Some Security Aspects of Batteries and Power Electronic Converters in a Microgrid

Matić, Luka; Draženović, Karla; Šunde, Viktor; Ban, Željko

https://doi.org/10.1109/ACCESS.2023.3327164

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 August 2023, accepted 19 October 2023, date of publication 23 October 2023, date of current version 6 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3327164

RESEARCH ARTICLE

Some Security Aspects of Batteries and Power Electronic Converters in a Microgrid

LUKA MATIĆ, KARLA DRAŽENOVIĆ, (Graduate Student Member, IEEE), VIKTOR ŠUNDE, (Member, IEEE), AND ŽELJKO BAN, (Member, IEEE)
Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia

Corresponding author: Luka Matić (luka.matic@fer.hr)

This work was supported by the ‘‘Development of an Advanced Electric Bicycles Charging Station for a Smart City’’ Project through the European Structural and Investment Funds under the Operational Program under Grant KK.01.1.1.07.0066.

ABSTRACT The motivation to write this paper is a need to contribute to research of methods of defence against intentional attacks on components of hybrid power systems (microgrids) based on renewable energy sources and storage systems. Spatially distributed electrical energy sources and energy storage devices are gradually being developed and installed, but the security protection of microgrids or individual components of a microgrid is not being improved accordingly. A good example is a fleet of EVs in an urban environment connected to a microgrid with low level of security measures in place (or sometimes none). The term security refers to protection against intentional attacks, not protection against accidents and malfunctions (safety). Lithium batteries, as potentially the most dangerous devices in a microgrid system, i.e. the most likely targets of intentional attacks, can be protected by adequate protection of their power converters and BMSs. This paper presents some of the possible intentional attacks on a battery energy storage system in a microgrid, as well as proposed improvements to the protection of communication channels, power converters' process data logging, and physical protection of battery energy storage systems.

INDEX TERMS Data integrity, distribution of cryptographic keys, lithium battery, magnetic tape, microgrid, physical protection, power converter, random numbers, secrecy of communications, security.

NOMENCLATURE

Abbreviations

AES	Advanced Encryption Standard.
BMS	Battery Management System.
DIN	Deutsches Institut für Normung.
DSP	Digital Signal Processing.
EV	Electric Vehicle.
FSK	Frequency-Shift Keying.
HDD	Hard Disk Drive.
HF	High Frequency.
IF	Intermediate Frequency.
LNA	Low-Noise Amplifier.
LNB	Low-Noise Block (LNA + IF downconverter).
LO	Local Oscillator.
MCU	MicroController Unit.
MPEG	Moving Picture Experts Group.
MPEG	*TS* MPEG - Transport Stream.
NIST	National Institute of Standards and Technology.
OTP	One-time Pad (Vernam's cipher).
POF	Plastic Optical Fibre.
PRNG	Pseudo-Random Numbers Generator.
RFID	Radio-Frequency IDentification.
RSA	Rivest-Shamir-Adleman.
SHA	Secure Hash Algorithm.
SSD	Solid State Drive.
TEMPEST	Eavesdropping on residually generated radiated signals (not actually an abbreviation).
TRNG	True-Random Numbers Generator.
VCO	Voltage-Controlled Oscillator.
W&F	Wow & Flutter.

The associate editor coordinating the review of this manuscript and approving it for publication was Christian Esposito.

Variables

Δd	Cross-sectional deformation of a pin.
Δl	Longitudinal deformation of a pin.
λ	Laser light wavelength.
ν	Poisson's ratio.
ω_1	Angular frequency of analogue signal input to tape head.
ω_2	Angular frequency of W& F speed variation during recording.
ω_3	Angular frequency of W&F speed variation at play- back.
ρ	Density of alloy.
A	Amplitude of analogue signal input to tape head.
a	Amplitude of W&F tape speed variation during recording.
B	Channel bandwidth.
b	Amplitude of W&F tape speed variation at playback.
C	Data transfer capacity of an information channel.
d	Key pin diameter.
E	Young's modulus.
e	Induced voltage at tape head.
f	Frequency of key pin vibration.
f_1	Frequency of analogue signal input to tape head.
f_2	Frequency of W&F speed variation during recording.
f_3	Frequency of W&F speed variation at playback.
g	Acceleration of gravity.
h	Pin drop height.
K	Induced voltage factor at playback.
K	Stiffness constant of a pin.
k	Magnetic flux factor during recording.
l	Key pin length.
m	Pin mass.
n	Index of a TV channel, master key or a tape block.
p	Mean playback speed to mean recording speed ratio.
S/N	Signal-to-noise power ratio.
S	Cross-sectional area of a pin.
s	Analogue signal input to tape head.
t	Time.
v	Velocity of a pin in a free fall.
v_0	Mean value of a tape speed during recording.
v_1	Mean value of a tape speed at playback.
v_{playback}	Tape speed at playback.
v_{record}	Tape speed during recording.

I. INTRODUCTION

Unlike traditional power grids, microgrids contain large numbers of spatially distributed batteries. They are located in residential buildings, energy storage systems in microgrids, in cars (e.g. fleets of taxis with bidirectional flow of electricity) and other places.

Lithium batteries, unlike their lead-acid counterparts, contain combustibles and oxidants (oxygen-rich volatile chemicals). If one cell catches fire, the fire will progressively spread throughout the entire battery. Lithium batteries can burn at temperatures exceeding 2000 °C and thus any such fire is unable to be extinguished by suffocating the oxygen supply because the battery cells contain oxidants that support combustion much better than atmospheric oxygen. Due to high temperatures, they cannot be extinguished by cooling either. Even if cooling is temporarily successful, the short circuit current continues to flow within the battery cell due to the deformation of electrodes, so the excessive heat will reignite the fire. This not only generates temperatures high enough to break the steel beams of a residential building structure, but also quickly releases large quantities of toxic gases that may pose an additional danger in an enclosed space.

A lithium battery as an energy storage device is even more dangerous than a petrol (petrol burns at lower temperatures and requires atmospheric oxygen) or hydrogen tank (hydrogen is dangerous when mixed with pure oxygen, and it is much lighter than air, so it is difficult to form an explosive mixture). Consequently, lithium batteries are the most dangerous components of the microgrid system, i.e. the most likely targets of intentional attacks aimed at destroying the microgrid. For this reason, the security of lithium batteries and their associated subsystems is critical.

The term "security" (German *Sicherheit*, or Russian безопасность) is not precisely defined in many languages and is often confused with "safety", which can be defined as protection against accidental failure (overvoltage or overcurrent) or with reliability of device operation. For this reason, it should be emphasised that the topic of this paper is security protection against intentional attacks, not protection against accidental failures (safety). Although the fields of security and safety partially overlap, research of safety is a separate branch, where different principles apply.

Safety research usually follows technological advancement better than security research. Safety of power converters is considered the most critical in solar power plants [1] and wind power plants [2]. The most sensitive components of power converters are semiconductor switches, which account for 30% to 40% of total failures. They are followed by capacitors at 30% and gate drivers with a slightly lower rate of failure [3]. If the health status of individual components can be estimated in real time [4], failures can be avoided by replacing components on a preventative basis, on a regular maintenance schedule. Online health-condition monitoring methods are being researched extensively [2], [5], [6], [7], both at a level of individual electronic components, and power converters.

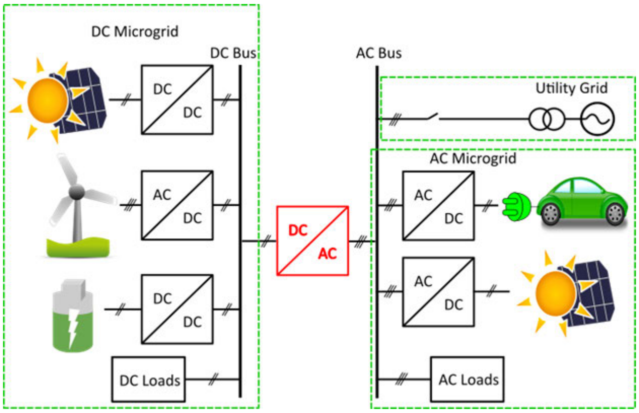

FIGURE 1. An example of a microgrid.

