Cybersecurity of Battery Management Systems

Madeline CHEAH

Richard STOCKER

Automotive cybersecurity is a challenge that must be considered as part of the vehicle electrification movement. Cybersecurity of the Battery Management System (BMS) is of particular interest due to its critical role in vehicle functionality, performance and safety as well as its multiple connections to external systems. Despite this, it is a topic that has scarce coverage in literature to date. This paper discusses potential attacks on a generic conventional BMS, outlining the methods and consequences. It also explores the future BMS trends and how this may affect the nature of attacks, and the reach and magnitude of the consequences. Finally, it discusses possible mitigation strategies that if incorporated could reduce the likelihood and impact of potential cybersecurity problems for this system.

Introduction

Historically, embedded systems were designed to operate in a tightly controlled environment, which required specialist knowledge to design, calibrate and deploy. However, the threat landscape has grown with the increasing number of microprocessors and complexity of software, along with the increase in functionality and growth of external-facing interfaces.

The discipline of cybersecurity deals with protecting digital systems from compromise. The foundations revolve around the central concepts of confidentiality, integrity and availability. This is often called the CIA triangle (see Figure 1).

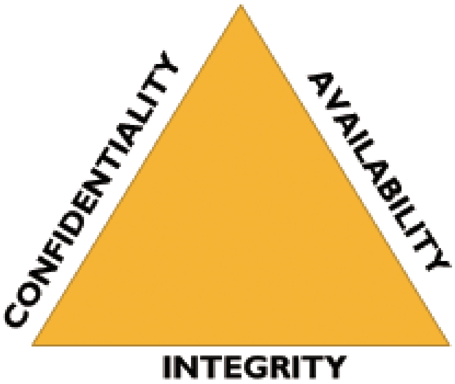

Figure 1 The CIA Triangle

Confidentiality is ensuring any information or data on a system is accessible only to those who are authorised. Integrity deals with the fact that data, information or the stream of data should not be modifiable without authorisation, and only by suitably authorised users. Availability is about ensuring that systems and services are operational in a timely manner when needed for use. The assurance - which can loosely be defined as a declaration of confidence - of these three properties is broadly what it would mean for a system to be considered acceptably secure.

Automotive cybersecurity

Automotive cybersecurity is still a relatively novel field in mainstream automotive engineering.[1] Previous engineering efforts have been focused on performance, efficiency and safety to comply with strict legislation.

There are several major developments which have contributed to the automotive threat landscape:
- Firstly, the presence of increased amounts of software, as well as the introduction of newer technologies such as artificial intelligence, which means that complexity of the system is compounded. Subsequently, testability (such as security testing) becomes an issue, and the likelihood of large numbers and severity of vulnerabilities increases.

- Secondly, advances made in wireless communication interfaces means that increased number of connections is possible. Now instead of physical access being required, only physical proximity is necessary (if that, since there are also long-range technologies being introduced into the vehicle). It also means that there are more externally accessible points for attackers to use (see Section Battery management systems).

- Lastly, impending legislation on the automotive world is also an issue - some of it is direct and some of it is in relation to Internet-of-Things (IoT) of which connected vehicles are considered a subset.

There have been many studies exploring the weaknesses that can be found in the vehicle, with demonstrations of attacks at system level, pivoting through the in-vehicular network,[2, 3] at subsystem or component level,[4] on externally facing interfaces such as WiFi or Bluetooth[1] or on peripheral devices that connect to the on-board diagnostics (OBD-II) port.[5]

In all cases, these demonstrations have leveraged vulnerabilities and weaknesses in the design of the system, the design of the protocols or the implementation thereof. Whilst the demonstrations show the need to consider cybersecurity in the vehicle, there is still much work to be done with regards to many systems in the vehicle. Here we focus on battery management systems (both current generation and future predictive architectures which also incorporate wireless connections) and the potential threats that these vehicular subsystems face.

