

Safety Aspects on a Micro-Hybrid Vehicle with Manual Gearbox

Armin Müller-Lerwe, Rainer Busch, Thomas Rambow,
Urs Christen, Uwe Gussen and Markus Kees
Ford Motor Company

Copyright © 2008 SAE International

ABSTRACT

The hazard analysis for the Stop-Start control strategy of a Micro-Hybrid vehicle with manual gearbox is presented. The strategy allows for stops in gear and in neutral; this leads to specific hazards. Implications for the architecture of the electronic control unit, the software architecture, and the development process, especially software testing, are discussed.

INTRODUCTION

In Micro-Hybrid vehicles, the engine is usually shut down if no power is required, for instance, while waiting at a traffic light. As soon as power is requested (e.g., by the driver pressing the accelerator pedal or for air conditioning), the engine is automatically restarted. This can be done with a belt-driven integrated starter generator (B-ISG) which is also used to generate electricity during coasting (regenerative braking) and, if needed, during normal operation.

In this paper, we highlight safety considerations for the Stop-Start strategy of diesel powered Micro-Hybrid vehicles with manual transmission. In addition to stopping the engine when the vehicle comes to a standstill in neutral, the engine is also stopped in gear. The ability to stop in gear makes the system more transparent to the driver: there is no need for a change of the driving behavior in order to make use of the engine shut-downs. However, stops in gear can only be done if the engine restart is achieved sufficiently fast and reliable. Moreover, it has implications for the safety analysis, as will be highlighted below.

This paper is organized as follows. The next section describes the Stop-Start functionality. This is followed by the description of the safety analysis process; the safety considerations are presented in the fourth section. Two sections cover the implementation in Simulink/Stateflow and model-based testing of the strategy. The paper concludes with some results measured in a prototype vehicle. In the remainder of this introduction, a system overview is given.

SYSTEM OVERVIEW – Besides a conventional diesel engine, the Micro-Hybrid powertrain comprises the components specific for Stop-Start operation: an electric motor which, depending on the size of the diesel engine, may be operated at conventional board net voltage (12 V) or at higher voltage, an energy storage (batteries or super capacitors), a DC/DC converter which couples the different voltage levels, and a power inverter to drive the electric machine. The electric machine integrates the functions of a starter and a generator and hence is called Integrated Starter Generator (ISG). Figure 1 shows the layout for a belt-driven ISG operated at 24 V.

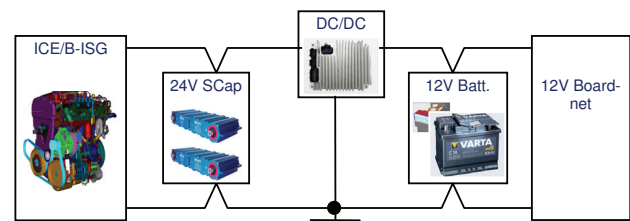


Figure 1 System Layout.

The gearbox considered in this study is not equipped with a dedicated sensor to detect neutral position. Instead, gear neutral is inferred from engine and vehicle speeds.

STOP-START FUNCTIONALITY

In order to improve fuel economy, the engine is stopped automatically whenever no power is required for vehicle propulsion or comfort features (such as air conditioning compressor), and automatically restarted as soon as power is requested. The Stop-Start strategy should be as unobtrusive to the drivers as possible: they should not be forced to behave differently in a vehicle with this strategy than they would in one without.

ENGINE STOP – Only the driver can induce an engine stop by interacting with pedals and the gearbox. For the engine to be stopped, the vehicle speed must be below a certain threshold and the accelerator pedal must be released. If a gear is engaged, the engine is stopped after a small delay. If gear neutral is detected, the engine is

stopped after a possibly different short delay. All this is visualized in Figure 2.

Various stop inhibitors can prevent automatic shutdowns of the engine. For instance, activated air conditioning, reverse gear, or low battery state of charge can be reasons for stop inhibitors, but also an open hood. Moreover, after each engine start, a timer has to expire or the vehicle speed needs to exceed a threshold before the next automatic stop can occur. This is to prevent chattering engine starts and stops.