This paper addresses three critical aspects of security protection: (i) crypto-protection of communications, (ii) protection of the integrity of recorded process data; and (iii) physical access security. These three aspects have been selected as the most important, although there are many other security aspects, e.g. defence against hardware trojans, secure data zeroisation (deletion without any possibility of recovery), defence against TEMPEST eavesdropping, etc.

Batteries can be attacked remotely or locally. In a remote attack, an attacker can manipulate the limitations of maximum charging and discharging currents, the maximum permissible temperatures, the maximum charging voltage, etc. To accomplish this, the attacker will attack the microcontroller of the networked power converter or the BMS using some of the remote methods described in [8], [9], [10], and [11], such as a buffer-overflow attack. Such an attack can be used to inject a malicious program (code-injection) [9], or rearrange/relink the existing code (code-reuse attack) [10], to remotely activate the microcontroller's bootloader or simply trigger an unwanted reset of the microcontroller [11]. The attacker thus changes the settings or the entire program of the micro-controller, puts the batteries in an unsafe mode of operation, leading to overheating and fire. This type of attack is particularly dangerous in systems connected to a public network [12], such as charging stations for electric vehicles where the control computer is connected to the Internet (via an Ethernet port) and to microcontrollers of power converters (e.g. via a local RS-485 network). The ability to remotely change the microcontroller's firmware (over-the-air firmware update), is particularly bad from a security point of view.

The most prominent recent example of defeating multiple hardware and software security protections, both on PC computers and embedded equipment was a terrorist attack by the STUXNET worm on a uranium enrichment plant in Iran, which is still being researched. For example, a model of its improved variant [13] was made recently, for attack on autonomous vehicles. Another comparable example was the attack on the Ukrainian power grid by BlackEnergy-3 malware in 2015.

TEMPEST eavesdropping is a type of special attack emanating from the residual electromagnetic radiations given off by all electronic devices. For example, CPU electric power consumption varies depending on the tasks performed and variables processed. Listening to radiated signals and processing the data may reveal the variables being processed, e.g. cryptographic keys. Recent advances are "Powerhammer" [14], a method to exfiltrate the data from an air-gapped (not connected to any network) computer by intentionally manipulating its CPU load, and an "Acoustic Cryptanalysis" attack [15] to steal crypto keys (also from an air-gapped computer) using only audible-range sound signals recorded by a plain digital audio recorder.

The basic principles of security engineering [16], [17], [18], [19] are that security is a chain as strong as its weakest link, and that complexity is its main enemy. This is why it is difficult to design a secure system using only highly-integrated, hi-tech digital electronic solutions. Complex digital ICs (e.g. FPGA) are difficult to secure (e.g. against planting hardware Trojans), and such designs open up too many attack points in a single spot. This is why security features and tasks are better distributed among several low-tech devices. Additionally, analogue circuits should be researched, along with mechanical protections, like locks and keys [20]. Book [17] deals with practical design of simple encryption devices. An approach to design a secure system as a complete unit [19], considering all the aforementioned aspects, is much better than retrofitting an insecurely designed system with secure features.

With all this in mind, let's start from encryption. One protection against remote attacks is encryption of network communications with BMSs and power converters for charging and discharging batteries. Generating high-quality random numbers [21] is the basis of any reliable crypto-protection. Cryptographic keys are generated from them. The keys must then be distributed to the network nodes. This protection measure is discussed in the second chapter of this paper, where a new method of both generating and distributing cryptographic keys through insecure public channels is proposed. Already known is the quantum key exchange method [22], based on a single photon polarisation detector, a public negotiation through a public channel after receiving weak and noisy radio signals from a satellite [23], and so-called Rip van Winkle cipher [24] based on crypto key generation from an "infinite" public source.

In the event of an incident or attack, reliable recording of the power converter's process variables and communications (process data logging) is a measure that does not prevent the attack, but is essential to determine whether it was intentional or just a malfunction. If it was a deliberate attack, the recorded data, i.e. the forensic traces left by the attacker, can be later examined. It is important to use a data logger with a reliable data integrity protection mechanism to ensure that the recorded data hasn't been tampered with after the incident. High-quality recording devices (so-called "black boxes") for conversations (cockpit-voice recorders) and slow process variables (flight-data recorders) for aircraft and ships already exist. The recording of fast variables of power converters and the preservation of their integrity is yet to be adequately addressed. Existing recorders for this purpose are usually ordinary PCs with very poor data integrity protection measures. The problems of integrity are dealt with in the third chapter of this paper. Magnetic tape, as a sequential access medium, is much superior for ensuring data integrity protection. An analogue tape recorder will be used for handling digital signatures instead of a digital tape recorder. May seem quite unusual, but the reason is very simple - digital tape drives are expensive. Furthermore, there are many proprietary digital tape drives and formats. On the other hand, analogue tape recorders and tapes are well standardised, cheap, and easily obtainable. The problems associated with analogue tape recorders, precisely described long ago [25], are still being researched and solved [26], [27], [28], although the technology itself is now more than a century old. It is important to stress that magnetic tape technology (especially digital) is far from obsolete, since it is still being researched and improved [29], reaching very high data storage densities.

In addition to remote attacks, the battery system of energy storage in microgrids should also be protected against local attacks. It makes no sense for an attacker to exploit the vulnerabilities in a BMS software or network firewall if they can break into the battery storage room and physically destroy batteries. Although many methods of physically securing the premises are known and available today, this security protection still depends largely on standard mechanical locks and keys [30]. In the fourth chapter of this paper, a new scenario of a physical attack on locks is presented and a method of defence is proposed. Mechanical locks and keys [20] are also far from obsolete and have not yet been replaced by advanced electronic RFID locks [31]. Attacks by duplicating a key from a photo snapshot [32], [33], [34], using 3D models enhanced by neural networks have been devised. Other methods under research [35], [36] use audible audio and video recording of a legitimate user's key while being inserted in a lock. In this paper, an improved method of attack using ultrasound is proposed, along with a defence against it.

To summarise, here is a list of the contributions contained within this paper:

1.) A new method for generating cryptographic keys (an advanced method based on principles of Vernam's one-time pads and Rip van Winkle's cipher) through one-way public channels (satellite TV) for crypto-protection of communications through insecure public networks (e.g. the Internet), e.g., between a main base station and EV charging point at a remote location.

2.)A tamper-resistant method for the protection of integrity of logged process data (e.g. from a DC/DC converter and batteries), using digital signatures in a daisy-chained data structure recorded on a magnetic tape. This way, the logged data can be considered reliable for forensic analysis after any incident.

3.) A method of attacking a mechanical lock (e.g., one protecting the secured perimeter around battery storage units and DC/DC converters), using a specially designed passive sonar (also a part of our research) to measure key pins lengths, and a method of defence against it, i.e., a method of calculating key pins dimensions and alloy composition, for a specially designed lock resistant to this type of attack.

II. AN IMPROVED METHOD FOR GENERATION AND DISTRIBUTION OF CRYPTOGRAPHIC KEYS FROM A PUBLIC SOURCE

High-quality random numbers are a basic requirement for secure communication. Keys for symmetric (e.g. AES) or asymmetric (e.g., RSA) encryption methods are generated from random numbers. If large quantities of random numbers can be generated and, above all, securely distributed to users, then the one-time pad (OTP) or the Vernam cipher can also be used as the only proven unbreakable encryption method.