Battery management systems

A battery management system (BMS) is an essential feature of automotive battery packs containing Li-Ion cells. Li-Ion cells are notoriously volatile when taken outside of their acceptable voltage[6] and current[7] limits, with these limits being strongly dependent on other battery cell states such as State of Charge (SoC) and temperature.[8]
This means that without careful control, dangerous situations can occur, as has been seen in battery cell test conditions.[9, 10] The battery cell states themselves are also not straightforward to estimate, due to their ‘black box’ nature making them impossible to directly observe, instead requiring algorithms to estimate them from externally observable parameters such as cell temperature, voltage and current.[11, 12] This is further complicated by significant changes in battery cells ability to store and transfer charge over lifetime, with this not only being affected by energy throughput but also time (with some level of degradation being an inevitable aspect of Li-ion cell function[14]).

A BMS is also required to coordinate battery pack thermal management, important due to the high sensitivity of performance and safety to battery cell temperature, and defining the charging strategy, which is both integral to and dependent on how the pack capability changes due to degradation.[15, 16]

Due to the complex usage requirements and operational sensitivity of Li-ion cells, the BMS has many roles, not least safety management. A key aspect of BMS functionality is defining current and voltage limits based on SoC and temperature and communicating these to the relevant control system (vehicle powertrain or external charger). Adherence to these limits from external control cannot be guaranteed, so the BMS also has the ability to physically break the electrical circuit through control of contactors within the electrical path of the pack. Monitoring the operation of the pack, identifying varying degrees of unacceptable or unknown behaviour, and deciding the appropriate course of action through contactor management and performance limit broadcasting, is a key aspect of BMS functionality.

All of the above combined necessitates a complex BMS with many tasks, requiring many sources of information and communication with both the externally controlled vehicle powertrain and external chargers. The components and architecture of a generic BMS (along with its connections to the wider system) is given in Table 1. Exact design varies between battery packs, but typically the architecture has one ‘brain’, the battery management controller (BMC), and many nodes acting as its senses, all managed by the battery management module (BMM).

Table 1 Battery pack component functionality and abbreviations (the keys refer to Figure 2)

Key	Component	Functionality	Abbreviation
1	Battery management controller	Data interpretation, state estimation and calculations, contactor control, power, current and voltage limits, safety analysis and shutdown	BMC
2	Battery management module	Sensor data interpretation, cell balancing, warning sensor calculation	BMM
3	Power relay assembly	Physical contactor operation, sends contactor status to the BMC	PRA
4	Current sensor	Senses current through the pack	-
5	Modules	Li-ion cell sensing (temperature and voltage)	-

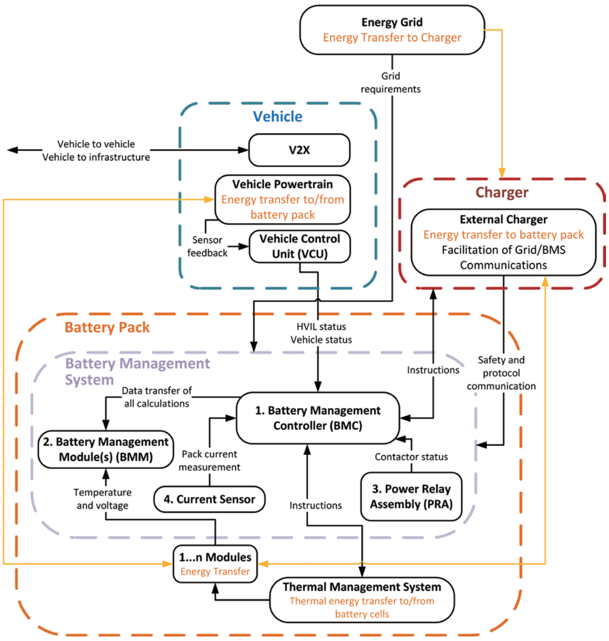
Energy Grid
Energy Transfer to Charger
Grid requirements
Vehicle
Vehicle to vehicle
Vehicle to infrastructure
V2X
Vehicle Powertrain
Energy transfer to/from battery pack
Sensor feedback
Vehicle Control Unit (VCU)
Charger
External Charger
Energy transfer to battery pack
Facilitation of Grid/BMS Communications
Battery Pack
HVIL status
Vehicle status
Battery Management System
Instructions
Safety and protocol communication
Data transfer of all calculations
1. Battery Management Controller (BMC)
2. Battery Management Module(s) (BMM)
Pack current measurement
Contactor status
Temperature and voltage
4. Current Sensor
Instructions
3. Power Relay Assembly (PRA)
1...n Modules
Energy Transfer
Thermal Management System
Thermal energy transfer to/from battery cells

Figure 2 General architecture of a generic BMS and its relationship to the wider vehicular system.

