Towards a unified x-by-wire solution with HUMS, HM & TTP: Lessons learned in implementing it to a drive-by-wire vehicle

John Melentis, Elias Stipidis, Periklis Charchalakis, Falah Ali

Towards a unified x-by-wire solution with HUMS, HM & TTP: Lessons learned in implementing it to a drive-by-wire vehicle

John Melentis Elias Stipidis Periklis Charchalakis Falah Ali
Vetronics Research Centre
University of Sussex
Brighton, UK BN1 9QT
Corresponding author: j.melentis@sussex.ac.uk

Abstract

Requirements for safer automotive control systems are ever-increasing, with issues such as safety-related systems, innovations, and cost reduction. Using Health and Usage Monitoring Systems (HUMS), Health Management (HM) techniques, and the Time Triggered Protocol (TTP), a Throttle-by-Wire (TbW) system was designed to gain experience in establishing a unified approach in integrating safety-related technologies. HUMS are used in aviation to reduce maintenance costs, and HM enables autonomous health management capability for vehicles. TTP is a safety-critical network, designed specifically to meet requirements for fault-tolerant systems. A TbW system replaces the mechanical connection in a vehicle, from the accelerator pedal to the engine throttle, with an electromechanical counterpart. This paper provides an insight in implementing these three technologies to a safety-critical system, and constructing such a system during the design and implementation phase.

1. Introduction

Traditional vehicle control systems based on mechanical parts are required to have robustness and safety-critical properties (designed to endure many years of operational life without failures). It follows that such parts have high manufacturing costs, require mechanical adjustments & tuning, and have to pass stringent safety-criticality tests.

For example, in a typical rack and pinion steering system, the designer provides a static and predefined steering ratio between the displacement of the steering column, and the final rotation angle of the wheels. This ratio would remain static for the operational life of the vehicle. This scenario, whist proven cheap and functional, is not necessarily efficient, since the various usages and driving profiles of the vehicle (different road conditions, loads, tyre wear, and combinations of these) should dictate a different steering ratio for the vehicle to optimally negotiate a turn.

In addition, requirements have arisen for transferring large volumes of data between automotive Electronic Control Units (ECUs) because there is a trend for more electronic vehicles.

This trend is attributed to the multitude of data required in a modern vehicle, which can be classified accordingly as: vehicle information systems (onboard computers, diagnostics and monitoring, navigation systems), driver information systems (modern dashboard and ancillary instruments to replace the analogue gauges), and onboard active / passive safety and driver convenience systems [2].

In addition, the emerging drivetrain technologies for alternatively powered vehicles such as hybrids and electric vehicles require additional real-time control due to the diversity of their designs.

Last but not least, there are ever-increasing dependability requirements in the automotive industry, [3] towards an integrated vehicle heath management (IVHM) system [12].

Consequently, high bandwidth and high safety-integrity networks that can adapt their controlling subsystems in real-time with health management features are required to accommodate present and future demands.

A recommended technology that does meet these requirements presently is TTP. TTP is safety-critical, fast, with health management features, and is fit for use in the automotive area.

This paper is organised as follows. In section 2, the HUMS principles are described along with the time triggered protocol, and their possible health management amalgamation towards IVHM. In section 3, a case study of a throttle by wire system is shown that illustrates these concepts and finally the paper concludes with the case study and the lessons learned.

2. HUMS, TTP and HM

An approach towards safer automotive control systems is the HUMS and HM, with TTP as the enabling technology. DEF STAN 00-970 "Design and Airworthiness Requirements for Service Aircraft" states that "the purpose of HUMS is to improve flight safety, rotorcraft availability, maintainability, the ability to complete mission, and to reduce life-costs" [7].

HUMS is a combination of sensors, data acquisition technologies, and software algorithms (both on-board and off board) that are provided as a unit with the goals of reducing maintenance costs and improving safety.

