Towards a secure and automated platform for fingerprint-based electronic voting machine

Ifthekhar Ahammad*, Pradip Lal Biswas, Juwel Chowdhury, Obaedur Rahim Rizbhi, Sanjana Siraj and Ashraful Islam

Department of Electrical and Electronic Engineering,
Leading University (LU),
Rang Mahal Tower, Bandar Bazar,
Sylhet-3100, Bangladesh
Email: ifthekharahammad@gmail.com
Email: ifthekhar@lus.ac.bd
Email: pradipbiswas22@gmail.com
Email: juwel.chow@gmail.com
Email: rizbhi91@gmail.com
Email: sanjanasiraj@gmail.com
Email: ashraful.islam@lus.ac.bd
*Corresponding author

Abstract: Electronic voting machines (EVM) inherit the act of voting using electronic systems to cast and count votes. This paper deals with the design and development of an electronic voting machine using biometric fingerprint identification system in order to provide better performance, flexibility and economic advantages with higher level of security to the casting and voting system. The proposed fingerprint-based EVM allows the voters to scan their fingerprint, which is then compared with the database. Upon completion of voter identification, voters are allowed to cast their votes and votes are updated immediately. The proposed electronic voting system is fast, efficient and fraud-free. It provides better security with biometric fingerprint system, makes the voting machine user friendly and reduces the cost to a minimum level.

Keywords: EVM; fingerprint; voting machine; automatic; biometrics; machines; robotics.

Reference to this paper should be made as follows: Ahammad, I., Biswas, P.L., Chowdhury, J., Rizbhi, O.R., Siraj, S. and Islam, A. (2018) 'Towards a secure and automated platform for fingerprint-based electronic voting machine', *Int. J. Intelligent Machines and Robotics*, Vol. 1, No. 1, pp.34–44.

Biographical notes: Ifthekhar Ahammad received his BSc degree in 2013 from American International University, Bangladesh. Currently, he is working as a Senior Lecturer at Leading University, Sylhet, Bangladesh. His current research interest focuses on brain-computer interfaces, prosthetic limbs, biosensors, automation, robotics and navigation system.

Pradip Lal Biswas completed his BSc degree in 2015 from Leading University, Sylhet, Bangladesh. His current research interests are biometrics, artificial intelligence, communication system and networking.

Juwel Chowdhury received his BSc Engineering degree in 2016 from Leading University, Sylhet, Bangladesh. His current research interest focuses on fingerprint technology, biosensors, and automation.

Obaedur Rahim Rizbhi received his BSc degree in Electrical and Electronic Engineering in 2015 from Leading University, Sylhet Bangladesh. Currently, he is working as a Junior Engineer at Baraka Power Limited (50MW Power Plant), Sylhet & Baraka Patenga Power Limited (50MW Power Plant), Chittagong, Bangladesh. His current research interest focuses on smart power grid system, nanotechnology, biosensors, automation, robotics and navigation system.

Sanjana Siraj received her BSc degree in Electrical and Electronic Engineering from Ahsanullah University of Science and Technology, Dhaka, Bangladesh, in 2012. She worked at Leading University Sylhet, Bangladesh as a faculty member from 2013 to 2016 in the post of a Senior Lecturer.

Ashraful Islam received his BSc degree in 2015 from Military Institute of Science & Technology. Currently, he is working as a Lecturer at Leading University, Sylhet, Bangladesh. His current research interest focuses on automation, wireless communication, image processing and antenna design.

1 Introduction

An everlasting debate is contributing many facts to the concept of electronic voting machines. The most alarming concern is the security of these systems. Biometrics is the science and technology of measuring and analysing biological data. In this project, biometric fingerprint impression is used for the purpose of voter identification and authentication. As the fingerprint impression of every individual is unique (Jain et al., 2016; Jasuja, et al., 2016) it helps in maximising the security. The arrangement demands the user to submit his fingerprint at the scanning module as an identity proof. The system reads the data from the fingerprint and verifies this data with the already stored information in its database. If the information saved in the database matches with the stored data, the system allows the person to vote. Illegal voting and repetition of votes is checked in the system. If the details of the finger do not match with the stored data or it detects repetition, the system immediately displays it on the monitoring device and turns on the alarm. The authorities then can come and take necessary actions. A database is created with the fingerprint impression of all the voters in the constituency. If this system is employed, elections would be fair and deception free.