Each of the BMS component functionality is given in Figure 2.

Future BMSs have to perform the same tasks as current generation systems but are made more complex by the fact that there are additional protocols that enable wireless communications (for example using Bluetooth[35]) and that they require predicting what the states of operation and degradation are and instructing changes in component behaviour based on that calculation. These are discussed further in the next section.

Cybersecurity of the BMS

Of almost everything else in the vehicle, there are no other non-human controlled components that are considered so safety critical as the battery and systems associated with it. At this point in time, the literature regarding cybersecurity in this area is sparse. This could be due to the fact that data regarding automotive components is usually treated as confidential, and that much attention has been taken up in the automotive security literature to date by the more externally facing systems such as the infotainment system. However, as the sophistication of battery management system increases, consideration as to what compromise might look like and the consequences it could have is essential.

As a package of electronics (with actuators, sensors and controllers), there is always hardware security of the BMS to be considered. Hardware Trojans, which are malicious modifications to a circuit (whether during the design or fabrication phases) are a danger. Susceptibility to such Trojans are due in part to globalisation of semiconductor processes, and where there are only early or partial solutions to a trustworthy (from a security point of view) global supply chain.

Trojans can be implemented as modifications to any circuit, microprocessor, digital signal processor or controller. Additionally, they could also come as firmware alterations, for example, to FPGA bitstreams.[17] These Trojans can be externally activated (e.g. through sensors or antennas) or internally activated (e.g. either always on or through logic). They can take many forms and could affect anything from chip form factor, to modification of functions or illicit transmission of information.[18]

The second general area which might be targeted is the data required for functionality as well as the connections which facilitate correct transmission of this information. As discussed previously, different kinds of connections (including wireless connections[32-34]) are currently being explored and the security of these would also be paramount[36]. In the next sections we give some examples of all of the above. This includes a discussion of a generic BMS, as well as potential future generations.

Generic BMS review

We outline in Table 2 some of the specific possible attack paths, with the possible failure states described. The target as stated in the table below is the theoretical aim of a malicious adversary. The context is to give some situational understanding as to how the attack might be carried out, and the possible methods give some specific examples (and is not limited to such a method only). The reaction is how the battery management system would react if such a scenario were to occur, and what would happen at system level, where we can more easily see the safety scenarios that might result.

There are also preliminary studies that suggest that environmental factors could affect the severity of the results