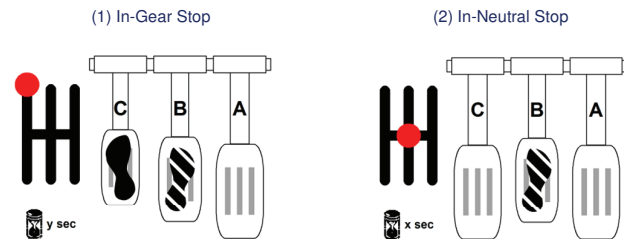


Figure 2 Engine stop conditions

Stop Abortion – A stop which has been triggered is aborted if any start trigger occurs before the engine has come to a stop. In these cases, the ISG is commanded to crank in order to ensure that the engine will continue to run.

Stop abortion is more likely during stops in gear than during stops in neutral. For instance, while waiting at a junction, the engine may begin to shut down when the driver spots a gap in the traffic flow. Pressing the accelerator pedal must restore power delivery by the engine very quickly.

USER INDUCED ENGINE START – User induced starts are directly triggered by driver interactions with the pedals or the gearbox. For the engine to be automatically restarted, the clutch pedal must be depressed – gear neutral cannot be detected if both, the engine speed and the vehicle speed are zero (see below). The following driver actions lead to an engine restart:

- Releasing the brake pedal.
- Pressing the accelerator pedal. This includes the heel-toe start where the brake and the accelerator pedals are pressed at the same time.
- Depressing the clutch pedal if it was released or pressed previously.¹

Figure 3 illustrates these situations.

There are a few start inhibitors which can prevent an automatic restart. For instance, if the battery state of charge is too low, or if the ISG performance is degraded.

¹ There are three states for the clutch pedal: Released, Pressed (the clutch may or may not be open), and Depressed (the clutch is open).

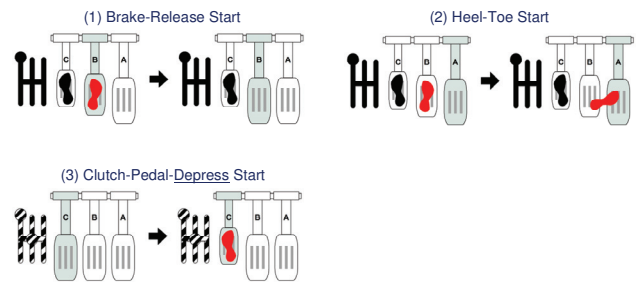


Figure 3 User induced start triggers

SYSTEM INDUCED ENGINE START – Several systems can request an engine restart. System triggers for a restart of the engine include the following:

- activation of air conditioning,
- battery state of charge dropping below a threshold,
- depletion of brake assist vacuum and
- rolling of the vehicle.

As with user induced restarts, any start inhibitor prevents system induced restarts as well.

STALL RECOVERY – If the engine is stalled, the engine can automatically be restarted with the B-ISG. As soon as the driver depresses the clutch (and if no start inhibitor is present), the engine is restarted. Depressing the clutch pedal is a natural reaction when the engine stalls; thus very quickly the engine is running again without the driver having to cycle the key.

ERRORS – Under a few situations, the strategy goes out of operation because a safe restart cannot be guaranteed. When the strategy is out of operation, a key cycle is needed to resume normal operation of the Stop-Start strategy.

VIRTUAL GEAR NEUTRAL SENSOR – Instead of using a dedicated sensor to detect neutral gear, an algorithm has been implemented which determines, based on other sensors, whether the gearbox is in neutral. When the clutch pedal is released, the gearbox has to be in neutral if vehicle speed and engine speed do not match. Conversely, if the clutch pedal is not released or if the two speeds do match (e.g., at standstill of the vehicle and the engine), it is assumed that a gear is engaged because this is, for Stop-Start application, the safe assumption.

CLUSTER INFORMATION – A status signal describes the states of the Stop-Start strategy:

- Stop available
- Stop not available
- Stopped
- Error
- etc.

SAFETY ANALYSIS

The safety process applied to Stop-Start system development is oriented to the international functional safety standard IEC 61508 and covers the whole lifecycle from the concept phase to the decommissioning phase. The safety tasks described in this paper only cover the concept phase.