True random numbers can be generated in various ways - for example, from electronic noise [37] and/or the Lorenz chaos generator [38] or small fluctuations of periods (clock jitter) of two oscillators [39]. Cryptographic keys are then calculated from these, which can also be used for the periodic reinitialisation of software pseudo-random number generators (PRNG). Such keys must be distributed to the users, which can be a problem.

One idea for how to generate cryptographic keys for symmetric cryptosystems such as AES and OTP is to process and combine radio signals from TV satellites (a public source) to generate number sequences with properties of randomness. Generation of crypto keys from a public source, a quantum crypto method, using photon-polarisation detection with four orthogonal states was simulated in [22]. In [23], a noisy public channel is used (e.g. a weak RF signal from a satellite or from an extraterrestrial radio source like a quasar), using a negotiation method similar to [22], to beat an eavesdropper, even one with superior receiver, antenna and preamplifier (with much better overall signal-to-noise ratio).

In this paper, a new method is proposed, based on Rip van Winkle's cipher [24]. This cipher, unlike [23], works by generating keys from an easily legible (high S/N ratio) "infinite" public source. Time delay T_d is the crypto key. Both stations record the bytes from the public source, and take those received e.g., exactly T_d = 1 month, 12 days, 4 hours, 15 minutes, 25 seconds and 145 milliseconds earlier, and use them as OTP keys. They will thus generate usable OTP keys and hence be able to secretly communicate. They only need a limited amount of buffer memory for this to work. On the other hand, an eavesdropper trying to crack this code needs much computing power, and much more memory to be able to crack their encryption. This is why the above-mentioned public source, the quasi-random bytes generator, must be "infinite".

At the time when Rip van Winkle's cipher was proposed, there wasn't any practical public source with properties of "infinity" available. Nowadays it's easy to receive

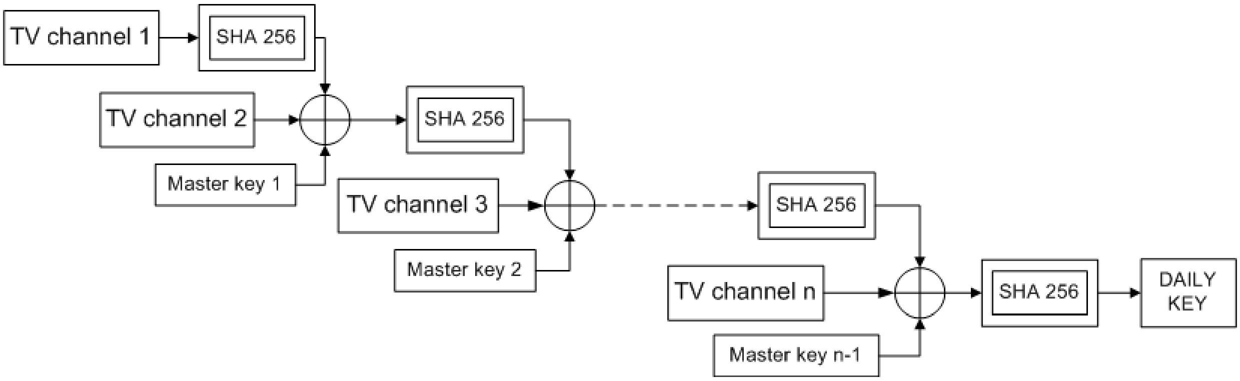

FIGURE 2. Daily crypto-key generator chart.

10000 digital satellite TV channels at a single location on Earth, each ticking at 1 Mb/s. A potential eavesdropper, would need a buffer memory storage space of almost 40000 TB to keep all the possible keys generated with a delay of up to one year, to stand any chance to crack the code, which is not very practical. On the other hand, both stations (because they need to listen to only one satellite) would need only 4 TB/year. A further improvement to this method is now proposed, to make it more practical for stations to generate strong crypto keys every day (e.g. for AES or OTP). They will need memory storage space of only a few MB, and the encryption will still be very difficult to crack. A method to improve the quality of randomness of received sequences will also be presented.

TV satellites (Astra, Hotbird, Eutelsat, etc.) broadcast signals to receivers on Earth, and this communication only goes in one direction. In this way, a potential attacker (a passive eavesdropper) cannot know from which TV channels and at what time the signals are received. The LNB receiver on the satellite dish receives the entire frequency range of approx. 1 GHz (from 10.7- 11.7 GHz or 11.7-12.7 GHz), which it amplifies by approx. 60 dB and downconverts it into the intermediate range (IF) of 950-2150 MHz by mixing these frequencies with the local oscillator of the LNB (LO) at 9.75-10.55 GHz. Frequencies up to 2.5 GHz are suitable for transmission through the coaxial cable from the LNB to the digital satellite receiver inside the building without any significant loss in the cable. LO operates at a constant frequency and the entire intermediate frequency range (1 GHz wide) passes through the cable, conveying up to 500 TV channels simultaneously. Therefore, eavesdropping on residual signals from the LNB receiver (the so-called TEMPEST attack) does not provide the potential attacker with any useful information. Channel selection is done on a digital receiver inside the building. This receiver is much easier to protect with shielding, to attenuate its residual radiation.

Well-compressed and/or encrypted data streams possess the necessary properties of randomness, which can be checked with the tests described in [40]. These are rigorous tests that show whether the sequences tested are suitable for use in cryptography, where the criteria are the strictest. In addition to the American NIST, the quality of random number sequences is also defined by other governmental bodies for standards and norms, e.g. the German DIN or the Russian ГОСТ [41], as well as gambling games committees, such as the American *"Nevada Gaming Commission"*. NIST prescribes 15 strict tests so that the quality of randomness can be measured and quantified. In the diploma thesis [42], the examination of output strings (encrypted texts) of various cryptographic functions was carried out - if they pass the tests of NIST, they can be considered good.

The main idea is to start from compressed (and encrypted - in the case of scrambled TV channels) MPEG-TS byte sequences (MPEG-TS is a variant of MPEG-2 for continuous transmission - streaming data over low reliability channels, enhanced with error correction codes) at the output of the demodulator of the digital satellite receiver. Cryptographic keys are then calculated from these sequences. The condition is that both stations can receive the signal of the same TV channel from the same satellite and that they are well synchronised. One possible procedure for calculating the daily keys is shown in Fig. 2.

SHA-256 is a non-linear cryptographic one-way hash function. Its inverse is very difficult to compute and changing one bit on the input results in an unpredictable change in the output bytes. For this reason, the SHA function also improves the quality of random sequences - this is called "whitening". If *n* TV channels are used, *n-1* fixed master keys should be set in advance for both channels. Every master key *n* is XOR-ed with the bitstream of TV channel *n+1* and SHA-256 output of the previous stage.

A commercial TV satellite (e.g. Astra 19-2) relays more than 1000 TV channels. Most of them are encrypted/ scrambled, which is good, because such bitstreams have even better randomness properties (as shown in [42]), and the bitstreams do not need to be decrypted at all to be used for key generation. Even a cheap satellite antenna with fixed azimuth and elevation and multiple LNB circuits can receive up to 10000 TV channels. If, for example, 100 of the 10000 available channels are selected and the start of recording of each of the 100 substreams is synchronised to one full second in a day, the total number of combinations to recover each daily key is then $(86400 \cdot 10000)^{100} = 2^{2968}$, i.e. 2968 bits. By comparison, 256-bit AES is considered resistant to a brute-force attack by a quantum computer by today's standards. The entropy of the master keys is not taken into account here, and furthermore, the synchronisation does not have to be on a full second. If the 2968-bit entropy of the key (daily!) is not sufficient, it can easily be increased. In addition to TV, there are many other satellites orbiting the Earth. Their signals must be received and demodulated - decryption is not required. It is necessary to precisely define the optimal protocol for generating daily keys and to solve the synchronisation of two stations, as well as quick testing of quality of the received bitstreams, using NIST tests.