Table 2 Cybersecurity scenarios with regards to generic BMS

Target	Context	Possible method	Reaction	System results
Compromise temperature sensors in the battery pack modules	Requires physical access	Placing a resistor on the sensor line	BMC reduces limits, thermal management systems kick in and PRA opens contactors	Loss of power to vehicle
Compromise voltage sensors in battery pack modules	Requires physical access	Physical tampering (e.g. damaging the sensor line)	BMC would instruct PRA to open contactors.	Loss of power to vehicle.
Remove connection between battery pack modules and BMM	Requires physical access unless connection is wireless, in which case would likely require proximity	Causing a short circuit (physical) or jamming (wireless)	BMM sends a warning, BMC tells PRA to open contactors	Loss of power to vehicle
Interfere with connection between BMC and BMM	Requires physical access unless connection is wireless in which case would likely require proximity	Physical tampering or jamming	PRA opens contactors	Loss of power to vehicle
		Injection of invalid or random data	This would interfere with state estimation (e.g. charge instead of discharge), which would lead to abuse conditions. Possible BMS shutdown	Accelerated battery degradation. If all cells are tampered with, then safety issues are possible with overcharge or over-discharge. Loss of power to vehicle.
		Flooding	PRA opens contactors	Loss of power to vehicle.
Modification of software that performs calculations on BMM	Requires access to supply chain	Introduce error in software calculations or spoof incorrect voltages	Affect performance or shutdown the pack	Anything from battery degradation to loss of power and possible safety concern.
Modification of software that performs calculations on BMC			Could lead to overcharge, over-discharge, shutdown, and the BMC becoming not able to control the pack	
Compromise random access memory	Requires physical access or access to supply chain	Rowhammer attack[19] through compromised BMS (can cause memory cells to leak charge and electrically interact, which may also cause corruption or leakage from nearby memory rows)	Could lead to overcharge, over discharge or damage to cells	Battery degradation, BMS shutdown (Loss of power to vehicle)
Disruption of scheduling routines on the BMC	Requires access to the supply chain	Modification of controller software, or physical sabotage (e.g. using a non-spec chip with insufficient processing power)	Limitation of BMS functionality due to missing potentially crucial signals, eventually leading to shutdown	Loss of power to vehicle
Modify the external charger	Requires access to supply chain	Physical tampering of the charger	Incompatible charging leading to lack of charge to the vehicle.	Eventual loss of power to vehicle
Compromise communication between BMC and external charger	Requires physical access unless connection is wireless, in which case would likely require proximity	Spoof current request to external charger	Battery could be overcharged. BMC instructs shutdown	Loss of power to vehicle
Compromise externally facing communication (CAN) to the BMC	Requires physical access unless a wireless device is attached to the vehicle, or another ECU with a wireless interface is compromised (for example through pivoting)	Send “vehicle ignition” off signals into CAN bus	BMC instructs shutdown	Loss of power to vehicle
		Transmit a zero for HVIL value	BMC instructs shutdown	Loss of power to vehicle
		Fuzzing the BMC using CAN protocol (as the BMC performs handshakes via CAN with the charger)	BMC instructs shutdown	Loss of power to vehicle
Compromise current sensor within the BMS	Requires physical access	Spoof current to non-zero	Manipulates state of charge, which can trigger conditions for shutdown	Loss of power to vehicle
Indirect compromise of the battery pack	Requires access to the CAN bus	Disable or interfere with sub-vehicular systems with large battery usage (e.g. disable regenerative braking systems)	Eventual shutdown	Loss of power to vehicle Battery draining and degradation.

of any of the above attacks. For example, attacks launched with a pack that has high state-of-charge leads to more damage to the battery. Additionally, when looking at voltage controller compromise, due to the sublinear relationship of cell resistance increase with time, newer packs may be more vulnerable than older ones to depletion attacks.[20]

In summary, many of the attacks could potentially lead to safety situations at systems level (loss of power during driving for example), as well as lead to battery degradation (either through total decrease in capacity, or degradation due to increased internal resistance in the cell) which could cost the owner of the vehicle financially. The problem would be exacerbated if several scores of vehicles were affected by a strategic adversary, for example, through compromise in the supply chain.

Since the BMC and BMM act as central components for the entire subsystem, compromise (for example through software modification or hardware trojans during manufacture) would in general mean a loss of integrity or availability of data from sensors, the calculations for state estimations, the scheduling routines and the lack of optimisation for cell balancing. Since an optimal range for voltage, state-of-charge, temperature and current are inter-dependent in keeping a cell operationally safe, forcing a state outside of all these parameters (using any or a combination of the attacks discussed above) may result in a situation where the default "shutdown" process (contactors opening) may not occur or is inadequate. This is the greatest risk of all, as thermal runaway could then occur, with all the attendant safety risks.

Predictive or intelligent BMSs

While current BMS technology often uses simple direct measurement algorithms, the next generation of BMSs looks to include predictive and optimisation capabilities. Much of the literature points to the use of machine learning techniques for areas such as state estimation[12, 21] and connection to or at least use of data resulting from wider connectivity (taking again the example of connecting BMCs to the cloud) as a key enabler of predictive optimisation.[22, 23]

This is a response to a combination of respect for the complexity of the states and degradation modes of Li-ion battery cells, and the limitation of simple on-board methods to sufficiently model these in all situations. Conventional methods such as SoC estimation through Open Circuit Voltage (OCV) observation, and SoC tracking through coulomb counting, are susceptible to measurement error and inaccuracies in cell data calibration, with no means of self-correction. To solve this issue, more intelligent algorithms have been developed which can dynamically adjust their SoC estimation based on new cell information,[24] comparing observed behaviour to that expected by on-board models connected to Kalman filters[25] which allow both for error estimation and results correction.