Electronic voting systems for electorates have been in use since the 1960s, when punched card systems debuted (Historical Timeline – Voting Machines – ProCon.org., 2016; The Electronic Voting Machine History, 2016; Hasan et al., 2016). Their first widespread use was in the USA where seven counties switched to this method for the 1964 presidential election and the name of the first electronic voting machine was ‘collector of electronic votes’ (Historical Timeline – Voting Machines – ProCon.org., 2016; The Electronic Voting Machine History, 2016; Hasan et al., 2016). Since the

beginning, security has been a big issue and inspection of the system was requested numerous times after the election period (Weldemariam et al., 2011; Shrivastava and Shrivastava, 2016). Smartcard-based voting system is one of the debated concepts of EVM because smart-cards are more likely to get damaged and it is even more susceptible to hacking (Newman, 2010; Karima et al., 2014). These are basically RFID related technology that can easily be hacked and illegal voters can carry multiple cards to vote in lieu of the authorised person, thus going back to the old age of voting. Basic voting machines which store the voting data in EEPROM (Bhatia and Gupta, 2014; Hoquec, 2014; Paul, 2013) are somewhat useful in some corporate environment where security is not an issue but not suitable to elect a government. To ensure a secure election procedure these systems provide little satisfaction. Modern biometric techniques can provide more user friendly and secure system (Weldemariam et al., 2011; Shrivastava and Shrivastava, 2016). This paper focuses on the biometric fingerprint-based voting system where voters can simply use their fingerprint to identify their presence and provide their vote with a push of a button. It meets the security requirements (Weldemariam et al., 2011; Shrivastava and Shrivastava, 2016) and helps both new and regular voters to vote easily.

A voting machine should be user friendly. People most of the time forget, or in the case of novel voters, it is quite possible to make mistakes while using the voting machine for the first time. Complicated voting system can lead to the election of a wrong candidate. To make everyone understand the procedure, we have used clear and understandable command or instruction. We have chosen an offline-based electronic voting system which is easy to implement and can organise the database properly by eliminating the prospects of hacking. This fingerprint-based voting system will give elections a secure voting procedure and confidence on the result of the election as authorised persons only able to declare the results. The result can be presented immediately with automated counting system which is impossible for the traditional voting procedure. This system is cost effective, secure and easy to operate.

2 Methodology

This fingerprint-based electronic voting machine works in four steps. Those are enrolment, voting, election result demonstration and restoring database for the next election. There are three types of users in this machine. Those users are voter, master user and super user. Master users show the result and super users erase the data of previous election.

When the power is turned on, the system initialises and does a complete system diagnosis to find errors. Then it waits for the initial command that will set its mode as Enrolment, Election, Result or Erase mode (Figure 2). Authorised person's fingerprints will issue this access to the particular section. A reset switch is used to go back to the initial command section after completing the operation of a particular section. The circuit diagram is shown in Figure 1.

Figure 1 Circuit diagram of EVM (see online version for colours)