HUMSs originally were developed for use in helicopters, by the UK Ministry of Defence (MOD) in the 1990s, in collaboration with Shell Aviation and UK Civil Aviation Authority (CAA).

One might wonder the reasons in using such an aerospace system in the automotive world, where safety, innovations, emissions, and costs are the industry drivers [10]. The motivation behind using HUMS & HM is (but not limited to0):

- Determine component failures more reliably.
- Predict part faults & failures.
- Migrate to Condition-Based Maintenance (CBM) in contrast to traditional scheduled maintenance (E.g. replace the oil filter because it is worn and not because the manufacturer suggests to do so every X miles). BMW and Mini already implement CBM in new commercial vehicles, called condition based service [11].
- It is common business and engineering practise. For instance, Boeing, the aircraft manufacturing giant, produced the Anti-lock Brake System, more commonly known as the ABS, in 1947, for use in the landing gear braking systems of the commercial airliners [9].

TTP is used as a distributed, safety-critical fault-tolerant control network for use mainly in avionics and vetronics. TTP is a highly deterministic network and focuses on the interconnection of components in order to form a highly dependable real-time system that is sufficient for critical applications such as X-by-wire in the vetronics (vehicle electronics) and avionics areas. TTP refers to the SAE's class-C classification for fault-tolerant, high-speed networks.

TTP is the core of the Time Triggered Architecture (TTA) which was developed at the Technical University of Vienna and is implemented commercially by TTTech [4], [5].

TTP has a primary distinction to other similar networks; it was designed specifically to meet requirements for fault-tolerant systems. In contrast to traditional automotive networks, which are event-triggered, TTP is time-triggered. All messages within a TTP system are broadcasted through the network according to a predefined static schedule, each time utilising the full bandwidth of the bus, and are neither prioritised nor prone to collisions. Hence, TTP is predictable and is highly suitable for safety related applications [6].

The time triggered protocol is implemented by a TTP communications controller in different hardware architectures, such as Infineon C167 and Freescale MPC555 Central Processing Units (CPU).

HUMS and TTP can work together, to provide a safer control environment that exemplifies the vehicle's 'health management'.

In a simplified example, a vehicular throttle/accelerator control system consists of three sensors, in a throttle by wire system. The sensors are the setpoint generator (input or pedal sensor), the engine RPM sensor, and a throttle position sensor. Data is collected in a healthy usage scenario when the system is operating optimally. Then, a model can be constructed with the normal driving profile of the vehicle. Any exceedances from the normal driving parameters can be used to detect faults. With some intelligent logic, one can design a system that would detect a faulty sensor. An example is shown below in Figure 1.

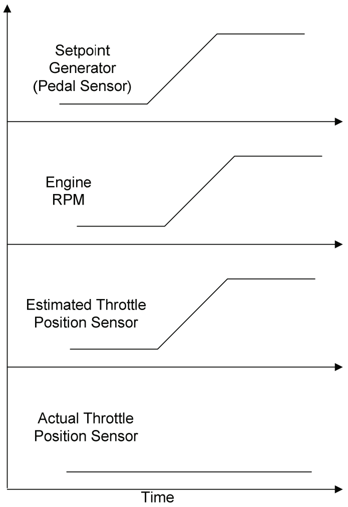

Figure 1: The detection of a faulty sensor based on usage data

In the figure, the pedal sensor has been changed, causing a similar change to the engine, as measured by the RPM sensor. However, the actual or measured throttle position sensor has not been moved as expected (from the model usage data); this error is usually an a) error in the throttle sensor itself, b) the wiring between the sensor and the receiving ECU or c) the analog to digital converter (ADC) module of the ECU, since in order to increase the engine RPM the throttle position must have been changed.

