Possible case studies for SoftFMEA

Jon Bell

Doc. ref. SD/TR/EX/01: January 17, 2003

1 Introduction

This report sets out to list potentially interesting case study or example systems for SoftFMEA. It is divided into a (brief) section for each system identified. Each system will have details of why it is interesting, what information we have about it, and what else we might need. There will follow a brief commentary on the system, where applicable.

There is an earlier report on case studies [4], but that report has more discussion than this, and is also more centred on CANbus systems. The two reports can, to some extent be regarded as complementary, but this one is more appropriate for the current direction of the project in that it proposes systems of interest because of their complex behaviour and function. I have included the systems from the earlier report here, for completeness, but without the discussion.

In cases where we have no models of these systems, this will be indicated. In these cases, it would obviously be preferable to get an actual example, but we might well be able to manage with a "home made" version. I have not included copies of schematics to keep the report to a reasonable size.

NOTE: At present we have no licence for Transcable, so I cannot provide a detailed breakdown of the models we have for some of these systems.

2 The case studies

This section lists each example system, in no particular order. Each system is in its own subsection, starting with a brief summary of why it is interesting followed by a note of what we have and what we need. These are followed by a short commentary. I have not entered different versions of similar systems individually, so there is only one section for a simple lighting system, for example, despite the fact that we have several version of the system, and different variations on the theme. Where this is the case, this will be made clear.

2.1 Simple lighting

We have several variations here. These have not been detailed separately.

Why: Simplicity allows study of bus support with few distractions.

What we have: Jaguar schematics (on paper) for front and rear lamps using SCP. Various example systems in AutoSteve, with different approaches to

modelling message passing. These include passing events and signals and also using the built in bus support in AutoSteve version 2.6.

What we need: More study of example systems.

Comments: These are developments of the long standing headlamps example complicated by the use of a bus and in some cases by a sensor triggering automatic switching on of dipped headlamps. This is taken from the Jaguar example, but the behaviour may not match that example as we have no behavioural model for the system. The example systems use a toggle switch as a dip switch. This complicates the system behaviour, as required system output cannot be mapped directly to input properties — switch positions. The sensor allows modelling of message conflicts and priorities as the system has two transmitters. A simple version of this system is discussed in [4] and has also been used as a example in [3]. The system was also used to illustrate the need to distinguish between sending events and sending signals between state charts, in [1]. The Jaguar systems differ from the AutoSteve system in how they use relays and control ECUs. As we have no state charts, the interaction of the "autolamp sensor" is unclear. We have a version of the simple lighting system that includes tail lamps and brake lamps to model broadcasting of CAN messages. The Jaguar systems appear to use different values of resistance and a voltage detector to find the switch position. This, of course, makes correct modelling of the system impossible with a three valued (or indeed an order of magnitude) qualitative circuit analyser. Modelling the different voltages using messages could sidestep this problem, but is not really a correct solution.

2.2 Simple heater circuit

The simplest system we could come up with that includes feedback.

Why: Shows up importance for modelling of having sensor send data, not instructions. Raises questions about modelling closed loop systems and feedback, but these questions are not being pursued.

What we have: Our own example system in Transcable/AutoSteve.

What we need: A genuine example of a (simple!) system with feedback would be interesting, but as we do not propose to pursue these questions, it is not a priority.

Comments: When systems incorporate sensors, the possibility of the system incorporating feedback is raised. The earlier case studies report [4] introduces a simple space heater circuit that looks to be as simple a system as we can model with feedback. However, it is not intended to pursue the questions that arise from this, discussed in [2]. It is probably the case that we have got most of what we want from this system. The questions that arose from it were discussed at some length in [2]. The system itself is described in [4].

2.3 Belt minder

This system was obtained for Dougal from Ford. It gives a warning if the driver sets off without seat belts being buckled.

Why: Correct fulfilment of system function depends on complex behaviour. Complex behaviours in some components. Significance of timing of input events.

What we have: Ford's Statemate behavioural model of the system, on paper. Ford schematic of restraint control system, of which Belt Minder is a part, also only on paper. I have made a simplified schematic derived from the Ford one, in Transcable, and an AutoSteve model of some of the system's functionality.

What we need: More complete functional model of the system. This, however, is up to me.

Comments: This system has been very useful in examining complex behaviour and function. The warning function depends on a chimer sounding intermittently for a set period. There is a need for more examination of how well this can be modelled in AQQA. There is a facility to allow the driver to temporarily disable the system by buckling and unbuckling his seat belt within a preset time. This means we need more expressiveness in the FMEA scenario, to capture the time between successive input events. The belt minder system has also been important in encouraging the change of emphasis in the project from CAN support to a more general examination of behavioural and functional complexity.

2.4 Wash / wipe

Why: Complex functional modelling, specifically non-continuous output (intermittent wipe) and functions with no active system output — difference between "park" and merely "off".

