Fault Diagnosis and Prognosis in a Network of Embedded Systems in Automotive Vehicles

K. Pattipati[1], C. Sankavaram[1], B. Wang[2], P. Zhang[1], Y. Zhang[3], M. Howell[3], M. Salman[3]
[1]Dept. of Electrical and Computer Engineering, [2]Dept. of Computer Science and Engineering, Storrs, CT 06268
[3]GM Research Center, General Motors Corporation, Warren, MI 48090

I. Problem Identification

The relentless competition among automotive companies and increased demands from customers for driver assistance functions, dynamically-controlled safety systems, driving comfort and infotainment services in vehicles are creating mounting time-to-market pressures and, consequently, shortened development times. With the shortened development times and increased vehicle complexity, guaranteeing hardware-software integrity and, hence, vehicle performance has become a salient issue. This is because poor vehicle performance increases maintenance costs to customers and warranty costs to automotive manufacturers; which, in turn, result in customer dissatisfaction and reduced competitiveness of US automotive industry. The development of methods for ensuring reliable embedded systems of heterogeneous components that are designed and implemented by different suppliers, and vehicle diagnostics and prognostics are of vital interest to US automotive industry.

II. Why Fault Diagnosis and Prognosis (D&P)?

The automobile is one of the most widely distributed cyber-physical systems. Today's high-end vehicles already contain more than 70 distributed microcontrollers (also termed electronic control units (ECUs)), 100 MegaBytes of code, 5 or more distinct communication networks, and have several thousand data and control signals being exchanged in real-time every second. The ECUs in modern vehicles perform a variety of cyber-physical functions such as stability control, remote monitoring, energy-efficient propulsion, navigation with real-time traffic, adaptive cruise control, by-wire steering and braking, keyless entry with push button start, side blind zone detection, lane departure warning, autonomous driving, to name a few. Approximately 80-90% of these vehicle innovations are based on software-embedded systems, and this has resulted in an increase in the number of interactions (coupling) among heterogeneous subsystems. Thus, in order to ensure vehicle performance, one has to be cognizant of the complex interactions among the various subsystems and faults in physical devices (e.g., sensors, batteries, motors) and software algorithms running on embedded processors. This is a challenging task and is receiving an increased amount of attention in order to ensure reliable embedded automotive systems.

Faults in an automobile range from issues that affect a single subsystem (either hardware or software), to issues that occur only as a result of interaction among multiple subsystems (interactions between hardware and software, i.e., HW/SW interaction failures). In addition, while software degradation is not a concern here, the performance of software is subjected to physical constraints that evolve as the hardware ages. For instance, the reliability of the system memory in electronic control unit (ECU), the accuracy of the sensors, and the linearity of actuators all change over the vehicle lifetime in regards to the original software design. Furthermore, with the increase in the number of vehicle features, the interactions among the ECUs over the communication network has significantly increased; this may result in an unpredictable or emergent behavior which may not be anticipated in the design stage. Thus, understanding the cyber-physical nature of these systems and dealing with network level issues to avoid costly vehicle recalls poses a significant challenge for automotive researchers. *Advanced diagnosis and prognosis technologies are needed to quickly isolate faults in complex embedded automotive systems (network level, ECU, and automotive subsystem failure modes), and to predict the degradation path so that appropriate corrective reconfiguration and maintenance actions can be taken.*

III. Fault Diagnosis and Prognosis Research Challenges in Automotive Cyber-physical Systems

The key research challenges for ensuring reliable networked embedded automotive systems are:

(i) *Integrated Hardware-Software Modeling:* Modeling networked and fault-tolerant embedded systems that include automotive subsystems, electronic control units and communication networks within a vehicle is a challenging task. Although modeling tools exist in each of the three areas (e.g., MATLAB-Simulink, PSAT, CANoe), easy-to-use integrated modeling tools that can model vehicular subsystems, control software and the network communication across ECU software components do not exist at present.

(ii) *Understanding Faults, Errors, Failures and Symptoms*: A fault (root cause, failure mode) is an abnormal event occurring in an embedded automotive system and it may be categorized as permanent, intermittent or transient. Faults manifest as errors in intended subsystem functions and these may propagate within the network of embedded systems causing errors in faultless subsystems. An observable error is termed a failure. Symptoms ("tests", "monitoring mechanisms", alerts, "alarms") are external manifestation of failures. The first and foremost issue in fault diagnosis involves understanding the fault-error-failure-symptom characteristics of embedded automotive systems via fault injection experiments and hardware-in-the-loop simulators in multi-core processors and high-density reprogrammable FPGA interfaces. Quite often, the failures are not anticipated at the design stage and yet can occur during integration, operation or even when ECU vendors are changed. Besides, it is difficult to model these complex interactions and to anticipate every possible driving scenario. Hence, characterizing the faults and their effects by understanding the interactions among multiple subsystems, ECUs and the controller area network (CAN) are critical to developing failure detection, diagnosis and prognosis methods.

(iii) *Integrated Diagnostic & Prognostic Framework*: In order to realize high-integrity heterogeneous embedded systems designed and implemented by different vendors, a D&P modeling framework that integrates physics-based models with data-driven and knowledge-based approaches in a unified way to automatically detect and diagnose hardware, software and interface faults is needed.

