



SURFACE VEHICLE INFORMATION REPORT

J3101™-4

JUN2026

Issued

2026-06

Side Channel and Fault Injection Attack Resistance

RATIONALE

Side channel and fault injection attacks have become increasingly relevant to embedded systems in recent years, with tools and technical know-how becoming more affordable and accessible. Guidance is needed on how these attacks apply to automotive embedded systems taking into account in their operational environment, as well as appropriate mitigation techniques. This information report is intended to complement the requirements and use cases for hardware protected security environments that are already defined in SAE J3101, enabling the specification of requirements for side channel and fault injection attack resistance in a consistent way throughout the automotive supply chain.

TABLE OF CONTENTS

1.	SCOPE.....	3
2.	REFERENCES.....	3
2.1	Applicable Documents	3
2.1.1	SAE Publications.....	3
2.1.2	ISO Publications.....	3
2.1.3	NIST Publications.....	3
2.1.4	Other Publications.....	3
3.	DEFINITIONS	7
4.	ABBREVIATIONS	7
5.	INTRODUCTION.....	8
6.	SURVEY OF ATTACKS AND COUNTERMEASURES.....	8
6.1	Side Channel Attacks.....	9
6.1.1	Type of Side Channel.....	10
6.1.2	Type of Analysis.....	11
6.1.3	Level of Invasiveness.....	12
6.2	Fault Injection Attacks.....	13
6.2.1	Fault Source.....	13
6.2.2	Type of Analysis.....	14
6.2.3	Level of Invasiveness.....	15
6.3	Hybrid Attacks	15
6.3.1	Collision-Based Side Channel Attacks.....	15
6.3.2	Combined Fault Injection and Side Channel Attacks.....	16
6.4	Side Channel Countermeasures.....	16
6.4.1	Reduce or Hide Information Leakage	16
6.4.2	Eliminate Relationship Between Leaked Information and Secret Data	16
6.5	Fault Injection Countermeasures	17
6.5.1	Detect the Source of the Injected Fault.....	17

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2026 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3101-4_202606

For more information on this standard, visit https://www.sae.org/standards/content/3101-4_202606/

Documents

Standard, visit Sharing Hub

6.5.2	Detect the Effect of the Injected Fault.....	17
7.	APPLICABILITY TO AUTOMOTIVE TARGETS	17
7.1	Cryptographic Key Leakage.....	17
7.2	Security State Unlocking	18
8.	NOTES	18
8.1	Revision Indicator.....	18
Figure 1	Taxonomy of selected side channel and related hardware attacks	9
Figure 2	Pseudo code example of a secure boot glitch vulnerability.....	18

1. SCOPE

This report provides a survey of side channel and fault injection attacks that have an impact on automotive embedded systems. The focus is on side channel attacks that target cryptographic algorithms and hardware security engines, as well as sensitive data leakage. The report also considers fault injection attacks against typical vehicle components that allow bypassing of security controls to compromise the target system security and outlines some countermeasures to detect and/or prevent them. The report provides a list of security countermeasures that can be considered by manufacturers based on their risk tolerance to such attacks. Additionally, it offers the automotive industry supply chain a common language to facilitate the communication of side channel and fault injection mitigation requirements among the various stakeholders.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J3101 Hardware Protected Security for Ground Vehicles

2.1.2 ISO Publications

Copies of these documents are available online at www.iso.org/store.

ISO/IEC 19790:2025 Information security, cybersecurity and privacy protection - Security requirements for cryptographic modules

