES-128 encryption. This ensures data confidentiality and reduces the risk of interception or tampering on unsecured networks. JSON is a widely used as a data format, used for example in [27] for storing data in machine learning.

To host the user interface, Apache webserver, php and phpMyAdmin are installed. The user interface can be accessed from any modern device capable of running a web browser. Although initial testing of the user interface has begun, it is not yet finalized and may be completed as a future student project. Access control should also be implemented to protect both the collected data and the system settings.

5 Conclusion and summary

Electrostatic discharge (ESD) has been recognized as a significant source of damage to unprotected electronic components and assemblies for more than 40 years. A fundamental approach to ESD protection is grounding, which safely dissipates potential differences. To ensure effectiveness, grounding systems must be tested regularly. While floors, mats, and equipment are typically checked annually, daily-use items such as wrist straps should be tested each day. However, daily manual testing introduces the risk of human error and oversight. Continuous ground monitoring can mitigate these issues and provide more consistent protection.

This paper describes the design and prototyping of a continuous ESD ground monitoring system. The system consists of a central server module and multiple workbench modules; this paper focuses on the server module. To enable remote monitoring from a PC or tablet, the server module connects to the user's LAN through a wired network. This configuration separates the user interface from the IoT network, allowing secure and efficient integration with local infrastructure. Wireless communication is performed via Wi-Fi using MQTT and JSON technologies. The server runs Raspberry Pi OS, a Debian-based Linux system, and uses Python scripts to process incoming data and store it in a MySQL database.

A prototype has been built and tested to demonstrate the feasibility of the concept. The system provides several practical contributions to ESD monitoring and industrial IoT. Unlike conventional ESD compliance methods that rely on manual daily testing, this solution enables fully automated, real-time monitoring of grounding resistance using custom electronics. The use of the Raspberry Pi Compute Module 5 (RPi CM5), combined with a custom-designed supercapacitor-based uninterruptible power supply (UPS), ensures high reliability and protection against data loss during power interruptions—an aspect often overlooked in similar systems. The development process offers participating students valuable experience in product design and hands-on exposure to a range of

IoT technologies. By involving students in the creation and testing of the system, the project also serves as an educational platform that fosters practical skills and encourages future innovation in IoT-based manufacturing solutions.

References

[1] X. Wang et al., "ESD protection for RF/AMS ICs: Design and optimization," 2009 IEEE International Conference on IC Design and Technology, Austin, TX, USA, 2009, pp. 25-28, doi: 10.1109/ICICDT.2009.5166257.

[2] IEC website: https://webstore.iec.ch/, 2025.02.02.

[3] ESD Association, “Fundamentals of Electrostatic Discharge Part Three - Basic ESD Control Procedures and Materials”, 2020, https://www.esda.org/assets/Documents/Fundamentals-of-ESD-Part-3-Basic-ESD-Control-Procedures-and-Materials.pdf

[4] T. Ohtsu and K. Sagisaka, "Study on discharge characteristics of the ESD protection material and the effect of protection element," 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Shenzhen, China, 2016, pp. 426-428, doi: 10.1109/APEMC.2016.7522758.

[5] T. Viheriäkoski, E. Kärjä, P. Horsma-aho, R. Gärtner and J. Smallwood, "ESD Risks of Containers Made of Conductive Compounds," 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, USA, 2018, pp. 1-9, doi: 10.23919/EOS/ESD.2018.8509696.

[6] T. Viheriäkoski, P. Tamminen, M. Laajaniemi, E. Kärjä and J. Hillberg, "Uncertainties in surface resistivity measurements of electrostatic dissipative materials," 2013 35th Electrical Overstress/Electrostatic Discharge Symposium, Las Vegas, NV, USA, 2013, pp. 1-7.

[7] A. Wallash, "A study of “soft grounding” of tools for ESD/EOS/EMI control," 2007 29th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Anaheim, CA, USA, 2007, pp. 2B.8-1-2B.8-6, doi: 10.1109/EOSESD.2007.4401746.

[8] Sanken Electric CO.LTD. website: https://www.semicon.sanken-ele.co.jp/en/support/reliability/4-9.html, 2025.05.07

[9] K. P. Yan, R. Gaertner and C. Y. Wong, "ESD protection program at electronics industry — Areas for improvement," Electrical Overstress/Electrostatic Discharge Symposium Proceedings 2010, Reno, NV, USA, 2010, pp. 1-6.

[10] M. Sahul and P. Janiga, "Optimization of ESD Protection Design for Assembly Lines of Headlights Through Risk Analysis," 2024 24th International Scientific Conference on Electric Power Engineering (EPE), Kouty nad Desnou, Czech Republic, 2024, pp. 1-5, doi: 10.1109/EPE61521.2024.10559564.