Note that in this concept, it is possible to sense faults that previously were not viable for detection. This can be shown by considering an example where the throttle position sensor to be electrically connected in the appropriate manner, but mechanically disconnected from the throttle valve. In a traditional system, the electrical connection of the sensor is considered to be the system boundary, since it is impossible to detect a mechanical error (unless one further increases the system complexity by adding either mechanical backups or additional sensors). Although one may monitor the electrical connection of the throttle position sensor for voltage and current levels, the actual mechanical connection to the throttle valve itself is assumed to be rigid and cannot be monitored; the system would perceive a mechanically disconnected sensor as a healthy one. By weighing the actual data the sensor provides, against the data provided by a usage model, that a mechanical error can be detected.

Moreover, by adding active intervention routines to the algorithms, the designer works towards a system that meets the requirements in intelligent Integrated Vehicle Health Management (IVHM) [12].

An example that illustrates the active intervention concept is shown in the next section, in a case study for a throttle by wire system.

3. Case Study: HUMS and HM implemented in TTP, for a Throttle by Wire (TbW) System

3.1. General description

A TbW system has been implemented in an off-road vehicle that originally used a traditional control system for acceleration. The system consists of a driver setpoint generator (accelerator position sensor), two ECUs, the actuators that control the throttle valve, and a feedback sensor, as shown in Figure 2.

TTP was implemented to facilitate communications for the overall system. A main attribute of the TTP is the access scheme to the bus. This is known as the Time Division Multiple Access (TDMA). Each node is allowed to send messages only during a predetermined time span, which is called TDMA or Node Slot. Every node is permitted in sequence to periodically utilize the full transmission capacity of the bus, until the process is restarted. A 2400 μs TDMA cycle was selected, in order for the system to react fast enough to excitations.

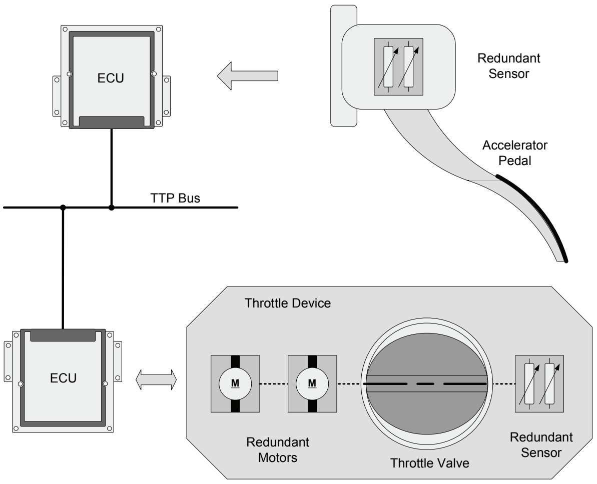

Figure 2: The Hardware Architecture of the TbW

In the figure, the accelerator pedal is connected to a dual-redundant sensor (potentiometer), connected to an ECU. That ECU is the TTC200 from TTTech [5], which is based on the Freescale MPC555 CPU. The ADC of the ECU translates the driver's setpoint value to a digitised signal. The signal is then processed and broadcasted as a TTP message to the TTP network.

Another ECU (TTC200) receives this signal and processes it, and translates it to a PWM value that rotates the redundant motors. The motors are mechanically connected to the throttle valve, which controls the engine Revolutions per Minute (RPM). A throttle valve position sensor provides feedback to the ECU.

The ECUs themselves are not replicated because the system is an alpha version and is work-in-progress. Since each TTC200 contains an internal watchdog that monitors and safeguards the power stages, the non-redundancy in this stage of development does not have dramatic effects. As shown in the next section, Health Monitoring and Management strategies provide additional robustness and reliability.

3.2. Application-level Health Monitoring and Management (HM&M)

On top of the TTP built-in health monitoring and redundancy management [12], extra health management policies were implemented. These were the additional monitoring & diagnostics, error codes and active intervention. Monitoring routines were designed to detect various errors and exceedances (in the HUMS domain, exceedance is defined as the departure from a predefined and usually static range of readings, which has already been established by usage systems) from normal operating profile. Error codes are effectively the results of the monitoring & diagnostics, produced as a TTP message that is broadcasted to every node in the network. Active intervention occurs when the error codes depict that there is a problem with a system component. This triggers a response, and the system takes preventive measures to reduce the effect of the failure.