These models work very well for new cells. As cells degrade however, methods must be applied to adapt on-board models that account for the resultant changes in cell capacity, resistance and stoichiometry. Cell ageing is very complex with several dependencies spanning both usage history and cell design, with a high level of nonlinearity and interaction effects[13, 14] and information available limited to full battery cell external parameters such as voltage, current and temperature. This makes applying rigid, non-adaptive models very difficult, encouraging adaptive intelligent approaches.[21-24] These approaches are free from the required simplicity of conventional models and can identify trends and patterns that can be used to predict and express the various aspects of degradation and can adapt control strategies accordingly.

Predictive capability of ageing is also required to evaluate integrated control problems. Fast charging without degradation presents a difficult challenge with multiple objectives e.g. avoiding lithium plating and temperature gradients,[8, 15, 26] with cell susceptibility to these effects changing with cell ageing. Vehicle to grid functionality requires prediction of degradation with expected usage profile, so that it can be evaluated against the monetary benefit of participating.[27]

Connected vehicle driving algorithms must consider several metrics, such as efficiency, range and lifetime, while evaluating different driving and route profile decisions. All of these require complex modelling and have therefore attracted machine learning research, eventually leading to multiple instances of interactive on-board intelligent and possibly unsupervised learning.

External controllers communicating with the battery management system, being vehicle control or grid integration, are also likely to have intelligent algorithms as part of their architecture.[28] Due to the complexity of cell degradation and its path dependent nature, cloud computing methods have also been suggested to handle the large datasets and model sizes.[23, 26]

There are many techniques used currently for state estimation including the use of artificial neural networks (ANNs), support vector machine (SVM), and genetic algorithms (GA) in combination with on-board models. Parameters such as battery terminal voltage, charging

Table 3 Additional review of possible future generation BMS

Target	Context	Possible method	Reaction	System results
Machine learning algorithm for state estimation within the battery pack	Requires access to training and test dataset	Poisoning the training set (e.g. deliberately performing aberrant automotive drive cycles during data acquisition), or changing the labelling of any dataset Poisoning the test dataset	Subsequent models would be inaccurate, causing misestimation of battery behaviour as states are not as transparent as when directly measured	Could compromise performance as optimisation might be inaccurate (e.g. thinking that the pack is newer than it is could lead to abuse of battery, or through the VCU have other effects such as loss of power)
Compromising algorithms on the vehicle outside the battery pack			Could compromise information given to the VCU which in turn gives incorrect information to the BMC	If BMS is predicting parameters such as range, this would lead to inaccurate optimisations at system level
External intelligent algorithms (e.g. grid or charging stations)	Charger is bidirectional	Charger could be compromised such that it tells the battery to continuously discharge	SoC goes to minimal level	Loss of power to vehicle
Responses to environmental data	Requires proximity to external facing sensors for environmental data Possible long-range action possible (e.g. through cellular and GPS)	Spoofing vehicle operation modes, spoofing environmental data that leads to incorrect conclusions about traffic data, interfering with GPS	Could compromise information given to the VCU which in turn gives incorrect information to the BMC	If BMS is predicting parameters such as range, this would lead to inaccurate optimisations at system level

current, discharge and surrounding temperature can be used in conjunction with one or a combination of these to estimate state of charge values without having knowledge of the internals of the battery.[29] This can be extended to state of health measurement with knowledge of usage history.

This predictive capability has two implications from a cyber security perspective. Firstly, the lack of transparency in machine learning (whether it's the dataset or the explanations that led to an action) makes it hard to verify and trust. Secondly, connectivity opens up a once-closed system to potential malicious influence beyond what was already possible through physical access.

We outline possible attack vectors and malicious actions that could be taken against a predictive or intelligent battery management system in Table 3.

Mitigations

A good way to ensure accuracy is using prior offline testing to characterise cell behaviour. Since this provides the reference data for the BMS controller algorithms, it is essential that the integrity of this data is considered and protected. Furthermore, protections (both in software and hardware) should be built such that the software on the BMS cannot be modified without appropriate authorisation.