The system used for testing this procedure was a commercial TV SAT receiver (set-top box) "*Amiko Mira-3*" connected to a small 60 cm satellite dish (through one standard 12 GHz LNB receiver/downconverter) pointed to Astra 19-2 TV satellite. Tapping to Q and I bitstream PCB traces on Amiko set-top box between RF QPSK demodulator IC and its main CPU was used to extract raw bitstreams received from Astra satellite before digital processing. Recording a certain TV channel to USB flash memory stick, in raw MPEG-TS format (as transmitted from Astra) was used to extract video packets from TS stream and compare the results. Received bitstreams were processed in MATLAB on a PC computer, according to chart in Fig. 2. NIST tests were then performed, also in MATLAB. This entire procedure needs to be fully automated, and implemented on a small embedded system, to be used in real-time online operation.

III. A TAMPER-RESISTANT METHOD FOR PROTECTION OF INTEGRITY OF LOGGED PROCESS DATA

In practice, recorders for slow signals are already well developed, e.g. flight-data recorders and cockpit-voice recorders for aircraft and ships. Most industrial process recorders are ordinary PCs where recorded data is relatively easy to manipulate. Their integrity is therefore weak. Reliable recorders have hardly been researched in scientific papers. Some of the problems of data integrity in process recorders are partially addressed in [43], [44], and [45].

The system and method to be presented are also applicable for recording fast process variables, e.g., in DC/DC power converters. Integrity is ensured by means of a daisy-chained data structure with OTP encryption and recording of digital signatures on a sequential access medium, such as a magnetic tape. This way, any tampering with recorded data becomes difficult. As already mentioned, an analogue tape recorder is used, because analogue tape recorders and tapes are well standardised, cheap, and easily obtainable. Furthermore, since the tape will only be handling digital signatures, the data transfer rate required is low (e.g., 1200 bps), which can be easily handled by an analogue audio tape recorder.

An ordinary PC and a tape recorder are connected. After each data block (e.g. 10 MB), the PC generates a hash (e.g. SHA-256) of this block and saves it on its HDD. This hash is then forwarded to the tape recorder in the secure box via a wired one-way data link. A simple 8-bit MCU (in the secure, tamper-resistant box, along with the tape recorder) computes digital signature of block *n* from:

- signature of previous block *(n-1)* stored on tape,
- OTP key for block *(n)* stored on tape, and
- hash of block *(n)* received from the PC.

This results in a chained data structure that is difficult to manipulate (on Fig. 3). The data on the PC can be tampered with, but if any 10 MB blocks of data stored on the HDD doesn't have a correct signature on the magnetic tape, or if the box has registered an unauthorised opening, the data saved on the PC is considered invalid.

The tape can only operate in one direction (forward), which is ensured by the mechanical assembly of the tape recorder. It is not possible to rewind it and change the recording on the tape by a command injected via data link (e.g. by a buffer-overflow attack). The tape recorder does not have an erase head, but two read/write heads constantly pressed on the tape. After head G1 has read the OTP key for block (*n*), the MCU calculates its digital signature and writes it to the tape via head G1.

During that time, the G2 head zeroises the OTP key not by classical erasure, but by masking i.e., by writing white noise with an amplitude 10 times higher than that of the signal used to record the OTP key, up to the saturation limit of the magnetic material of the tape. This way, it is essentially "encrypted" with an OTP code, which is more secure than the classical erasure with a high-frequency signal (HF-bias). Cheap tape recorders work with a min/max signal span of 50 dB, and this only requires a span of 20 dB.

A series of OTP-key blocks are written to the tape before the device is installed in the facility, and a copy is kept in a secure location for later verification. Each OTP key is erased (masked by noise) after it is used, so it is not feasible to properly sign a subsequently changed block with the same key, even if it is possible to open the box and rewind the tape.

Inevitable tape speed fluctuations, known as *wow&flutter* (W&F), cause changes in the frequency of the recorded FSK signal, confusing the FSK modem, which converts pulsations of different frequencies into a series of ones and zeros. The term *wow* refers to slow speed fluctuations, while *flutter* refers to fast ones with a frequency up to several kHz. Wow is mainly caused by elasticity, gaps, inertia and other imperfections in the mechanical components of the tape recorder (gears, friction wheels, rubber belts and pulleys). Flutter is caused by higher frequencies, e.g. vibrations of mechanical components, and by tautness of magnetic tape segments.

The mechanisms behind W&F have already been described in detail (e.g. [25]), but the compensation methods are not

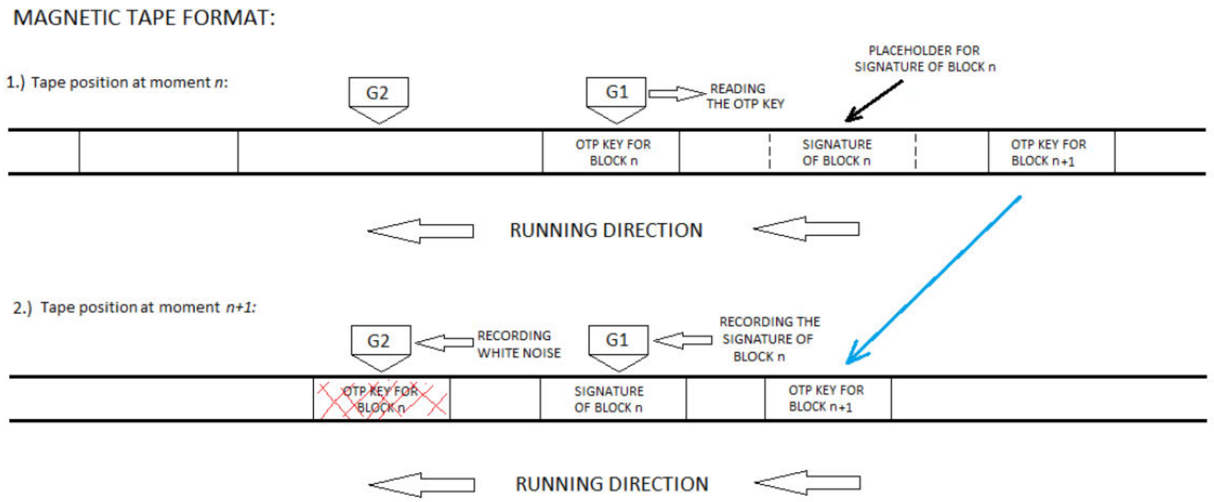

FIGURE 3. Magnetic tape format for recording of digital signatures.