These policies can be shown for the throttle by wire system, as shown in a basic Fault Tree Analysis (FTA) for the setpoint generator in Figure 3.

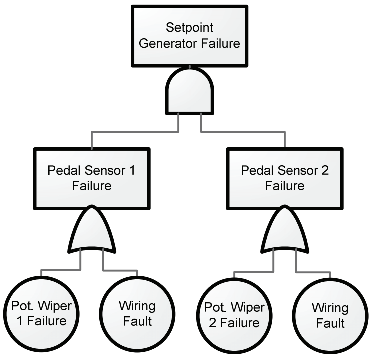

Figure 3: The FTA for the pedal sensor

In the figure, the setpoint generator consists of two redundant potentiometers. In order for the setpoint generator to fail, both sensors must fail, as indicated by the logical 'AND' gate. Moving one level down, a single pedal sensor failure can occur from a potentiometer wiper failure, or a wiring fault, shown with the logical 'OR' gate.

In the pedal sensor ECU, the health monitoring & management algorithms, shown in Figure 4, would detect the fault by either as a disagreement in values with the other (healthy) pedal sensor, or as an exceedance from the normal parameters (e.g. the operating range in voltage).

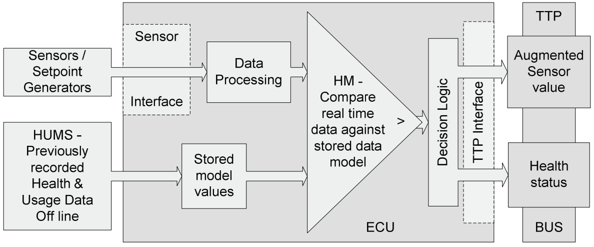
Sensor
Interface
Sensors / Setpoint Generators
Data Processing
HM - Compare real time data against stored data model
>
Decision Logic
TTP Interface
TTP
Augmented Sensor value
Health status
BUS
HUMS - Previously recorded Health & Usage Data Off line
Stored model values
ECU

Figure 4: The Pedal Sensor ECU Health Monitoring and Management

In either case, the error is classified, and assigned a predefined error code. According to that error code, the active intervention routine then isolates the faulty sensor from the rest of the system while the error code is then broadcasted in the TTP network as a TTP message.

In case of a total setpoint generator failure, when both pedal sensors are inoperative, the pedal sensor ECU intervenes and isolates both sensors, transmitting a continuous 'idle' value, as well as transmitting an error code, which is different from the single fault error code.

The same policies are applied in the actuator ECU heath management as shown in Figure 5.

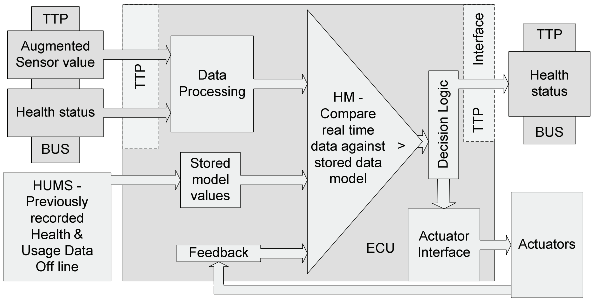

Figure 5: The Actuator ECU HM&M

Each motor that controls the throttle valve have several failure modes: the motor can be stuck to a specific setting, the motor can move freely without any power, or it moves uncontrollably.

The monitoring in this case is the current measurement in the power cables connected to the nodes. The algorithms are designed to detect too much current (motor stuck or motor tries to move uncontrollably and would try to fight the healthy motor which is mechanically connected to it) or too little current (no power). The detection thresholds are again defined by usage systems. Error codes detect the various failure modes a motor would have. Active intervention occurs in these failures, by switching the motor off, which allows it to be rotated freely by the healthy motor. Since the healthy motor is then responsible for rotating the throttle valve, the malfunctioning motor, and the throttle valve position sensor, its current requirement would be roughly doubled; this must be taken into account so that the detection threshold changes and does not disable the healthy motor.