2.1.3 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

NIST SP 800-63-4 Digital Identity Guidelines

2.1.4 Other Publications

- [1] Kocher, P. et al. (1999). *Differential Power Analysis*. CRYPTO '99. LNCS, 1666, Springer. https://link.springer.com/chapter/10.1007/3-540-48405-1_25.
- [2] Brier E. et al. (2004). *Correlation power analysis with a leakage model*. CHES 2004. LNCS, 3156, Springer. <https://www.iacr.org/archive/ches2004/31560016/31560016.pdf>.
- [3] Lu, J. et al. (2010). *Principles on the Security of AES against First and Second-Order Differential Power Analysis*. ACNS 2010: Applied Cryptography and Network Security. https://link.springer.com/content/pdf/10.1007%2F978-3-642-13708-2_11.pdf.
- [4] Kim et al. (2010). *Practical Second-Order Correlation Power Analysis on the Message Blinding Method and Its Novel Countermeasure for RSA*. ETRI Journal. <https://pdfs.semanticscholar.org/f3fa/ad103781026690e24d33a286f15a222bb676.pdf>.
- [5] Bauer, A. et al. (2014). *Side-Channel Attack against RSA Key Generation Algorithms*. CHES 2014: Cryptographic Hardware and Embedded Systems. https://link.springer.com/content/pdf/10.1007%2F978-3-662-44709-3_13.pdf.

- [6] Lo, O., Buchanan, W.J., and Carson, D. (2016). Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *Journal of Cyber Security Technology*. <https://www.tandfonline.com/doi/full/10.1080/23742917.2016.1231523>.
- [7] Duan, X. et al. (2016). *Differential power analysis attack and efficient countermeasures on present*. 8th IEEE International Conference on Communication Software and Networks (ICCSN). <https://ieeexplore.ieee.org/abstract/document/7586627>.
- [8] Reparaz, O. and Gierlichs, B. (2017). *A First-Order Chosen-Plaintext DPA Attack on the Third Round of DES*. CARDIS 2017: Smart Card Research and Advanced Applications. https://link.springer.com/chapter/10.1007/978-3-319-75208-2_3.
- [9] Rai, V. et al. (2019). *Correlation power analysis and effective defense approach on light encryption device block cipher*. Security and Privacy. <https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.87>.
- [10] Randolph, M., and Diehl, W. (2020). *Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman*. Cryptography Special Issue Side Channel and Fault Injection Attacks and Countermeasures. <https://www.mdpi.com/2410-387X/4/2/15>.
- [11] Kuhn, M. (2003). *Compromising emanations: eavesdropping risks of computer displays* (Technical Report UCAM-CL-TR-577). University of Cambridge, Computer Laboratory.
- [12] Van Eck, W. (1985). Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers & Security*, 4(4), 269-286.
- [13] Strenzke, F. (2010). *A Timing Attack against the Secret Permutation in the McEliece PKC*. PQCrypto 2010: Post-Quantum Cryptography. https://link.springer.com/chapter/10.1007/978-3-642-12929-2_8.
- [14] Hund, R., et al. (2013). *Practical Timing Side Channel Attacks against Kernel Space ASLR*. IEEE Symposium on Security and Privacy. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6547110>.
- [15] Jiang, Z. et al. (2017). *A Novel Side-Channel Timing Attack on GPUs*. Proceedings of the on Great Lakes Symposium on VLSI. <https://dl.acm.org/doi/pdf/10.1145/3060403.3060462>.
- [16] Kayaalp, M. et al. (2016). *A high-resolution side-channel attack on last-level cache*. Proceedings of the 53rd Annual Design Automation Conference. <https://dl.acm.org/doi/abs/10.1145/2897937.2897962>.
- [17] Bruinderink, L. et al. (2016). *Flush, Gauss, and Reload - A Cache Attack on the BLISS Lattice-Based Signature Scheme*. Cryptographic Hardware and Embedded Systems - CHES 2016. https://link.springer.com/chapter/10.1007/978-3-662-53140-2_16.
- [18] Lipp, M. et al. (2016). *ARMageddon: Cache Attacks on Mobile Devices*. USENIX. <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lipp>.
- [19] Zhang, X. et al. (2016). *Return-Oriented Flush-Reload Side Channels on ARM and Their Implications for Android Devices*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications. <https://dl.acm.org/doi/abs/10.1145/2976749.2978360>.
- [20] Irazoqui, G. and Guo X. (2017). *Cache Side Channel Attack: Exploitability and Countermeasures*. Black Hat Asia. <https://syssec-s18.unexploitable.systems/l/week09/bh-side-channel.pdf>.
- [21] Schaik, S. et al. (2017). *Reverse Engineering Hardware Page Table Caches Using Side-Channel Attacks on the MMU*. https://download.vusec.net/papers/revanc_ir-cs-77.pdf.
- [22] Lipp, M. et al. (2018). *Meltdown: Reading Kernel Memory from User Space*. 27th USENIX Security Symposium (USENIX Security 18). <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-lipp.pdf>.