A mitigation for compromise of any state estimation calculations could be to calculate these states in different ways and in different locations in the battery management system. These alternative ways would then be able to cross-verify accuracy and robustness. Having multiple dimensions would also help with quantifying errors and error tolerance. Having a value outside of the tolerance could then be used as a good indicator of possible compromise. Note that this solution does come with the limitation in that sensors and measurements thereof is based on accumulation of history and may change throughout its lifetime. The optimal balance between changes observed is where the application of advanced techniques such as machine learning could be used.

In terms of considering BMS design, hardwiring should be considered a priority for the components of the BMS that could be considered safety triggers (e.g. temperature and current sensors). The response to an incident could also be designed such that immediate shutdown isn't the only safety measure. There is already work done to look at solutions that are not binary, such as backing off the current in stages,[30] giving warnings instead of shutdowns (for example, if only one out of a multitude of similar signals is lost),[31] or extend the time before a shutdown.[30]

Broadening out to the system level, since everything in the vehicle is interconnected to varying degrees, defending the intra-vehicular network communications is also essential. The current CAN protocol has no defensive capabilities nor security properties: no verification as to identity of nodes take place, the communication is unencrypted, and the CAN network is sensitive to injection of invalid data or data rates due to its bus architecture. Future vehicular protocols promise to remedy such issues, but since components will remain connected, architectures and topologies should be reviewed such that the risk of indirect compromise of the battery through inducing aberrant behaviour in systems with large battery usage is minimised.

Along with the specific safeguards and strategies that could be implemented at subcomponent or vehicle system level, we can see that many of the contexts in which an attack is possible involve access to components during the manufacturing process. This includes poisoning datasets, that are used for advanced techniques such as machine learning, tampering with the hardware or compromising sensors. This means that all the necessary requirements for security of the supply chain should also be considered, including knowing what possible assets might be, their value, who suppliers are as well as their level of maturity with regards to their own security arrangements. A risk driven approach can then be taken with regards to over-reliance, suppliers who have continually failed to meet security expectations as well as further communication and continuous improvement.

Finally, in terms of future BMS design, transparency will be a key feature. Since there are so many factors to balance and optimise, explainability (how algorithms come to a particular decision and what factors affect those decisions) will play a large part in testing, verification and - once integrated - communication with the larger system. This transparency is also beneficial for cybersecurity as it maintains a "human-in-the-loop" that would mean tampering, sabotage or other malicious modifications might be more apparent before it becomes a risk. Understanding the cybersecurity risks and potential attacks is also key to developing a secure testing platform which can be used to anticipate problems and verify that the system reacts appropriately.

Conclusions and Further Research

In conclusion, this discussion aims to highlight possible risks to the BMS from a cybersecurity perspective. We take the position here that whilst some attacks may seem infeasible to carry out, the safety impact of compromise requires that such considerations take place.

For future research, we would need to empirically validate such considerations on actual vehicles by carrying out the attacks as described above in controlled testing and simulation environments, using this to develop and quantify mitigation strategies. Characterisation and observation of any wireless protocols in use would also be useful in understanding where the exact attack vectors might be. This would need to be benchmarked with different battery management system designs or implementation. For future predictive capabilities, the more general research area of security of artificial intelligence (currently an emerging topic) would need to be further explored and specific security strategies developed for this area of technology.

Despite the recommendations and mitigations discussed above, there are no absolute solutions in the cybersecurity world. However, by reviewing the state-of-the-art, including emerging technologies that may impact future battery management systems, we can anticipate possible risks, and thus take our understanding one step further in ensuring the security and safety of vehicles.

* This content is based on our investigation at this publish unless otherwise stated.

References

[1] M. . Cheah, S. A. Shaikh, O. C. Haas and A. R. Ruddle, "Towards a systematic security evaluation of the automotive Bluetooth interface," *Vehicular Communications*, vol. 9, no. , pp. 8-18, 2017.

[2] K. Koscher, A. Czeskis, F. Roesner, S. N. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2010.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX conference on Security*, San Francisco, CA, 2011.

[4] R. Verdult, F. D. Garcia and J. Balasch, "Gone in 360 seconds: Hijacking with Hitag2," in *21st USENIX Security Symposium*, Bellevue, WA, 2012.