IEC 61508 [1] is a generic standard. Various industry sectors have derived their own standards, e.g., IEC 51511 for process industry. The automotive industry is working on an automotive specific standard (ISO 26262). Although this is work in progress, we used the ISO WD 26262 [2] part 3 "Concept phase" for the hazard analysis and functional safety concept definition in the Stop-Start system development. This was done to validate the applicability of the risk classification scheme proposed in the working draft.

HAZARD ANALYSIS – For the hazard analysis a two step approach was used. In the first step all hazards associated to the system functions were identified, followed by a second step of classifying those hazards. The core team leading the analysis consisted of two safety experts and one powertrain expert. On request other experts from the chassis, electrical and powertrain areas supported the analysis.

System Functions – The initial step to start the hazard analysis is to identify the system functions as well as the assumptions on the system and application (vehicle). The definition of the functions is done at the "top-level", ignoring detailed system design aspects. We distinguish between primary functions that are essential for the system to achieve its goal and secondary functions that are not necessarily needed and might not be included for a specific application. For the Stop-Start system there are two primary functions: to stop the internal combustion engine and to start the internal combustion engine. It was found to be useful to break down the engine start function into two sub-functions according to the two actuators, the starter device and the engine itself, involved in the start of the engine. Therefore we defined the engine cranking as one sub-function and the engine start as a separate sub-function. The secondary functions are the indication of the system state to the driver and the deactivation/activation of the system by the driver, e.g., via a switch on the dashboard. In general, system functions should be defined as independently as possible from system design and vehicle application. Nevertheless the analysis must be reviewed if the Stop-Start system is used on another vehicle application; but it makes it easier.

System Design Assumptions – Another important step in the analysis is to document the assumptions that it is based on. Even if the system functions are defined independently of the system design and the vehicle application, assumptions about those are necessary for both the identification and classification of the hazards. The

power assisted steering system is an example where the vehicle application is important for the hazard identification. In principle the hazard "Sudden loss of steering assist while driving" can be caused by a Stop-Start system if it commands an engine stop erroneously. The question whether this hazard is applicable for a certain vehicle application depends on the power assisted steering system of the vehicle. If for example hydraulic power assisted steering is fitted where the pump is mechanically driven, the hazard exists; with an electro-hydraulic power assisted steering system that has an electrically driven pump, the hazard does not exist.

An example of the influence of the system design is the hazard "Unintended vehicle acceleration while driving". For this hazard to occur, the cranking device controlled by the Stop-Start system must be able to apply torque to the driveline when the engine is already running. This is obviously the case for a B-ISG system but probably not for systems based on a conventional starter motor because the starter motor disengages mechanically as soon as the engine speed exceeds the speed of the starter device.

Driving Situations – The driving situations that were considered in the Stop-Start hazard analysis were based on a list of situations already used in former analyses. Nevertheless this list was extended before the hazard identification was started to include situations like "vehicle waiting with engine automatically stopped" that are of particular interest for the Stop-Start function. Other situations were added during the hazard identification when identified in the discussions.

Hazard Identification – A useful approach for the hazard identification is to define the possible system behaviors and to analyze the consequences considering the defined driving situations. A HAZOP [3] type approach was used where the system functions were combined with guidewords to define relevant system behavior. The following guidewords are generally considered:

- NO – the expected function is not performed at all or there is no result.
- MORE – the output/result of the function is higher than intended.
- LESS the output/result of the function is lower than intended.
- PART OF – the expected function is only partly performed and the result is incomplete.
- INTERMITTENT – while a function is expected, its output toggles between the expected value and no output.
- EARLY – the function is performed or the result is delivered too early.
- LATE the function is performed or the result is delivered too late.
- REVERSE – the function delivers the opposite of the expected result.
- UNINTENDED – the function is performed or a result is delivered when not appropriate.

Not all of the guidewords are meaningful for every function, therefore only a subset might be applied to a specific system function. For the Stop-Start system functions, eight different functional failure modes are identified. For instance, the combination "engine crank" with "NO" leads to the failure mode "Inability to crank the engine". Note that functional failure modes are not necessarily caused by faults of the Stop-Start system. They also reflect all situations where the system reaction is not adequate, e.g., due to functional limitations. Once all functional failure modes are defined, their possible consequences, at the vehicle level and considering all driving situations, are explored.