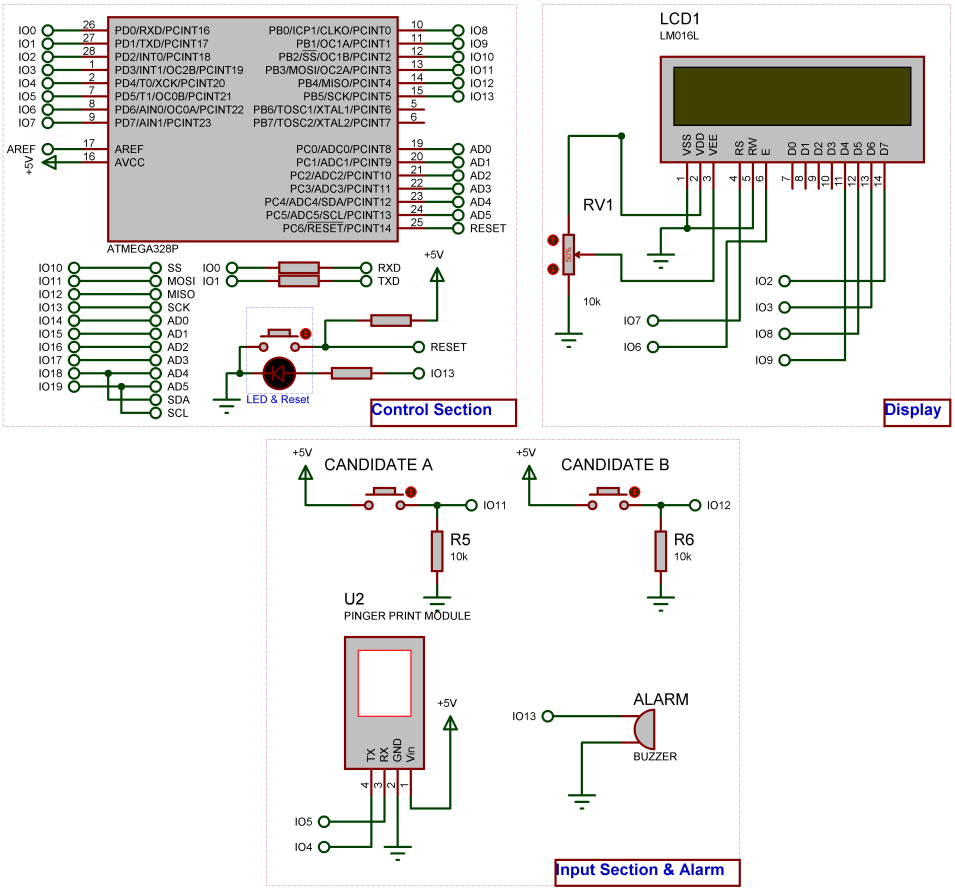
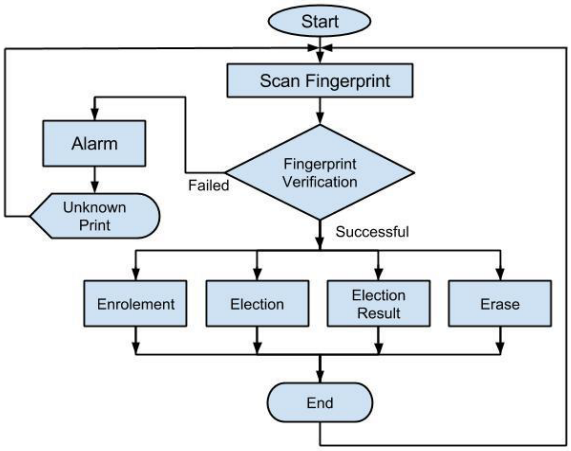


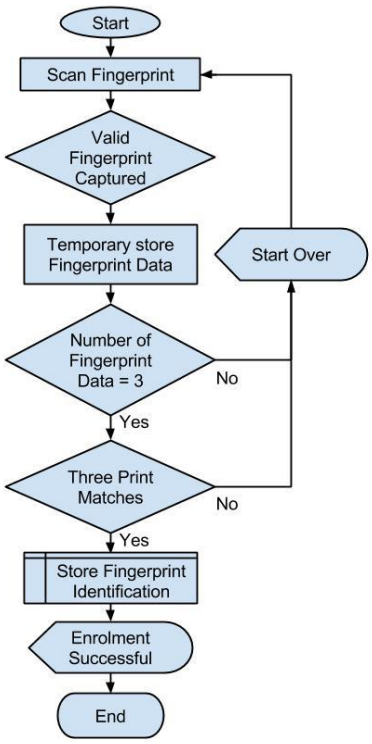
Figure 2 Flow chart of EVM (see online version for colours)



2.1 Enrolment

After the system becomes authorised to start the enrolment process, voters are enrolled using their fingerprint (Figure 3). Individuals are asked to provide fingerprint for three times and after a successful enrolment, identification of that voter is stored in the system's database.