(iv) *On-line and Off-line Inference Methods:* The development of on-line and off-line inference methods to detect and isolate incipient faults in coupled, heterogeneous, and hierarchical systems with error propagation as well as network delays and losses is needed. In addition, the inference methods should enable the prediction of remaining useful life of (hardware) components based on the inferred failing components and the various tracked paths of degradation. These diagnostic and prognostic procedures are essential for run-time fault detection, isolation, as well as predictive maintenance.

(v) *Sensor Suite and Redundancy Optimization:* Automatic fault diagnostic schemes rely on various types of sensors (e.g., temperature, pressure, vibration, etc) to measure the system parameters. High-integrity systems employ physical or functional or analytical redundancy to improve system availability. An optimized sensor and redundancy allocation that maximizes the fault diagnosability and availability, subject to specified weight, volume, power, and cost constraints is required. The D&P modeling framework should be usable at the design stage to optimize sensor suite, redundancy allocation, test designs and to quantify the benefits of diagnostic and prognostics in terms of reduced operating and warranty costs.

(vi) *Adaptation:* The D&P modeling framework should enable the collection of actual fault-error-failure-symptom progression data through on-board and dealership data to evolve the fault models.

IV. Proposed Solution

We formulated an integrated diagnostic process that combines data-driven techniques, graph-based system-level functional dependency models and mathematical/physical models (for components with well-understood dynamics) for fault diagnosis and prognosis of embedded systems. This integrated diagnostic process represents a structured, systems engineering approach that can be employed during all stages of a system life cycle, viz., concept, design, development, production, operations, and training. From a design perspective, it has been well-established that a system must be engineered simultaneously with three design goals in mind: performance, ease of maintenance, and reliability. Ease of maintenance and reliability are improved by performing testability and reliability analysis at the design stage.

Our D&P framework comprises of six major steps: model, monitor, develop and update test procedures, inference, adaptive learning, and prediction. In the **modeling step**, failure behavior analysis techniques and actual failure progression data (from test vehicles, engineering data, field maintenance data, dealership repair logs, and expert knowledge) are used to understand fault-error-failure-symptom characteristics of hardware, software and HW/SW interfaces. In the **monitoring step**, the efficacies of measurable variables in hardware and software are systematically evaluated and quantified to ensure that adequate diagnosis and prognosis are achievable via testability optimization algorithms. In the **develop test procedures** step, test procedures that detect failures, or onsets thereof, are developed to minimize false alarms, while improving their detection capability (power of the test and detection delays). The procedures should have the capability to detect trends and degradation, assess the severity of hardware failures for early warning and ensure system's recovery actions effectively in the event of a failure. In the **adaptive learning** step, the model is evolved to correspond to actual failure progression data observed in test vehicles, onboard data and dealership data. In the **inference** step, the fault-test dependencies are used to evaluate the health of the embedded system; the inference algorithms can be embedded in the ECU and/or a diagnostic maintenance computer for real-time maintenance, or downloaded to a service facility to assist repair personnel in rapidly identifying replaceable component(s). In the **prediction** step, the remaining useful life (RUL) of components are computed and used for managing parts and the supply chain. Model-based prognostic techniques based on singular perturbation methods of control theory, coupled with an interacting multiple model (IMM) estimator, provide a systematic method to estimate the RUL of vehicle components. The functional dependency model enables us to generate model-based failure modes, effects and criticality analysis (FMECA) and conduct testability analysis (viz., fault detection, isolation, ambiguity groups, and detection and isolation delays). If the results of the analysis are not satisfactory, additional and/or improved test procedures are designed to improve the diagnostic metrics, thus improving vehicle performance and avoiding costly recalls.

V. Promising Applications

The integrated D&P framework provides a systematic and repeatable process for effective monitoring of embedded systems via online/remote diagnosis and system recovery actions for “fail-safe” operation. This ensures customer safety, and helps realize high-integrity systems that provide early detection/early warning of problems for improved customer satisfaction and reduced warranty and maintenance costs.

BIOGRAPHICAL SKETCHES

Dr. Krishna Pattipati is a Professor in the Dept. of ECE at the University of Connecticut. He has over 28 years of industrial and academic experience in supervising and performing research on a variety of problems including automated diagnostics and prognostics, adaptive organizations, large-scale mixed-integer optimization, multi-target tracking, and machine learning. He is a Fellow of IEEE. {krishna@engr.uconn.edu, *Ph*: (860) 486 2890}

Ms. Chaitanya Sankavaram is currently a PhD student at the University of Connecticut. Her research interests include fault diagnosis and prognosis, reliability theory, data mining and optimization. {chaitanya@engr.uconn.edu}

Dr. Bing Wang is an Assistant Professor in the Dept. of CSE at the University of Connecticut. Her research interests include computer networks, distributed systems, and network diagnostics. {bing@engr.uconn.edu}

Dr. Yilu Zhang is a Senior Researcher at GM Corporation. His research interests include onboard/remote diagnosis and prognosis technologies; machine learning and data mining. {yilu.zhang@gm.com}

Dr. Mark Howell is a Staff Researcher at GM Corporation. His research interests include vehicle health management, diagnostics and prognostics, intelligent control and systems optimization. {mark.howell@gm.com}

Dr. Mutasim Salman is a Group Manager at GM Corporation. His research interests include vehicle health management, diagnostics and prognostics, vehicle dynamics. {mutasim.a.salman@gm.com}