講演番号	075

A Study on Implementing Model Traceability with Cryptographic Hash Functions

Masahiro Okamura[1)] Kimitoshi Tsuji[2)] Tsunehiro Saito[3)] Toshiji Kato[4)]

1) JSOL Corp., KUDAN-KAIKAN 1-6-5,Chiyoda-ku,Tokyo, 102-0074, Japan
2) Digital Twins Inc., 3-11-1 Senpukugaoka,Susono-shi,Shizuoka,410-1115, Japan
3) AGC Inc. 1-1 Suehiro-cho, Tsurumi-ku, Yokohama-shi, Kanagawa, 230-0045, Japan
4) Department of Electrical Engineering, Doshisha University, Kyoto, 610-0321, Japan

KEY WORDS: **Traceability, Virtual Test, off-cycle credits, Cryptographic Hash Function**

This paper presents a practical approach to ensuring model traceability and integrity in simulation-based vehicle performance evaluation by using cryptographic hash functions. As test requirements for automotive environmental performance—especially for electric vehicles (EVs)—become increasingly complex, physical testing alone is insufficient. Consequently, simulation-based evaluation and virtual testing are gaining importance. However, simulations are inherently vulnerable to risks such as data tampering, unintended parameter changes, and human error, which can directly affect evaluation results and undermine credibility.

To address this issue, a data integrity verification framework based on cryptographic hash functions, focusing on future applications such as off-cycle credit evaluation is proposed. A small EV model developed within an automotive MBD research framework is used as a case study. The model is clearly separates immutable vehicle models (binary files) from modifiable scenario and input condition files (ASCII files), such as ambient temperature and driving speed profiles.

The study defines both normal and tampered scenarios in which input files are subtly modified while preserving file size and timestamps to evade conventional checks. Simulation results show that such manipulations can lead to approximately 2% apparent performance improvement, highlighting the severity of the risk. Using SHA-256 hash values generated via Python's standard library, the proposed method successfully detects all tampered files while confirming the integrity of unchanged components, even under concealment techniques.

Beyond technical validation, the paper proposes two operational frameworks: a third-party evaluation scheme and a self-evaluation scheme, both leveraging externally managed hash registries to ensure transparency and reproducibility. These schemes emphasize verification of procedural correctness rather than absolute model correctness.

Finally, remaining challenges, including balancing transparency with intellectual property protection, establishing international standards, and securely binding simulation results to verified models are discussed.

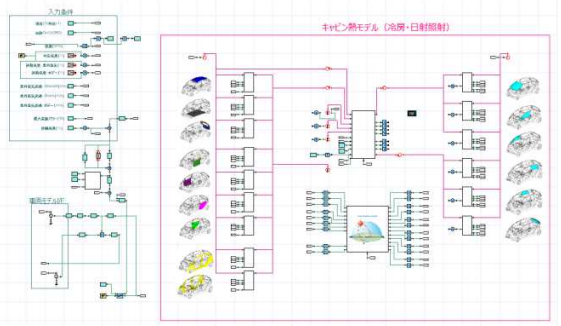

Fig.1 EV model used in this study

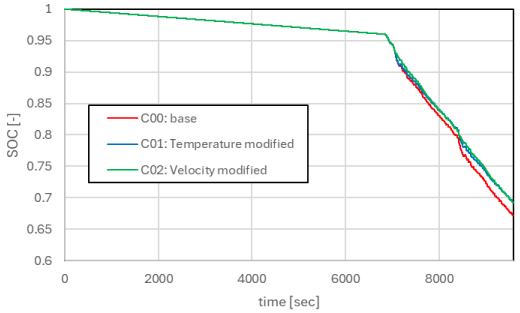

Fig.2 Comparison of SOC with base and tampered model

Fig.3 Hash comparison