3.3. Testing, Results & Discussion

The testing methodology is based on the TTP bus monitoring software, the TTP-View. Information from the TTP Bus is shown to the PC via the TTP Monitoring Node (a TTP to Ethernet interface) using an

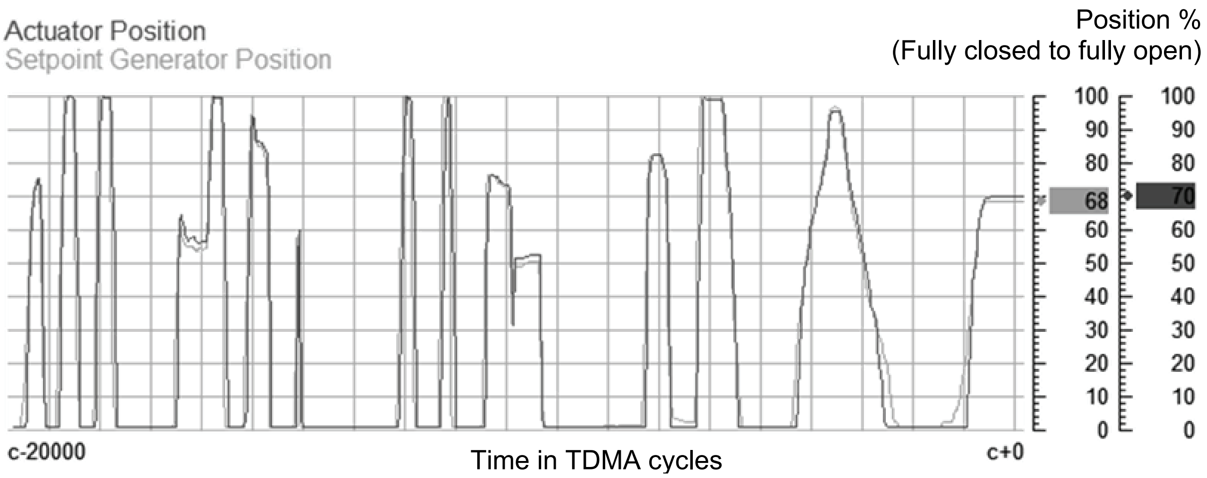

Figure 6: Error between the setpoint generator and the throttle valve position

Ethernet connection. The monitoring data is recorded and saved as a file, which the developer can then playback in a similar fashion to a video tape recording.

In Figure 6, one can see the setpoint generator position compared to a throttle valve position; in the control system domain this is known as the 'error' [13].

The vertical axis describes the setpoint generator and throttle valve position as a percentage between the two extremes (i.e. idle and full throttle), and the horizontal axis describes time in TDMA cycles, with the leftmost reading being the oldest (20000TDMA cycles*2400µs/TDMA cycle = 48 seconds) and the righthand reading is the most recent. The horizontal grid is also set to 1000 TDMA cycles.

It is evident that the closer the throttle valve position (darker line) is to the setpoint generator (lighter line) the better the design is, and the faster the system response is.

A fault injection scheme was then applied. It follows that the health management strategies mentioned in section 3.2 are applied here. One scenario is to physically remove the pedal sensors. This is shown in Figure 7.

In the figure, an extra data set is introduced; this is the error code, which scales from zero to 3 and has the darkest colour. Zero stands for 'full health' mode, 1 and 2 that there is a problem with one of the 2 sensors, and 3 for total sensor failure.