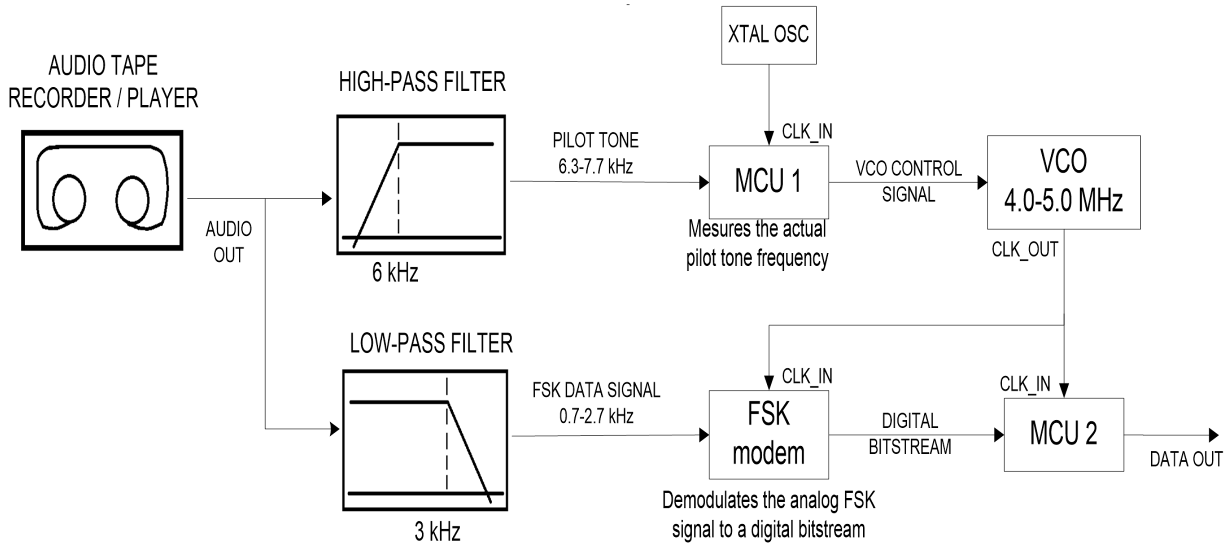

FIGURE 4. Block-diagram of wow-flutter compensation by continuously adjusting the CPU-clock frequency.

well developed for all applications. Useful analogue signal $s(t) = A\sin(\omega_1 t)$ is recorded on the tape. The tape, which should run at an average speed v_0, has W&F speed variations of amplitude a (about 5% for low-quality tape recorders) and frequency f_2, so the tape speed is (1):

$$v_{\text{record}} = v_0 \cdot (1 + a\sin(\omega_2 t)). \tag{1}$$

The magnetic flux recorded on the tape will then be (2):

$$\Phi(t) = kA \cdot \sin\left(\omega_1\left(t - \frac{a}{\omega_2}\cos(\omega_2 t)\right)\right) \tag{2}$$

When played back at the mean velocity $v_1 = p \cdot v_0$, variation of amplitude b and frequency f_3, tape velocity is:

$$v_{\text{playback}} = v_1 \cdot (1 + b\sin(\omega_3 t)), \tag{3}$$

and the magnetic flux at the tape read head will be:

$$\Phi(t) = kA \cdot \sin\left(p\omega_1\left(t - \frac{a}{p\omega_2}\cos(p\omega_2 t) + \frac{b}{\omega_3}\cos(\omega_3 t)\right)\right) \tag{4}$$

Finally, the voltage induced on the magnetic tape read head during playback can be described by (5):

$$\begin{aligned} e(t) = K\frac{d\Phi(t)}{dt} &= KAp\omega_1 . \\ &\cdot \cos\left(p\omega_1\left(t - \frac{a}{p\omega_2}\cos(p\omega_2 t) + \frac{b}{\omega_3}\cos(\omega_3 t)\right)\right) \\ &\cdot (1 + a\sin(p\omega_2 t) - b\sin(\omega_3 t)) \end{aligned} \tag{5}$$

The upper part of (5) describes a certain frequency modulation of the original signal with frequencies pf_2 and f_3, and it can be seen (in the bottom line) that there is also some amplitude modulation (which is not a serious problem for the FSK modem).

It is necessary to work out a reliable method of compensating for W&F speed variations so that the system can be used in practice. One possible approach to this problem is to use a pre-recorded *"pilot tone"* with a frequency of about 7 kHz. In essence, the method boils down to continuous adjustment (in real time) of the varying-frequency CPU-clock signal for the FSK modem and the MCU-2 reading the data from the tape, based on the actual measured pilot-tone frequency.

The clock signal for the MCU-2 and the FSK modem comes from the VCO oscillator and is controlled depending on the current pilot-tone period measured according to a specific algorithm (Fig. 4). The output variable is electrical, not mechanical, and therefore, fast regulation is possible. Articles [26], [27], [28] describe methods suitable for the restoration of analogue audio recordings, using residually recorded signals of mains hum or HF tape bias pre-magnetisation signals as pilot tones.

Measurements of the pilot-tone frequencies and the responses of the W&F compensation system during playback can be used to confirm the effectiveness of this method. It is also possible to develop a W&F compensation method by measuring only part of the pilot-tone period. A similar principle is used by many FSK modems and additional improvements are also possible.

The system used for testing and measurements here was a commercial compact cassette player/recorder (tape speed 4.75 cm/s) and also one microcassette dictaphone (tested at tape speeds 2.4 cm/s and 1.2 cm/s). Analogue filters were implemented using LM324 operational amplifiers, FSK modem IC was TCM3105, and the two MCUs were Atmel ATMEGA8. The sensitivity analysis will be performed when the W&F compensation algorithm is fully implemented.

IV. ATTACK ON MECHANICAL LOCKS WITH AN ULTRASONIC PASSIVE SONAR AND A METHOD OF DEFENCE

Physical access control still heavily relies on mechanical locks [20], [30]. Electronic locks (e.g. with an RFID reader) have not yet replaced mechanical locks [31]. The most common type of lock is still a *pin-tumbler lock* in Fig. 5, or its variants, including a *dimple lock*, and also a *tubular lock* [20].

New ways to attack mechanical locks are emerging, such as copying a key based on a photo or a 3D model of the key [32], [33]. These methods are being improved using neural networks [34], to improve the reading of key dimensions from photographs taken at any angle and under any lighting conditions. Making a key to match a lock (without an original key) is a slow and expensive process [30]. Existing devices for mechanically reading pin lengths, such as the "Sputnik" in Fig. 6 described in [30], are expensive, cumbersome and slow. Is it possible to build an electronic device for the quick reading of pin lengths without opening and disassembling a lock, so that a key can be precisely cut later?

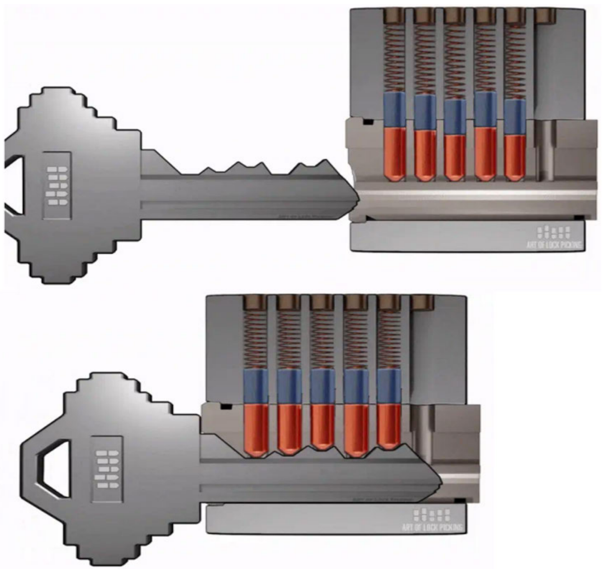

FIGURE 5. A standard pin-tumbler lock and key.

The red pins of the lock in Fig. 5 (the so-called *key pins*, as opposed to the blue ones, the *driver pins*) are of different lengths, and the depths of the notches in the key must be cut according to their lengths in order to open the lock. In article [35] an attack method is presented in which the depths of the notches in the key are calculated from the audio recording of the pins clicking in contact with the key when the key is inserted and withdrawn from the lock. The sound is recorded in the audible range (up to 20 kHz). The article [36] presents an enhanced method, an improvement of [35], which improves the synchronisation of key displacement and clicking sounds by video recording.

In this paper, an improved and more practical method compared to [35] and [36] is proposed, followed by a protection against this new method. In the proposed method, the rightful owner of the key does not need to be shadowed by a potential attacker, who does not need to stand near the lock for more than one minute.