- [23] Kocher, P. et al. (2019). *Spectre Attacks: Exploiting Speculative Execution*. 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA. <https://doi.org/10.1109/SP.2019.00002>.
- [24] Yuan, Z. et al. (2018). *Recovering Memory Access Sequence with Differential Flush+Reload Attack*. ISPEC 2018: Information Security Practice and Experience. https://link.springer.com/chapter/10.1007/978-3-319-99807-7_26.
- [25] Van Bulck, J. et al. (2018). *Foreshadow: Extracting the keys to the Intel SGX kingdom with transient out-of-order execution*. Proceedings of the 27th USENIX Conference on Security Symposium, ser. SEC'18, Berkeley, CA, USA, USENIX Association. <http://dl.acm.org/citation.cfm?id=3277203.3277277>.
- [26] Mohamed, M. et al. (2012). *Improved algebraic side-channel attack on AES*. IEEE International Symposium on Hardware-Oriented Security and Trust. <https://ieeexplore.ieee.org/abstract/document/6224335>.
- [27] Wang, W. et al. (2017). *Ridge-Based Profiled Differential Power Analysis*. CT-RSA 2017: Topics in Cryptology. https://link.springer.com/chapter/10.1007/978-3-319-52153-4_20.
- [28] Picek, S. et al. (2017). *Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks*. Progress in Cryptology - AFRICACRYPT 2017. https://bib.irb.hr/datoteka/877192.ML_final.pdf.
- [29] Choudary, M. and Kuhn, M. (2018). *Efficient, Portable Template Attacks*. IEEE Transactions On Information Forensics and Security. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8052147>.
- [30] Xu, J. and Heys, H. (2018). *Template Attacks of a Masked S-Box Circuit: A Comparison Between Static and Dynamic Power Analyses*. 16th IEEE International New Circuits and Systems Conference (NEWCAS). <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8585541>.
- [31] Ni, Z. and Ju, T. (2019). *Application of Gaussian Mixture Clustering Algorithm in Template Attack*. IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8729081>.
- [32] Weissbart, L. et al. (2019). *One Trace Is All It Takes: Machine Learning-Based Side-Channel Attack on EdDSA*. SPACE 2019: Security, Privacy, and Applied Cryptography Engineering. <https://eprint.iacr.org/2019/358.pdf>.
- [33] Schramm, K. et al. (2004). *A Collision-Attack on AES*. CHES 2004: Cryptographic Hardware and Embedded Systems. https://link.springer.com/content/pdf/10.1007%2F978-3-540-28632-5_12.pdf.
- [34] Bogdanov, A. (2008). *Multiple-Differential Side-Channel Collision Attacks on AES*. CHES 2008: Cryptographic Hardware and Embedded Systems. https://link.springer.com/chapter/10.1007/978-3-540-85053-3_3.
- [35] Clavier, C. et al. (2010). *Passive and Active Combined Attacks on AES: Combining Fault Attacks and Side Channel Analysis*. 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5577362>.
- [36] Roche, T. et al. (2011). *Combined Fault and Side-Channel Attack on Protected Implementations of AES*. CARDIS 2011: Smart Card Research and Advanced Applications. https://link.springer.com/content/pdf/10.1007%2F978-3-642-27257-8_5.pdf.
- [37] Ruhrmair, U. et al. (2014). *Efficient Power and Timing Side Channels for Physical Unclonable Functions*. CHES 2014: Cryptographic Hardware and Embedded Systems. https://link.springer.com/content/pdf/10.1007%2F978-3-662-44709-3_26.pdf.
- [38] Kovacs, E. (2017). *Hard Drive LED Allows Data Theft From Air-Gapped PCs*. Security Week, retrieved 03-18-2018.
- [39] Ferrigno, J. and Hlaváč, M. (2008). When AES blinks: introducing optical side channel. *IET Information Security*, 2(3), 94-98. <https://doi.org/10.1049/iet-ifs:20080038>.
- [40] Grand, J. OpticSpy. <http://www.grandideastudio.com/opticspy/>.