Figure 3 Flow chart of enrolment section (see online version for colours)



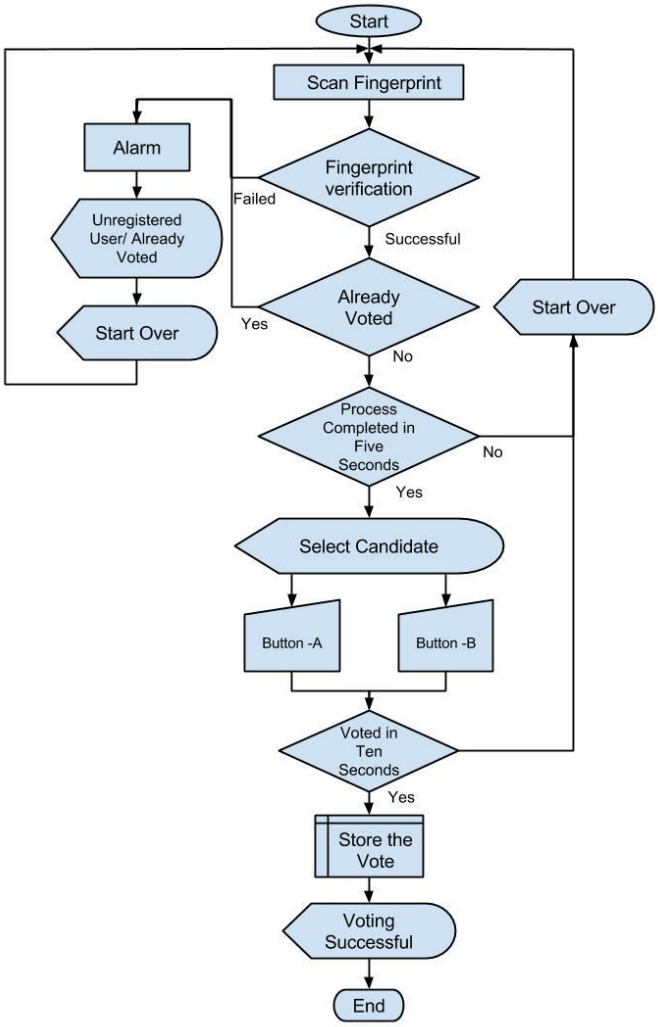
2.2 Election

During the voting period, the authorised person activates the voting mode of the EVM then voters are asked to provide their votes using their fingerprint for the identity verification (Figure 4). The scanner captures the finger image and the system checks it to the

pre-stored impression in the database. If the finger image matches, the system grants access to the voting procedure, but not before it checks the voting status of that person. If the voter has already voted, it shows a message on the LCD display and informs the authority about the situation by turning on the alarm. Unlisted voters are also detected in a similar manner. If the finger print matches and the voter has not voted until now, the EVM asks the person to vote. In this EVM system, currently there are two push switches for identifying two political parties or candidates. When the voter presses a particular switch (A/B) to vote for his candidate, EVM stores the vote for that candidate. If the voter does not complete the session in ten seconds, he has to start over from the

fingerprint section. After providing the vote, a confirmation message is shown in the display. The voting information is saved in a non-volatile memory, so power failure and interruption cannot hinder the voting procedure.

Figure 4 Flow chart of election section (see online version for colours)



2.3 Election result

For the result section, there is a two-step verification process. To open the result section, two Master Users must provide their finger prints one after another within five seconds (Figure 5), otherwise it returns to the default window. When the first user provides the biometric information, it allows the second user to provide his biometric identification and only after that verification, the display shows the total votes of both parties.

Figure 5 Flow chart of result section (see online version for colours)