What we have: Half drawn Transcable schematic of example system using a bus. I think there may be old AutoSteve models of a wash / wipe system.

What we need: A real example system (schematic and behavioural models of the more complex components).

Comments: Wash / wipe systems seem to raise some quite interesting questions regarding system function. Is there a need for a "parked" function, distinct from the system being off? If so does it really have a system level output, or does it map to a state? How complex is it to model the intermittent wipe function? What effect does this function have on modelling of time? Work started on an example system, but stopped, partly because of problems modelling parking. It seems well worth re-starting work on this system. This model system will, of course, be more realistic if we have actual case studies to use as a pattern.

2.5 Central locking

We have different versions of central locking examples.

Why: Test significance of inputs while in transitional functional states (such as "locking" and "unlocking"). Possible modelling of message passing and interruptions. Significance of temporal modelling in these transitional states.

What we have: Jaguar schematic for a central locking system using SCP. Old AutoSteve model of a central locking system, both schematic and behavioural models. Edel Sherratt also has a version of our central locking system modelled using state charts and block diagrams in SDL.

What we need: Real behavioural model (and matching schematic) would be nice.

Comments: Probably the main activity here should be for me to become more familiar with how they work. It should be possible to devise a suitable behavioural model using the Jaguar schematic and the existing AutoSteve (and / or SDL) models. Some interest attaches as we need to model the effects of new inputs interrupting the system while it is in a state such as locking, rather than a resting state, such as locked. There is also the possibility of modelling messages from different transmitters, if we find (or devise) a system where both the driver's and passenger's doors can trigger locking, but the passenger door only unlocks itself, not the whole car. Is this a realistic functional model of central locking? Correct behavioural modelling of messages interrupting a moving state might entail some quite elaborate state charts.

2.6 Restraint control

This might be of interest as a relatively simple system where time is critical.

Why: Possible problems with late fulfilment of function.

What we have: A schematic from Ford for a Restraint Control system that we have because of its including belt minder (Section 2.3).

What we need: Behavioural and functional models.

Comments: The interest in this is somewhat speculative, but it seems possible that a restraint control system might have one or two interesting features while being relatively simple. The most obvious of these is the idea that it must fire quickly, so late fulfilment of a function might be important. It is not clear how complex these systems are. It might be the case that they are actually too simple for SoftFMEA; in other words, that they could be modelled in AutoSteve as it stands.

2.7 Other possible systems

It is the case that all the systems listed here are "accessory" systems, whereas one of the trends in the automotive sector is to use software and network components in control systems such as engine management and anti-lock brakes

(ABS). This trend is continuing with investigations into and development of "drive by wire" systems. Should SoftFMEA be looking into such systems? It is, I suggest, clear that they raise additional questions regarding speed of operation, reliability and fault mitigation. These questions are briefly discussed below, in Section 3.

The difficulty is getting hold of examples. David Ward promised to try to get us some systems for drive by wire systems, but we've not heard from him for some time.

3 Requirements for example systems

In this section I shall briefly list some system features that it would be interesting to find examples of. I have not yet identified definite example systems for these, although some possible examples are included in Section 2 This might be worth raising at a meeting with industrial partners.

- Systems in which ordering of incoming data is significant, with the intention of trying to model effects of some incoming data being delayed.
- Systems with fault tolerant behaviour incorporated. We wish to investigate whether it is useful or important to distinguish between functions achieved "normally" and similar functions achieved through fault mitigation.
- Time critical systems that use a bus, to establish interest in late achievement of functions. For example a late message in an engine management system will presumably mean re-use of earlier information. At what point does this become critical? Is a default setting used rather than an old reading?
- Mixed domain systems (such as ABS?) to look at behavioural interactions between domains. It also might be interesting to look at this in relation to splitting systems into subsystems. It suggests another alternative to either a split along functional lines or by proximity of components.
- Different systems that use the same sensors. This raises the possibility of the sensor subsystem being analysed independently (as it will presumably be electrically self contained) and given its own failure modes, derived from its component failure modes in the analysis. It can then be treated more or less as a component in analysis of the systems that use the sensor data. Possible examples are the traction control and anti-lock braking systems both using wheel rotation sensor data and maybe both restraint control and belt minder wanting to use the seat occupancy detector for the passenger seat.

4 Conclusion

This report as it stands is not complete. We clearly need to identify and obtain examples of suitable systems to match the requirements listed above, in Section 3. Work on the systems we do have models of is currently held up because of the difficulties with our Transcable licence.

References

[1] Jon Bell. Events and signals. SoftFMEA Document ref. SD/TR/FSM/03, 2002.

[2] Jon Bell. The heater circuit - matters arising. SoftFMEA internal report, 2002.

[3] Jon Bell. Proposed approaches to network simulation. SoftFMEA document ref. SD/TR/03, 2002.

[4] Jon Bell. Systems with telematic components. SoftFMEA document ref. SD/TR/02, 2002.