- [41] Tang, A., Sethumadhavan, S., and Stolfo, S. (2017). *CLKSCREW: Exposing the perils of security-oblivious energy management*. USENIX Security '17, Vancouver, BC, USENIX Association.
- [42] Skorobogatov, S.P. and Anderson, R.J. (2003). Optical fault induction attacks. Kaliski, B.S., Koç, K., and Paar, C. (Eds.) CHES 2002. LNCS, 2523, 2-12. Springer, Heidelberg (2003). https://link.springer.com/content/pdf/10.1007/3-540-36400-5_2.pdf or <https://www.cl.cam.ac.uk/~rja14/Papers/faultpap3.pdf>.
- [43] Biham, E. and Shamir, A. (1996). *The Next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems*.
- [44] Boneh, D., DeMillo, R., and Lipton, R. (1997). *On the Importance of Checking Cryptographic Protocols for Faults*. Eurocrypt.
- [45] *Laser-Based Audio Injection on Voice-Controllable Systems*. <https://lightcommands.com/>.
- [46] Kim, Y., Daly, R., Kim, J., Fallin, C., Lee, J.H., Lee, D. et al. (2014). *Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors*. Proceedings, ISCA 2014. <https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf>.
- [47] Lipp, M. et al. (2020). *Nethammer: Inducing Rowhammer Faults through Network Requests*. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy. <https://ieeexplore.ieee.org/document/9229701>.
- [48] Mutlu, O. and Kim, J.S. (2019). RowHammer: A retrospective. *Trans. Comput.-Aided Design Integr. Circuits Syst.*, 39(8), 1555-1571. https://people.inf.ethz.ch/omutlu/pub/RowHammer-Retrospective_jeec_tcad19-official.pdf.
- [49] Kim, D., Park, H., Yeo, I., Lee, YK, Kim, Y., Lee, HM, and Kwon, KW. (2024). Rowhammer Attacks in Dynamic Random-Access Memory and Defense Methods. *Sensors* 24(2), 592. <https://www.mdpi.com/1424-8220/24/2/592>.
- [50] Mazumder Shuvo, A. et al. (2023). *A Comprehensive Survey on Non-Invasive Fault Injection Attacks*. <https://eprint.iacr.org/2023/1769.pdf>.
- [51] Giechaskiel I. and Rasmussen, K. (2019). Taxonomy and challenges of out-of-band signal injection attacks and defenses. *IEEE Communications Surveys Tutorials*, 22(1), 645-670.
- [52] Zhang, G. et al. (2017). *DolphinAttack: Inaudible Voice Commands*. Proceedings of the 24th ACM CCS.
- [53] Spadavecchia, L. (2005). *A network-based asynchronous architecture for cryptographic devices*. Edinburgh Res Archive.
- [54] Molnar, D. et al (2005). *The Program Counter Security Model: Automatic Detection and Removal of Control-Flow Side Channel Attacks*. IACR Cryptology ePrint Archive, 156-168.
- [55] *Side-channel Attack*. Wikimedia Foundation, uploaded May 28. 2024. https://en.wikipedia.org/wiki/Side-channel_attack.
- [56] E. Prouff, E., et al. (2013). *Masking against Side-Channel Attacks: A Formal Security Proof*. Advances in Cryptology - EUROCRYPT 2013. Lecture Notes in Computer Science, 7881, 142-159. [doi:10.1007/978-3-642-38348-9_9](https://doi.org/10.1007/978-3-642-38348-9_9). ISBN 978-3-642-38347-2.