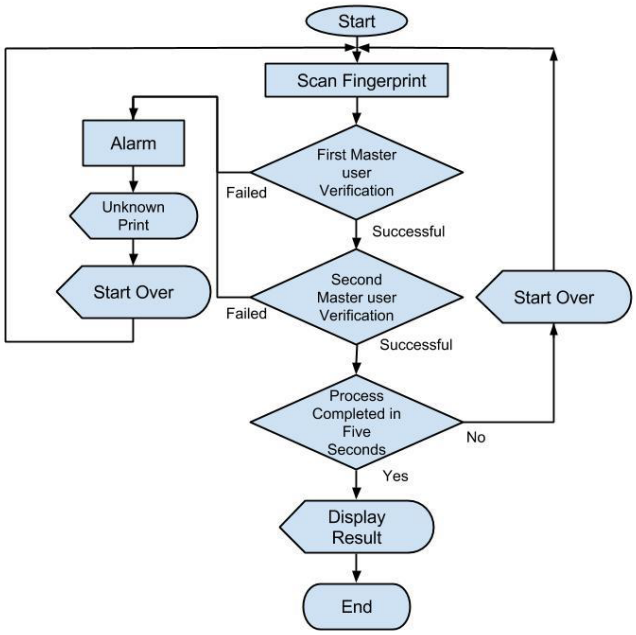
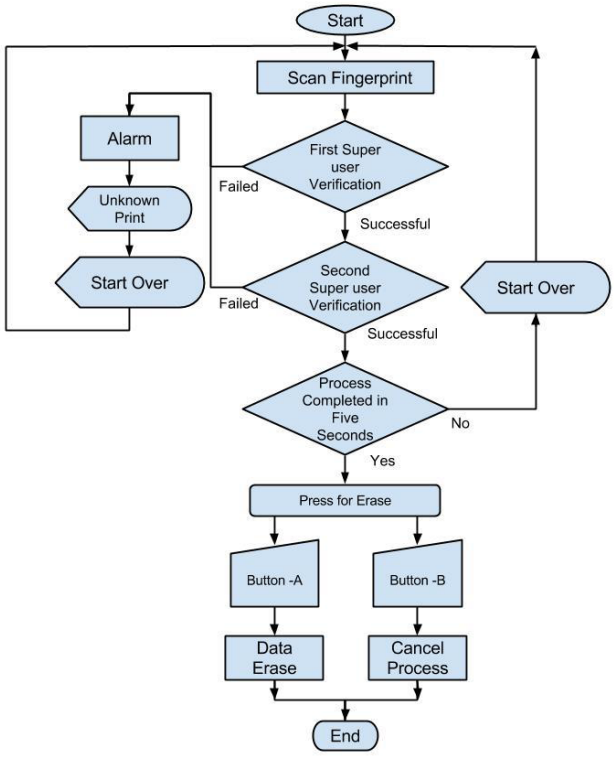


Figure 6 Flow chart of erase section (see online version for colours)



2.4 Erase

The erasing system works the same way as the result section but with two different super users (Figure 6). After the verification process, the display shows two options (Yes/No) to erase the data.

3 Result

The main goal for this project was to provide better security, making the electronic voting machine user friendly and cost effective. This paper deals with the design and development of an electronic voting machine where biometric fingerprint method has been successfully introduced to provide high performance with higher level of security to the voting system.

It registers a voter with biometric fingerprint identification (Figure 7). The proposed fingerprint EVM allows the voters to scan their fingerprint which is then verified with an already saved fingerprint impression within the database. Upon completion of voter identification, voters are allowed to register their votes (Figure 8). After the election period the result can be displayed immediately without any mistakes (Figure 9) and after a successful election the system can be re-organised for the next election (Figure 10). This electronic voting system is fast, efficient and fraud-free.

Figure 7 Fingerprint verification process (see online version for colours)

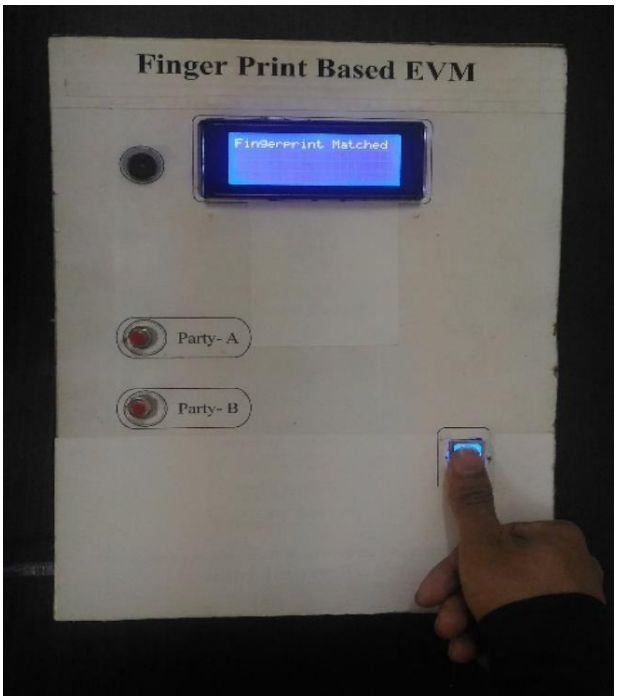


Figure 8 Selection process of candidate (see online version for colours)

Figure 9 Result section of EVM (see online version for colours)