Depending on the error code, the system responds accordingly. In the first 5000 TDMA cycles (from the leftmost side until point "A") the system is healthy, as depicted by the darkest line being zero. Then, in the time frame between 5000 cycles to 15800 (point "A" to point "B"), the system detects the pedal sensor 1 to have failed; this is shown by the darkest line having the error code of '1'. As one can see, this has no effect

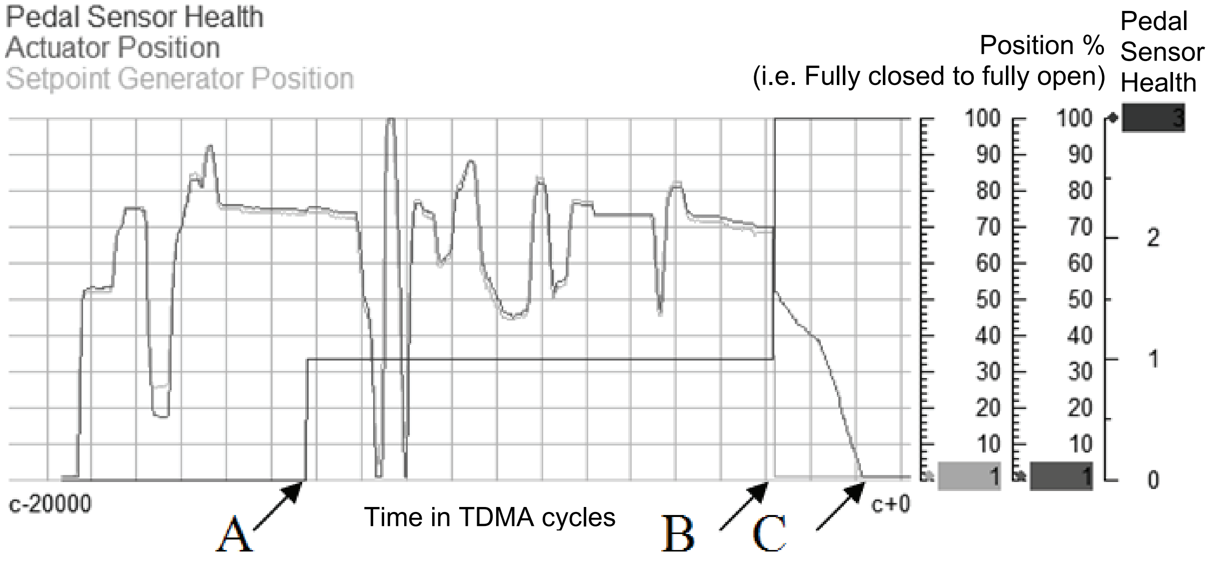

Figure 7: Error Codes

on the functionality of the system, since the redundant pedal sensor is used for input, autonomously.

The crew is alerted of the failure, and the faulty sensor is isolated from the rest of the system until the problem is fixed. The isolation is necessary in order to prevent the faulty sensor from propagating erroneous measurements through the entire system. This could happen for example if the wiring between the faulty sensor and the ECU breaks, but it could still contact and become a short circuit while the vehicle crosses a road bump.

However if both sensors fail (from 15800 TDMA cycles onwards – point “B”), the error code becomes ‘3’ and the setpoint generator immediately returns to the ‘0’ or idle position, as indicated by the lighter line in the proximity of point “B”. The actuator position (medium dark line) promptly returns to the idle position, shown in “C”. This provides a ‘limp home’ capability to the vehicle. The interval between the total sensor failure and recovery in limp mode (time between point ‘B’ and point ‘C’) is 1956 TDMA cycles, or 1956*2400us = 4.70 seconds, and exaggerated for effect.

This case study describes one simple fault of many fault scenarios that could take place in such a system; there are obviously many more that are addressed, as this is work in progress.

4. Lessons Learned and Conclusion

This paper discusses the challenges and techniques of bringing three different technologies together towards a safer system. When working in a safety-related application such as a throttle by wire system, a level of safety measures must be defined in the early stages & applied through the lifecycle of the project. This will increase the overall safety integrity of the system.