The dimensions and material from which the lock pins are made determine the frequency of their vibration after excitation by a sharp, step impact. It is possible to design a device and develop a method for measuring the ultrasonic vibrations of pins so that the lengths of the pins can be calculated from the ultrasonic frequency. For a thin rod (whose length is much greater than its diameter), its natural frequency can be approximated as follows:

$$f = \frac{1}{2l}\sqrt{\frac{E}{\rho}}, \tag{6}$$

where l is rod length, E is Young's modulus and ρ is density.

The resonant frequency of one standard brass pin, assuming a thin rod approximation (e.g. $E = 120$ GPa,

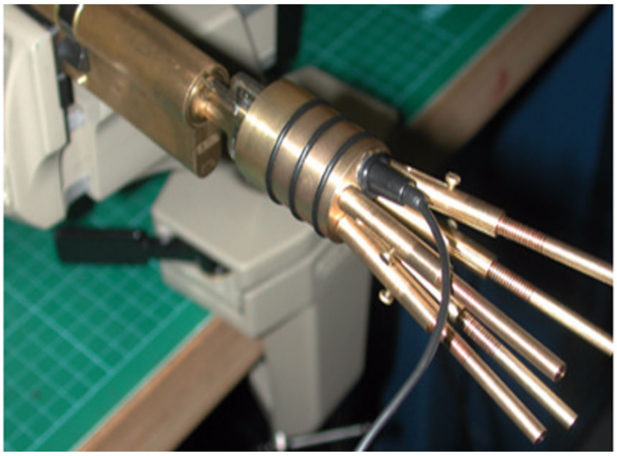

FIGURE 6. "Sputnik", a mechanical tool for reading lengths of key pins.

$\rho = 8530$ kg/m^3, $l = 7$ mm, $d = 2.5$ mm) is $f = 268$ kHz. The experimentally measured value was close to 300 kHz.

An electronic device with a laser optical microphone (Fig. 7) and plastic optical fibre (POF cable, with a diameter d=1 mm) can measure the frequency of the vibrations of each pin, if the plastic optical fibre can be inserted into the lock, close to the pin. This is possible with most of these locks. The next step is to develop a more precise mathematical model for the vibrations of a short cylinder with a conical tip, so that the measured frequency can be more accurately related to the dimensions of the pin. The frequency will depend not only on its length, but also on its diameter and dimensions of the conical tip.

One possible defence against this kind of attack is to design a lock with pins of different diameters and lengths, all having approximately the same resonant frequency. It is possible to devise a method of iterative optimisation, e.g. a method for calculating the diameter and dimensions of the taper from a defined resonance frequency, length and Young's modulus.

Another possible variant is to start from a defined length and a maximum permissible diameter and to determine the Young's modulus and the density as a result. Further improvement is a method for calculating pins with varying density and Young's modulus along the longitudinal axis. Such a pin will not have a single resonance frequency that could reveal its length.

Even with an inferior ultrasonic microphone with a diameter of 10 mm, it is possible to measure ultrasonic signals emanating from pins. The velocity and hence the kinetic energy of a pin in free fall, falling from a height of 10 cm onto a hard surface in front of this microphone, corresponds approximately to the kinetic energy accumulated after the driver pin spring has been tensioned and abruptly released inside the lock. This can be achieved easily and quickly with any lock picking tool (e.g. a pick or a rake) or even with a blank (uncut) key. The decay of the ultrasonic pulse takes approximately 3-5 ms and the frequencies of the tested pins are measured in the range between 150 kHz and 420 kHz, depending on the pin dimensions and material (brass or stainless steel). The feasibility of this procedure can be verified with the help of the Shannon-Hartley theorem (7):

$$C = B \cdot \log_2 \left(1 + \frac{S}{N}\right) \tag{7}$$

The data transfer capacity of a noisy information channel, i.e. the theoretical amount of bits per second C [bit/s] that can be transferred over the channel, depends on the analogue frequency bandwidth of the channel B [Hz] and the ratio of signal power to noise power *S/N*. The bandwidth of the optoelectronic preamplifier of the laser microphone and its subsequent amplifier stages is $B = 500$ kHz. The pins are usually produced in 10 discrete lengths (depending on the manufacturer and the quality of the lock). This is less than 4 bits of useful information transmitted in the 3-5 ms of the ultrasonic pulse emitted by the vibrating pin. As an additional margin, it can be assumed that 8 bits of useful information are needed to be transmitted during only 2 milliseconds of pin ringout. This means that a channel capacity of C =8 bits/2 ms = 4 kbit/s is required. Assuming a very poor ratio *S/N* = 1/30 - noise power 30 times higher than the power of the useful signal - the capacity C is (8):

$$C = 500 \cdot 10^3 \cdot \log_2(1 + 1/30) = 24\text{kbit/s} \tag{8}$$

which is much more than the 4 kbit/s minimum requirement. A brass pin with a diameter $d = 2$ mm and a length $l = 5$ mm will have a mass (9):

$$m = d^2\pi/4 \cdot l \cdot \rho = 0.13 \text{ g}. \tag{9}$$

When dropped from a height of $h = 10$ cm it will reach the velocity (10):

$$v = \sqrt{2gh} = 1.4 \text{ m/s}. \tag{10}$$

The stiffness constant of this pin is (11):

$$K = ES/l = 7.54 \cdot 10^7 \text{ N/m}. \tag{11}$$

Therefore, the following initial maximum deformation in the longitudinal direction is to be expected, assuming that the entire kinetic energy of the pin will be converted without losses and accumulated in its initial deformation (12):

$$\Delta l = \text{v} \cdot \sqrt{m/K} = 1840 \text{ nm}. \tag{12}$$

The Poisson's ratio for a standard brass is ν = 0.3, which means the initial cross-sectional deformation will be (13):

$$\Delta d = \nu d \Delta l/l = 216 \text{ nm}. \tag{13}$$

For example, if a red laser with a wavelength of λ = 660 nm is used, this means that in addition to a modulated intensity of the light reflected from the vibrating pin, there is also a significant phase shift after reflection. If the optical splitter allows some of the incident light to pass through to the phototransistor in addition to the reflected light, there will be varying interference that amplifies the ultrasonic frequency signal at the phototransistor. This is important because the

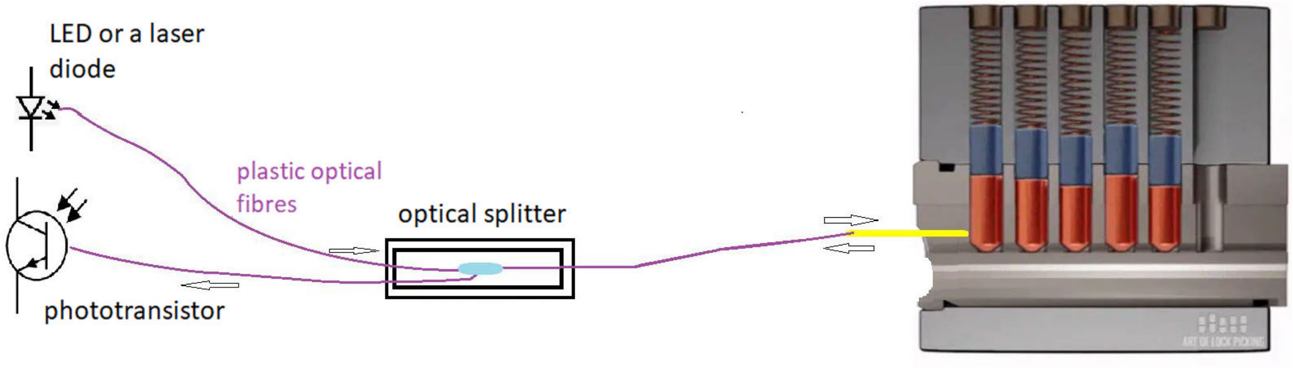

FIGURE 7. A laser microphone can detect ultrasonic vibrations of pins inside a lock.

useful signal at the phototransistor will be weak, so various methods of analogue and digital signal processing must be used to accurately measure the ultrasonic frequency of the pin vibration. This method of attack on a mechanical lock is possible to perform, under a condition that all the practical problems regarding analogue and digital signal processing are properly addressed and solved.