Figure 10 Erase section of EVM (see online version for colours)

4 Discussion

EVM machines should be secure and easy to use. With the multiple stages of verification and authorisations, the whole process of voting is no longer controlled by a particular human being or authority. It ensures the transparency and security of the election system. From enrollment to voting session and result publication to erasing old data, at every stage instructions are shown on the LCD display, so that any confusion regarding the decisions can be understood clearly. Furthermore, during the election period, it will be very helpful if the voting procedure is shown in the mass media. Further improvements can be made to the security system by adding multiple biometric security platforms. A GSM system can also be added to send a confirmation to the voter and to make it more user-friendly, besides a speech assistance system along with visual aid can be used inside the polling booth.

5 Conclusions

The findings that this paper has presented suggest that EVM system can be the future of the election procedure if the security of the overall procedure can be guaranteed and the voters are aided with the right information. This research has resolved these two important issues of the electronic voting machines. Biometric fingerprint-based identification system ensures the security of the overall system and interactive graphical

LCD display guarantees user-friendliness. The proposed system was developed for under 100$ which is far cheaper than the traditional ballot paper system. Overall, it is the solution of security and transparency complications with the advantages of cost effective approach and easiness.

References

Bhatia, V. and Gupta, R. (2014) 'A novel electronic voting machine design with voter information facility using microcontroller', *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, DOI: 10.1109/indiacom.2014.6828142.

Hasan, S.M., Rashid, M.T., Chowdhury, M.S. and Rhaman, M.K. (2016) 'Development of a credible and integrated electronic voting machine based on contactless IC cards, biometrie fingerprint credentials and POS printer', *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, DOI: 10.1109/ccece.2016.7726821.

Historical Timeline – Voting Machines – ProCon.org. (n.d.) (2016) [online] http://www.bing.com/cr?IG=71A7BFD825FE429EA9B27112D3A016A5&CID=2D1BBBC75AE565EA1564B22D5BD464DF&rd=1&h=bG9wOK9lbwKZrX1TqWQWeOGJuVBQl8XUAqckCuqaA0k&v=1&r=http://votingmachines.procon.org/view.timeline.php?timelineID=000021&p=DevEx,5050.1 (accessed 13 December 2016).

Hoquec, M.M. (2014) 'A simplified electronic voting machine system', *International Journal of Advanced Science and Technology*, January, Vol. 62, pp.97–102, DOI: 10.14257/ijast.2014.62.07.

Jain, A.K., Nandakumar, K. and Ross, A. (2016) '50 years of biometric research: accomplishments, challenges, and opportunities', *Pattern Recognition Letters*, Vol. 79, No. 2016, pp.80–105, DOI: 10.1016/j.patrec.2015.12.013.

Jasuja, O.P., Bumbrah, G.S. and Sharma, R.M. (2016) 'Emerging latent fingerprint technologies: a review', *Research and Reports in Forensic Medical Science*, August, Vol. 6, pp.39–50, DOI: 10.2147/rrfms.s94192.

Karima, D., Victor, T. and Faycal, R. (2014) 'An improved electronic voting machine using a microcontroller and a smart card', *2014 9th International Design and Test Symposium (IDT)*, DOI: 10.1109/idt.2014.7038617.

Newman, R. (2010) *Security and Access Control Using Biometric Technologies: Application, Technology, and Management*, Course Technology, Boston, MA.

Paul, D. (2013) 'A preview on microcontroller based electronic voting machine', *International Journal of Information and Electronics Engineering*, March, Vol. 3, No. 2, pp.185–190, DOI: 10.7763/ijiee.2013.v3.295.

Shrivastava, V. and Shrivastava, V. (2016) 'An analysis of electronic voting machine for its effectiveness', *International Journal of Computing Experiments (IJCE)*, Vol. 1, No. 1, pp.8–14.

The Electronic Voting Machine History (n.d.) (2016) [online] http://english.tse.jus.br/electronic-voting/the-electronic-ballot-box-history (accessed 13 December 2016).

Weldemariam, K., Kemmerer, R.A. and Villafiorita, A. (2011) 'Formal analysis of an electronic voting system: an experience report', *Journal of Systems and Software*, Vol. 84, No. 10, pp.1618–1637, DOI: 10.1016/j.jss.2011.03.032.