[5] M. Cheah, J. W. Bryans, D. Fowler and S. A. Shaikh, "Threat Intelligence for Bluetooth-Enabled Systems with Automotive Applications: An Empirical Study," in *3rd Workshop on Safety and Security in Vehicles (SSIV): Dependable Systems and Networks Workshop (DSN-W) 2017*, Denver, 2017.

[6] A. W. Golubkov, S. Scheikl, R. Planteu, G. Voitic, H. Wiltsche, C. Stangl, G. Fauler, A. Thaler and V. Hacker, "Thermal runaway of commercial 18650 Li-ion batteries with LFP and NCA cathodes

- impact of state of charge and overcharge," *Royal Society of Chemistry*, vol. 5, pp. 57171-57186, 2015.

[7] P. Keil and A. Jossen, "Charging protocols for lithium-ion batteries and their impact on cycle life - An experimental study with different 18650 high-power cells," *Journal of Energy Storage*, vol. 6, pp. 125-141, 2016.

[8] S. Tippmann, D. Walper, L. Balboa, B. Spier and W. G. Bessler, "Low-temperature charging of lithium-ion cells part I : Electrochemical modeling and experimental investigation of degradation behavior," *Journal of Power Sources*, vol. 252, pp. 305-316, 2014.

[9] Q. Wang, P. Ping, X. Zhao, G. Chu, J. Sun and C. Chen, *Thermal runaway caused fire and explosion of lithium ion battery*, vol. 208, 2012, pp. 210-224.

[10] F. Larsson, P. Andersson, P. Blomqvist, A. Lorén and B. E. Mellander, "Characteristics of lithium-ion batteries during fire tests," *Journal of Power Sources*, vol. 271, pp. 414-420, 20 12 2014.

[11] Y. Zhou and X. Li, "Overview of lithium-ion battery SOC estimation," *2015 IEEE International Conference on Information and Automation, ICIA 2015 - In conjunction with 2015 IEEE International Conference on Automation and Logistics*, no. August, pp. 2454-2459, 2015.

[12] N. Watrin, B. Blunier and A. Miraoui, "Review of adaptive systems for lithium batteries state-of-charge and state-of-health estimation," in *IEEE Transportation Electrification Conference and Expo, ITEC 2012, no. 3, 2012*, London, 2012.

[13] S. F. Schuster, T. Bach, E. Fleder, J. Müller, M. Brand, G. Sextl and A. Jossen, "Nonlinear aging characteristics of lithium-ion cells under different operational conditions," *Journal of Energy Storage*, vol. 1, no. 1, pp. 44-53, 2015.

[14] J. Vetter, P. Novák, M. Wagner, C. Veit, K.-C. Möller, J. Besenhard, M. Winter, M. Wohlfahrt-Mehrens, C. Vogler and A. Hammouche, "Ageing mechanisms in lithium-ion batteries," *Journal of Power Sources*, vol. 147, no. 1-2, pp. 269-281, 2005.

[15] T. Waldmann, M. Kasper and M. Wohlfahrt-mehrens, "Optimization of Charging Strategy by Prevention of Lithium Deposition on Anodes in high-energy Lithium-ion Batteries - Electrochemical Experiments," *Electrochimica Acta*, vol. 178, pp. 525-532, 2015.

[16] P. Keil and A. Jossen, "Charging protocols for lithium-ion batteries and their impact on cycle life - An experimental study with different 18650 high-power cells," *Journal of Energy Storage*, vol. 6, pp. 125-141, 2016.

[17] M. Tehranipoort and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 10-25, 2010.

[18] R. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in *IEEE High Level Design Validation and Test Workshop*, San Francisco, CA, 2009.

[19] R. Qiao and M. Seaborn, "A new approach for rowhammer attacks," in *Proceedings of 2016 IEEE International Symposium on Hardware Oriented Security and Trust*, McLean, VA, 2016.

[20] S. Sripad, S. Kulandaivel, V. Pande and V. Viswanathan, *Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks*, arXiv preprint arXiv:1711.04822, 2017.

[21] X. Hu, S. E. Li and Y. Yang, "Advanced Machine Learning Approach for Lithium-Ion Battery State Estimation in Electric Vehicles," *IEEE Transactions on Transportation Electrification*, vol. 2, no. 2, pp. 140-149, 2015.