[11] T. Viheriäkoski, J. Kohtamäki, T. Peltoniemi and P. Tamminen, "Benchmarking of factory level ESD control," 2015 37th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), Reno, NV, USA, 2015, pp. 1-7, doi: 10.1109/EOSESD.2015.7314769.

[12] L. B. Levit, G. C. Rider and I. Mirshad, "Electrostatic Damage in Semiconductor Manufacturing Through the Inappropriate Use of Grounding," 2022 44th Annual EOS/ESD Symposium (EOS/ESD), Reno, NV, USA, 2022, pp. 1-8, doi: 10.23919/EOS/ESD54763.2022.9928507.

[13] I. -H. Wu and M. -D. Ker, "ESD-Event Detector for ESD Control Applications in Semiconductor Manufacturing Factories," in IEEE Transactions on Electromagnetic Compatibility, vol. 64, no. 6, pp. 1793-1801, Dec. 2022, doi: 10.1109/TEMC.2022.3195233.

[14] T. Namaguchi and H. Uchida, "Wrist strap designs and comparison of test results according to MIL-PRF-87893 and ANSI EOS/ESD association S1.1," Electrical Overstress/ Electrostatic Discharge Symposium Proceedings. 1998 (Cat. No.98TH8347), Reno, NV, USA, 1998, pp. 245-251, doi: 10.1109/EOSESD.1998.737044.

[15] Andras Nagy, “Development of an IoT-Based Continuous Ground Monitoring System for Enhanced Reliability”, 29th IEEE International Conference on Intelligent Engineering Systems, 2025

[16] S. Koprda, Z. Balogh, M. Magdin, J. Reichel, Gy. Molnár, “The Possibility of Creating a Low-Cost Laser Engraver CNC Machine Prototype with Platform Arduino”, Acta Polytechnica Hungarica, Vol. 17, No. 9, 2020, DOI:10.12700/APH.17.9.2020.9.10

[17] Kenzhetayev, Yernar & István, Nagy. (2024). “A Real-time, Remotely Operated Vehicle, using a Raspberry Pi and a Virtual Reality Headset.” Acta Polytechnica Hungarica. 21. 125-146. 10.12700/APH.21.8.2024.8.7.

[18] Drenyovszki, Rajmund & Zsupányi, Krisztián. (2023). SZEMÉLYEK DETEKTÁLÁSA HŐMÁTRIX SZENZORRAL ÉS HIERARCHIKUS KLASZTEREZÉSSEL HUMAN DETECTION USING THERMAL ARRAY SENSOR AND HIERARCHICAL CLUSTERING. Gradus. 10. 10.47833/2023.2.CSC.026.

[19] S.E. Mathe, H.K. Kondaveeti, S. Vappangi, S. D. Vanambathina, N.K. Kumaravelu, “A comprehensive review on applications of Raspberry Pi”, Computer Science Review, Volume 52, 2024, 100636, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2024.100636.

[20] BCAP0025-P270-S01 supercapacitor datasheet from Maxwell Technologies, 2025: https://maxwell.com/wp-content/uploads/2021/08/2_7_25F_ds_3001978_datasheet.pdf,

[21] H. Li, J. Peng, J. He, Z. Huang, J. Pan, “Synchronized Cell-Balancing Charging of Supercapacitors”, IFAC-PapersOnLine, Volume 50, Issue 1, 2017, Pages 3338-3343, ISSN 2405-8963, DOI: 10.1109/TIE.2018.2798615

[22] B.T., Prashant & Bobba, Phaneendra & Suresh, K.. (2019). Extensive review on Supercapacitor cell voltage balancing. E3S Web of Conferences. 87. 01010. 10.1051/e3sconf/20198701010.

[23] Raspberry Compute Module 5 datasheet: https://datasheets.raspberrypi.com/cm5/cm5-datasheet.pdf, 2025

[24] Hegyi, Henrietta & Erdődi, László. (2024). Modern Passenger Vehicles as Cyber Threat Source: Analyses of Surveillance Options through Smart Vehicles. Acta Polytechnica Hungarica. 22. 2025. 10.12700/APH.22.2.2025.2.2.
[25] Owen H, Zarrin J, Pour SM. A Survey on Botnets, Issues, Threats, Methods, Detection and Prevention. Journal of Cybersecurity and Privacy. 2022; 2(1):74-88. https://doi.org/10.3390/jcp2010006
[26] Ehsan Bazgir, Ehteshamul Haqu, Numair Bin Sharif and Md. Faysal Ahmed: Security aspects in IoT based cloud computing, World Journal of Advanced Research and Reviews, 2023, 20(03), 540–551, DOI: https://doi.org/10.30574/wjarr.2023.20.3.2481
[27] Jozsef, Cserko & Pasztor, Attila. (2023). Mesterséges intelligencia adatkészletek hatékony fordítása nyílt forrású technológiák segítségével. Gradus. 10. 10.47833/2023.2.CSC.021.