V. CONCLUSION

The security of microgrid components, particularly with respect to lithium batteries and their associated circuits, is becoming more and more important as an increasing number of new energy storage units are installed each year. In this paper, among the many security aspects that are important for secure operation of lithium batteries and their power converters, three are selected to be addressed. These are the security of communication between microgrid nodes, the integrity of logged process data and physical access control.

Secure communication channels between BMSs, power converters and their control centre are essential for their security against intentional attacks. To make this possible, high-quality random numbers are needed for generating strong cryptographic keys. A method for calculating daily session keys for symmetric cryptosystems is presented, using compressed and/or encrypted bitstreams transmitted by TV satellites. The condition is that both receivers receive a signal from the same satellite and that they can be synchronised. It is shown that by selecting only 100 channels out of the possible 10000 available on an average digital satellite TV receiver, each with a synchronization on one full second (out of 86400 during a day), the total entropy for the generated daily secret key is 2968 bits, and it can be easily increased if necessary. By comparison, symmetric AES encryption with a 256-bit key is considered resistant (by today's standards) to a brute-force attack by a quantum computer.

This research will have to continue to address several problems. First, a device to receive and record byte sequences from TV satellites needs to be designed and assembled. The next challenge is to solve the synchronization between two stations, so they can generate the same crypto keys from received MPEG-TS streams. Then, the embedded system will be programmed to calculate the keys and check the randomness quality online (and to coordinate the entire receiving, calculating and recording procedure), using one of fast NIST tests possible to calculate online in real time, e.g. Maurer's test and the histogram test. Extensive offline testing of the crypto keys generated then must be performed, using all the NIST and other randomness test calculations, to fully confirm the quality of the generated keys, so they can be used for the crypto-protection of sensitive communication.

The integrity of logged process data associated with the operation of a power converter charging/discharging a battery storage is particularly important for process logs that can be used for forensic analysis and ultimately as evidence in a court of law in the event of an intentional attack on a microgrid. A low-cost and simple tamper-resistant method for logging fast power converter variables is presented. The integrity of the logged data is preserved with a daisy-chained data structure of digital signatures on a magnetic tape using a potentially unbreakable OTP code. Analogue magnetic tape was chosen as a cheap and ubiquitous sequential data access medium, which further enhances data integrity along with its mechanical assembly with two read/write heads, no erase head, and no possibility of rewinding, all in a tamper-resistant enclosure. Magnetic tape technology is still being improved, nowadays reaching data storage density measurable in [Gb/cm^2]. To ensure overall reliability, a method of compensating for wow/flutter effects is proposed.

A future challenge in this research is to devise and test an algorithm for fast online control of a VCO CPU clock generator for MCU-2 and FSK modem. After a successful Matlab simulation, the electronic device will be designed and tested in real time operation. Procedures for quick online measurement of pilot tone frequency can also be researched.

Physical access security, although enhanced with electronic technology, still heavily relies on traditional mechanical locks. A new method of attack on a pin-tumbler lock is proposed, where the lengths of pins can be read quickly without the need to shadow a legitimate key owner, as well as possible methods to protect against this type of attack.

The presented method of attacking a mechanical pin tumbler lock opens many further research challenges. A method and a device to quickly capture a short ultrasonic pulse coming from a key pin must be designed. Analogue and digital DSP filters will have to be designed, along with the procedure to record the ultrasonic pulse and quickly process it online on that embedded MCU-DSP system. In order to calculate the parameters of key pins for a lock resistant to this type of attack, a precise mathematical model of a pin will first have to be devised, so an effective optimization method can be implemented.

The three critical security aspects were addressed with three separate devices using digital and analogue electronics, along with mechanical technology, to enhance the overall security. A usual modern-day approach would be to use one single highly integrated digital device. This would open too many attack points on one spot, and such system would be difficult to properly secure, so we decided to take a different approach. On the other hand, using different technologies may lead to additional problems regarding repairs and maintenance, availability of spare parts, and training of service personnel. Magnetic tapes are very reliable for long-term data storage (up to 100 years), but tape drives require more regular maintenance (adjusting and cleaning the tape heads and rotating parts). Tape drives, tapes and spare parts are still being produced and sold at reasonable prices (music entertainment industry is still producing cassette tapes), so servicing the equipment isn't a problem and doesn't require any special training. Installing and servicing mechanical locks resistant to passive sonar attacks also isn't a problem, since they are the same as standard locks, only their key pins are made of different alloys. Any locksmith can replace standard pins with special ones, hence no specialized training is required for installation and maintenance of such locks as well.

REFERENCES

[1] L. M. Moore and H. N. Post, "Five years of operating experience at a large, utility-scale photovoltaic generating plant," *Prog. Photovolt., Res. Appl.*, vol. 16, no. 3, pp. 249–259, May 2008.

[2] B. Rannestad, A. E. Maarbjerg, K. Frederiksen, S. Munk-Nielsen, and K. Gadgaard, "Converter monitoring unit for retrofit of wind power converters," *IEEE Trans. Power Electron.*, vol. 33, no. 5, pp. 4342–4351, May 2018.

[3] S. Yang, D. Xiang, A. Bryant, P. Mawby, L. Ran, and P. Tavner, "Condition monitoring for device reliability in power electronic converters: A review," *IEEE Trans. Power Electron.*, vol. 25, no. 11, pp. 2734–2752, Nov. 2010.

[4] B. Saha, J. R. Celaya, P. F. Wysocki, and K. F. Goebel, "Towards prognostics for electronics components," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, Mar. 2009, pp. 1–7.

[5] B. Rannestad, K. Fischer, P. Nielsen, K. Gadgaard, and S. Munk-Nielsen, "Virtual temperature detection of semiconductors in a megawatt field converter," *IEEE Trans. Ind. Electron.*, vol. 67, no. 2, pp. 1305–1315, Feb. 2020.

[6] S. Tang, J. Wang, R. Zheng, D. Wang, X. Yin, Z. Shuai, and Z. J. Shen, "Detection and identification of power switch failures using discrete Fourier transform for DC–DC flying capacitor buck converters," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4062–4071, Aug. 2021.

[7] S. Zhao, F. Blaabjerg, and H. Wang, "An overview of artificial intelligence applications for power electronics," *IEEE Trans. Power Electron.*, vol. 36, no. 4, pp. 4633–4658, Apr. 2021.

[8] L. Budin, M. Golub, D. Jakobović, and L. Jelenković, *Operacijski sustavi*, Zagreb, Croatia: Element, 2013.

[9] J. Erickson, *Hacking—The Art of Exploitation*. San Francisco, CA, USA: No Starch Press, 2008.

[10] A. De, A. Basu, S. Ghosh, and T. Jaeger, "Hardware assisted buffer protection mechanisms for embedded RISC-V," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4453–4465, Dec. 2020.

[11] L. Matić, *A Handbook on DIY Electronic Security and Espionage*. London, U.K.: Elektor International Media BV, 2021.

[12] A. S. Siddiqui, Y. Gui, J. Plusquellic, and F. Saqib, "Poster: Hardware based security enhanced framework for automotives," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016.

[13] H. Ahn, J. Choi, and Y. H. Kim, "A mathematical modeling of Stuxnet-style autonomous vehicle malware," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 673–683, Jan. 2023.

[14] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "PowerHammer: Exfiltrating data from air-gapped computers through power lines," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1879–1890, 2020.

[15] D. Genkin, A. Shamir, and E. Tromer, "Acoustic cryptanalysis," *J. Cryptol.*, vol. 30, no. 2, pp. 392–443, Apr. 2017.