However this is not always possible, since requirements & specifications could change, software is updated and functions differently, or the system developer is required to make a change because of external factors. It is very important at that time to compare the new system against the safety measures that were originally taken, and analyze whether the system is adversely affected.

HM&M algorithms have to be an integral part of the design process, otherwise simulations and tests could provide unexpected results. For example, if a wire is physically disconnected from a sensor, the developer could detect this early by diagnostics on in the design phase, instead of trying to find solutions to a problem that otherwise could be masqueraded as a mechanical connection fault between a pedal and a sensor.

By introducing error codes to the HM&M routines, a problem can be immediately traced and resolved. In the design phase, the developer tabulates the error codes with a probable cause of the problem. The developer should opt for producing as many distinctive faults or problems and combinations of these as possible. Then the error codes should be broadcasted to the control network so that all affected nodes are aware of this.

This could be further extended by using these error codes to provide solutions in real-time. This presumes that each problem is carefully tested and the remedy is stress-tested under various conditions, depending on the criticality of the problem and the impact on the affected system. Obviously the solution must be rapid in order to reduce impact on the system.

Keeping a simple system with excellent documentation and comments allow for traceability in the system; for example, when the project is paused for a period of time and the recommenced, or when the specifications change.

One can analyse the principles used in other industries, such as the HUMS and HM and provide these concepts in the application layer, by means of monitoring & diagnostics, error codes and active intervention techniques. Additionally by utilising TTP, a rigid communications protocol as the enabling technology, one can add additional robustness, reduce maintenance costs, and introduce new innovations. The proposed solution is a first step in fulfilling an integrated and unified solution in the automotive industry.

5. Acknowledgements

This work is supported by QinetiQ & TTTech.

6. Disclaimer

This paper refers to a hardware and software architecture that remain under development. Results presented herein do not reflect normal performance of these technologies and their respective development kits used.

7. References

[1] Schauffele J, Zuranka T, *Automotive Software Engineering – Principles, Processes, Methods, and Tools*, 2005, USA, SAE

[2] Robert Bosch Gmbh, *Automotive Handbook*, 7th ed., BentleyPublishers, USA, 2007

[3] P. Johannessen, F. Törner, and J. Tornin, *Lessons Learned from Model Based Development of a Dependable Control-by-Wire System*, ICM '04. Proceedings of the IEEE International Conference on Mechatronics, 2004.

[4] Rushby, J; *Bus architectures for safety-critical embedded systems,* EMSOFT 2001: First workshop on embedded systems, Lake Tahoe CA.

[5] TTTech Computertechnik AG, TTTech's website is at http://www.tttech.com

[6] Stöger, G, *What are Time-Triggered Architectures?*, Presented at Ultra Electronics Electrics / TTTech TTA Symposium, Cheltenham, UK, 2008

[7] MoD, *Defence Standard 00-970: Design and Airworthiness Requirements for Service Aircraft*. 2003.

[8] Birch S, Looking, Listening, Recording, Analysing, *SAE Aerospace engineering & manufacturing magazine,* SAE USA, April 2008, pp. 42–45.

[9] Altrock, C., "Fuzzy Logic in Automotive Engineering", *The Computer Application Journal*, Circuit Cellar INK, Issue 88 November 1997 pp. 12-21.

[10] Robert Bosch GmbH, *Automotive Electrics Automotive Electronics – Systems and Components*, 5th ed., BentleyPublishers, USA, 2007

[11] BMW Condition Based Service Website: http://www.bmw.com/com/en/owners/service/serviceinclusive_cbs.html

[12] M. Jakovljevic, and M. Artner, "Protocol-Level System Health Monitoring and Redundancy Management for Integrated Vehicle Health Management", *25th Digital Avionics Systems Conference*, 2006 IEEE/AIAA.

[13] N.S. Nise, *Control Systems Engineering*, The Benjamin/Cummings Publishing Company, USA, 1992, p19.