[22] M. Abdul-Hak, N. Al-Holou and U. Mohammad, "Predictive Intelligent Battery Management System to enhance the performmance of electric vehicles," in *Electric Vehicles - Modelling and Simulations*, S. Soylu, Ed., InTech, 2011, pp. 365-384.

[23] R. Xiong, L. Li and J. Tian, "Towards a smarter battery management system: A critical review on battery state of health monitoring methods," *Journal of Power Sources*, vol. 405, no. 30, pp. 18-29, 2018.

[24] F. Han, K. See, Y. Feng, X. Yu and X. Yi, "Online SoC Estimation for Li-ion Batteries: A survey," in *12th IEEE Conference on Industrial Electronics and Applications*, Siem, Reap, 2017.

[25] K. Stetzel, L. Aldrich, M. S. Trimboli and G. Plett, "Electrochemical state and internal variables estimation using a reduced-order physics-based model of a lithium-ion cell and an extended Kalman filter," *Journal of Power Sources*, vol. 278, pp. 490-505, 2015.

[26] A. Hoke, A. Brissette, K. Smith, A. Pratt and D. Maksimovic, "Accounting for Lithium-Ion Battery Degradation in Electric Vehicle Charging Optimization," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. PP, no. 99, 2014.

[27] D. Wang, J. Coignard, T. Zeng, C. Zhang and S. Saxena, "Quantifying electric vehicle battery degradation from driving vs. vehicle-to-grid services," *Journal of Power Sources*, vol. 332, pp. 193-203, 2016.

[28] R. Abduljabbar, H. Dia, S. Liyange and S. A. Bagloee, "Applications of Artificial Intelligence in Transport:," *Sustainability*, vol. 189, no. 11, 2019.

[29] V. Mishra, A. R. Kodakkadan, R. Koduri, S. Nandyala and M. Manalikandy, "Wireless Charging for EV/HEV with Prescriptive Analytics, Machine Learning, Cybersecurity and Blockchain Technology: Ongoing and Future Trends," SAE International, 2019.

[30] W. Kong, Y. Luo, Y. Qi and Y. Wang, "Full Protection Scheme and Energy Optimization Management of the Battery in Internal Combustion Engine Vehicles Based on Power Partitioning Model," *SAE Technical Paper*, Vols. 2019-01-1205, 2019.

[31] J. Xie, J. Chen, L. Li and Y. Chen, "Advanced battery early warning and monitoring system". US Patent US9454888B2, 27 09 2016.

[32] D. E. Alonso, O. Opalko, M. Sigle and K. Dostert, "Towards a Wireless Battery Management System: Evaluation of Antennas and Radio Channel Measurements Inside a Battery Emulator," in *IEEE 80th Vehicular Technology Conference*, Vancouver, 2014.

[33] M. Schneider, S. Ilgin, N. Jegenhorts, R. Kube, S. Püttjer, K. Riemschneider and J. Vollmer, "Automotive Battery Monitoring by Wireless Cell Sensors," in *IEEE International Instrumentation and Measurement Technology Conference*, Graz, 2012.

[34] C. Shell, J. Henderson, H. Verra and J. Dyer, "Implementation of a Wireless Battery Management System (WBMS)," in *IEEE International Instrumentation and Measurement Technology Conference*, Pisa, 2015.

[35] G. D. Maso-Gentile, A. Bacà, L. Ambrosini, S. Orcioni and M. Conti, "Design of CAN to Bluetooth gateway for a Battery Management System," in *12th IEEE International Workshop on Intelligent Solutions in Embedded Systems*, Ancona, 2015.

[36] G. Kwon, J. Kim, J. Noh and S. Cho, "Bluetooth low energy security vulnerability and improvement method," in *IEEE International Conference on Consumer Electronics-Asia*, Seoul, 2016.

Madeline CHEAH

Cybersecurity Innovation Lead
Horizon Scanning
HORIBA MIRA Ltd.
Ph.D.

Richard STOCKER

Energy Systems Innovation Lead
Horizon Scanning
HORIBA MIRA Ltd.