[16] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ, USA: Wiley, 2000.

[17] B. Schneier and N. Ferguson, *Practical Cryptography*. Hoboken, NJ, USA: Wiley, 2003.

[18] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[19] D. Deogun, D. B. Johnsson, and D. Sawano, *Secure by Design*, 1st ed. Shelter Island, NY, USA: Manning, 2019.

[20] D. Ollam, *Practical Lock Picking: A Physical Penetration Tester's Training Guide*. Waltham, MA, USA: Syngress-Elsevier, 2012.

[21] J. E. Gentle, *Monte Carlo Methods*. New York, NY, USA: Springer-Verlag, 1998.

[22] I. B. Adiyaman and I. Sogukpinar, "Simulation of BB84 quantum key exchange protocol and attack analysis," in *Proc. 5th Int. Conf. Comput. Sci. Eng. (UBMK)*, Diyarbakir, Turkey, Sep. 2020.

[23] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[24] U. M. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher," *J. Cryptol.*, vol. 5, no. 1, pp. 53–66, Jan. 1992.

[25] C. B. Pear, "Flutter in magnetic recording of data," *IRE Trans. Audio*, vol. 9, no. 5, pp. 159–166, Sep/Oct. 1961.

[26] A. Czyzewski and P. Maziewski, "Some techniques for wow effect reduction," in *Proc. IEEE Int. Conf. Image Process.*, 2007, p. 29.

[27] P. Maziewski, "Wow defect reduction based on interpolation techniques," *Bull. Polish Acad. Tech. Sci.*, vol. 54, no. 4, pp. 469–477, 2006.

[28] A. Czyzewski, B. Kostek, and A. Kupryjanow, "Automatic sound restoration system concepts and design," in *Proc. Int. Conf. Signal Process. Multimedia Appl.*, Jul. 2011, pp. 1–5.

[29] J. B. C. Engelen, S. Furrer, H. E. Rothuizen, and M. A. Lantz, "Where tape and hard-disk technology meet: The HDD head-tape interface," *IEEE Trans. Magn.*, vol. 51, no. 7, pp. 1–10, Jul. 2015.

[30] M. W. Tobias, *Locks, Safes and Security, an International Reference*, Springfield, IL, USA: Charles C Thomas, 2002.

[31] D. Jakub and L. Filip, "Comparison of the difficulty overcoming of RFID electronic access control systems and overcoming of pin tumbler locks," *Transp. Res. Proc.*, vol. 55, pp. 1620–1626, Jan. 2021.

[32] J. Straub, "Comparison of the impact of different key types on ease of imaging and printing for replica key production," *Proc. SPIE*, vol. 9867, Jun. 2016, Art. no. 986715.

[33] J. Straub and S. Kerlin, "Consideration of techniques to mitigate the unauthorized 3D printing production of keys," *Proc. SPIE*, vol. 9869, May 2016, Art. no. 98690F.

[34] R. Smith and T. Burghardt, "DeepKey: Towards end-to-end physical key replication from a single photograph," in *Proc. German Conf. Pattern Recognit.*, Stuttgart, Germany 2018, pp. 487–502.

[35] S. Ramesh, H. Ramprasad, and J. Han, "Listen to your key: Towards acoustics-based physical key inference," in *Proc. 21st Int. Workshop Mobile Comput. Syst. Appl.*, Mar. 2020, pp. 1–8.

[36] S. Ramesh, R. Xiao, A. Maiti, J. T. Lee, H. Ramprasad, A. Kumar, M. Jadliwala, and J. Han, "Acoustics to the rescue: Physical key inference attack revisited," in *Proc. 30th USENIX Secur. Symp.*, 2021, pp. 3255–3272.

[37] L. Matić, "Truly random number generator," *Elektor Mag.*, vol. 43, no. 482, pp. 66–73, Mar./Apr. 2017.

[38] P. Tobin, "On the application of PSpice for localized cloud security," Ph.D. thesis, DIT Dublin, Dublin, Ireland, 2018.

[39] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smartcard IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[40] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, document NIST SP 800-22, Rev. 1A, Apr. 2010.

[41] *Random Numbers Generation*, document GOST R-ISO 28640–2012, Dec. 2013.

[42] M. Štampar, "Evaluation of encryption algorithms quality by statistical testing of pseudo-random number generators," diploma thesis, FER Zagreb, Zagreb, Croatia, 2005.

[43] S. K. Chaudhary, P. Ghimire, F. Blaabjerg, P. B. Thógersen, and P. D. P. Rimmen, "Development of field data logger for recording mission profile of power converters," in *Proc. 17th Eur. Conf. Power Electron. Appl.*, 2015, pp. 1–10.

[44] S. Pop, V. Bande, and D. Pitica, "Six channel AC/DC current data logger used in industrial application," in *Proc. IEEE 19th Int. Symp. Design Technol. Electron. Packag. (SIITME)*, Oct. 2013, pp. 223–226.

[45] H. R. Iskandar, A. Purwadi, A. Rizqiawan, and N. Heryana, "Prototype development of a low-cost data logger and monitoring system for PV application," *Proc. 3rd Conf. Power Eng. Renew. Energy*, 2016, pp. 171–177.

LUKA MATIĆ received the M.Sc. degree from the University of Zagreb, Croatia, in 2003. He is currently pursuing the Ph.D. degree. Since 2021, he has been a Researcher with the Department of Control and Computer Engineering, Faculty of Electrical Engineering and Computing, University of Zagreb. From 2013 to 2020, he worked in offshore pipelaying and oil drilling, where he devised ideas for the Ph.D. thesis. He is the author of two books on electronic hardware security. His research interests include non-invasive implementation attacks and secure communications in automation.

KARLA DRAŽENOVIĆ (Graduate Student Member, IEEE) received the M.Sc. degree from the University of Zagreb, Croatia, in 2017, where she is currently pursuing the Ph.D. degree. She is also a Research Assistant with the Department of Electric Machines, Drives and Automation, Faculty of Electrical Engineering and Computing, University of Zagreb. Her research interests include the reliability of power converters, power converters control, and renewable energy systems.

VIKTOR ŠUNDE (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Electrical Engineering and Computing, University of Zagreb, in 1984, 1992, and 1999, respectively. He is a Professor with the Department of Electrical Machines, Drives and Automation, Faculty of Electrical Engineering and Computing, University of Zagreb. From 1985 to 1991, he was with the Electrical Engineering Institute, Rade Končar Company. From 2002 to 2008, he was with the Faculty of Engineering, University of Rijeka. His research interests include power electronics and technology of electronic and electrical components.

ŽELJKO BAN (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Electrical Engineering and Computing, University of Zagreb, in 1985, 1991, and 1999, respectively. From 1985 to 1988, he was a Research Fellow with the Končar Institute of Electrical Engineering, Zagreb. Since 1988, he has been with the Faculty of Electrical Engineering, University of Zagreb, where he is currently a Professor with the Department of Control and Computer Engineering in Automation, Faculty of Electrical Engineering and Computing. Since 2006, his research activities have been focusing on intelligent control of fuel cell energy sources, and control of microgrids consisting of photovoltaic systems, fuel cell systems, and wind energy sources. In his professional activity, he was a project leader of several projects related to adaptive control and control of fuel cell energy sources, funded by the Ministry of Science and Technology, Croatia. More recently, he was also a project leader of projects related to a modular redundant UPS systems, a robust uninterruptible power supply for railroad signaling systems, and charging stations for light electric vehicles. In addition, he also participated in several projects dealing with control of energy flow in regenerative braking of railway vehicles, and model simulation and design of predictive controllers for renewable energy sources and hybrid power system based on solar, wind, and storage systems. His research interests include adaptive and optimal control and control of energy storage systems.