Hazard Classification – The hazard classification was performed using the risk classification scheme of the ISO 26262 working draft. With this an automotive safety integrity level (ASIL) was assigned to each identified hazard. The ASIL rating contains four levels going from the least severe ASIL A to the most severe ASIL D. If the risk of a hazard is lower than ASIL A, "QM" is assigned. It means that no further risk reduction besides the normal quality management is necessary. The risk classification itself is based on the three risk parameters *severity*, *exposure*, and *controllability*. In the next sections these parameters are briefly explained and some experiences during the analysis are mentioned.

Severity – The severity classification of the possible consequence of a hazard is divided into four categories, S0 to S3. S0 just includes damage to physical properties (vehicle, environment) whereas S1 to S3 are related to the abbreviated injury scale (AIS) [4] to reflect injuries to human beings.

Since the AIS only considers threat to life but not potential permanent physical disability, there is one hazard, "Exposure to moving parts," that is difficult to rate. The hazard is someone touching rotating parts of the front end accessory drive when the system starts to crank the engine during service or maintenance. A possible consequence could be to lose a finger. Since this injury is not really life threatening, it would not be more than AIS 2 and therefore the severity would be rated S1 according to the ISO scheme. On the other hand all engineers involved in the analysis of the Stop-Start system tend to rate the loss of a finger as S2. To solve this conflict the severity should not only be based on the AIS but also on other rating schemes like IIS [5] or FCI [6] to take permanent disabilities into account.

Exposure – The exposure parameter also has four categories, E1 to E4, corresponding to the frequency of occurrence of a driving situation or the contribution of its duration to the total vehicle operating time (duration). The descriptions are *very low* (E1), *low* (E2), *medium* (E3) and *high* (E4) *probability*. Interpreted in terms of frequency, these categories correspond to situations that occur "less often than once a year" (E1), "a few times a year" (E2), "once a month or more often" (E3) and "almost every drive" (E4). If the exposure needs to be interpreted according to the duration of a situation, they mean

"less than 1%" (E2), "1% to 10%" (E3), and "more than 10%" (E4) of the vehicle operating time. Regarding the duration, E1 is not specified as a percentage of vehicle operating time but includes rare events that last only for a very short time like jump starts etc.

These alternative interpretations are useful if we look whether a failure needs to coincide with a situation or not. For instance, the vehicle might be exposed to a side impact with oncoming traffic if the Stop-Start system commands the engine to stop in a launch situation at a junction. The same situation, vehicle exposed to a side impact with oncoming traffic, could occur if the performance of the starter motor is impaired, e.g., because of insufficient electrical power in the 24V energy storage device, resulting in poor launch performance of the vehicle. This is especially true for Stop-Start functionality with in-gear starts in a vehicle with manual gearbox. Because the drivers control the clutch and expect normal starting times, they will probably engage the clutch before the engine is fully started and therefore begin to launch the vehicle without getting the necessary launch performance. The difference between the two scenarios is the exposure: the erroneous engine stop command needs to coincide with the launch situation to affect the launch performance. The failure due to insufficient power, caused by a wrong charging strategy for instance, could happen at any time and will affect all following engine starts and therefore the launch performance.

Besides this useful differentiation the exposure parameter was found to be the most difficult parameter to rate because there is often no or little data available to support the rating.

Controllability – The controllability parameter distinguishes four categories, *difficult to control or uncontrollable* (C3), *normally controllable* (C2), *simply controllable* (C1) and *controllable in general* (C0). In ISO 26262 the controllability parameter is mainly related to the ability of the driver or other road users to avoid the accident in a hazardous driving situation. This is related to the time the participants have to react and the complexity of the required action. For one of the most critical identified hazards of the stop start system, "Unintended vehicle lurch", the appropriate driver reaction is probably to stop the vehicle movement. This hazard can occur when the Stop-Start system begins to crank the engine while the driveline is closed and torque is transferred to the wheels. The distance the vehicle can move until the driver can react is dependant on the acceleration which itself is determined by the B-ISG performance, vehicle weight etc. This shows that the hazard analysis cannot be completely independent of the system design or vehicle application. Contrary to the situation that supporting data for the exposure rating is difficult and time consuming to collect, tests to support controllability rating can normally be performed during the development. During the Stop-Start hazard analysis, several tests had been specified and performed to support the controllability rating. Figure 4 shows an example: unintended cranking at low speed maneuvering.