
Changes to legislation: There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

ANNEX III

Special requirements to be applied to the safety aspects of complex electronic vehicle control systems

1. General

This Annex defines the special requirements for documentation, fault strategy and verification with respect to the safety aspects of complex electronic vehicle control systems for the purposes of this Regulation.

This Annex may also be applied for safety related functions which are controlled by electronic system(s).

This Annex does not specify the performance criteria for complex electronic vehicles control systems but covers the methodology applied to the design process and the information which must be disclosed to the technical service for type-approval purposes.

That information shall show that a complex electronic vehicle control system respects, under normal and fault conditions, all the appropriate performance requirements set out in this Regulation.

2. Definitions

For the purposes of this Annex, the following definitions shall apply:

- 2.1. ‘*Safety concept*’ means a description of the measures designed into the system, for example within the electronic units, so as to address system integrity and thereby ensure safe operation even in the event of an electrical failure.

The possibility of a fall-back to partial operation or even to a back-up system for vital vehicle functions may be a part of the safety concept.

- 2.2. ‘*Electronic control system*’ means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing.

Such systems, often controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements.

- 2.3. ‘*Complex electronic vehicle control systems*’ mean those electronic control systems which are subject to a hierarchy of control in which a controlled function may be overridden by a higher level electronic control system/function.

- 2.4. ‘*Higher-level control systems/functions*’ mean those systems/functions which employ additional processing and/or sensing provisions to modify vehicle behaviour by commanding variations in the normal function(s) of the vehicle control system.

This allows complex systems to automatically change their objectives with a priority which depends on the sensed circumstances.

- 2.5. ‘*Units*’ mean the smallest divisions of system components covered by this Annex: those combinations of components will be treated as single entities for purposes of identification, analysis or replacement.

- 2.6. ‘*Transmission links*’ mean the means used for inter-connecting distributed units for the purpose of conveying signals, operating data or an energy supply.

Changes to legislation: There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

This equipment is generally electrical but may, in some part, be mechanical, pneumatic, hydraulic or optical.

- 2.7. ‘*Range of control*’ means an output variable corresponding to the range over which the system is likely to exercise control.
- 2.8. ‘*Boundary of functional operation*’ means the boundaries of the external physical limits within which the system is able to maintain control.

3. Documentation

3.1. Requirements

The manufacturer shall provide a documentation package which gives access to the basic design of the complex electronic vehicle control system for which type-approval is applied (hereinafter referred to as ‘the System’) and the means by which it is linked to other vehicle systems or by which it directly controls output variables.

The function(s) of ‘the System’ and the safety concept, as laid down by the manufacturer, shall be explained.

Documentation shall be brief, yet provide evidence that the design and development has had the benefit of expertise from all the system fields which are involved.

For periodic technical inspections, the documentation shall describe how the current operational status of ‘the System’ can be checked.

3.1.1. Documentation shall be made available in the following two parts:

- (a) the formal documentation package for the approval, containing the material listed in Section 3 (with the exception of that of point 3.4.4) which shall be supplied to the technical service at the time of submission of the type-approval application. This will be taken as the basic reference for the verification process set out in point 4;
- (b) additional material and analysis data referred to in point 3.4.4, which shall be retained by the manufacturer, but made open for inspection at the time of type-approval.

3.2. Description of the functions of ‘the System’

A description shall be provided which gives a simple explanation of all the control functions of ‘the System’ and the methods employed to achieve the objectives, including a statement of the mechanism(s) by which control is exercised.

- 3.2.1. A list of all input and sensed variables shall be provided and the working range of these defined.
- 3.2.2. A list of all output variables which are controlled by ‘the System’ shall be provided and an indication given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each such variable shall be defined.
- 3.2.3. Limits defining the boundaries of functional operation shall be stated where appropriate to system performance.
- #### 3.3. System layout and schematics
- 3.3.1. Inventory of components

Changes to legislation: There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

A list shall be provided, collating all the units of ‘the System’ and mentioning the other vehicle systems which are needed to achieve the control function in question.

An outline schematic showing those units in combination shall be provided with both the equipment distribution and the interconnections made clear.

3.3.2. Functions of the units

The function of each unit of ‘the System’ shall be outlined and the signals linking it with other units or with other vehicle systems shall be shown. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.

3.3.3. Interconnections

Interconnections within ‘the System’ shall be shown by a circuit diagram for the electric transmission links, by an optical-fibre diagram for optical links, by a piping diagram for pneumatic or hydraulic transmission equipment and by a simplified diagrammatic layout for mechanical linkages.

3.3.4. Signal flow and priorities

There shall be a clear correspondence between these transmission links and the signals carried between units.

Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety for the purpose of this Regulation.

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware and marking or software output for software content) to provide corresponding hardware and documentation association.

Where functions are combined within a single unit or within a single computer, but shown in multiple blocks in the block diagram for clarity and ease of explanation, only a single hardware identification marking shall be used.

The manufacturer shall, by the use of this identification, affirm that the equipment supplied conforms to the corresponding document.

3.3.5.1. The identification defines the hardware and software version and, where the latter changes such as to alter the function of the unit for the purpose of this Regulation, this identification shall also be changed.

3.4. Safety concept of the manufacturer

3.4.1. The manufacturer shall provide a statement which affirms that the strategy chosen to achieve ‘the System’ objectives will not, under non-fault conditions, prejudice the safe operation of systems which are subject to the provisions of this Regulation.

3.4.2. In respect of software used in ‘the System’, the outline architecture shall be explained and the design methods and tools used shall be identified. The manufacturer shall be prepared, if required, to show evidence of the means by which the realisation of the system logic has been determined during the design and development process.

3.4.3. The manufacturer shall provide the technical authorities with an explanation of the design provisions built into ‘the System’ so as to generate safe operation under fault conditions. Possible design provisions for failure in ‘the System’ are for example:

Changes to legislation: There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

- (a) fall-back to operation using a partial system;
- (b) change-over to a separate back-up system;
- (c) removal of the high level function.

In case of a failure, the driver shall be warned for example by warning signal or message display. When the system is not deactivated by the driver, e.g. by turning the ignition (run) switch to 'off', or by switching off that particular function if a special switch is provided for that purpose, the warning shall be present as long as the fault condition persists.

- 3.4.3.1. If the chosen provision selects a partial performance mode of operation under certain fault conditions, then those conditions shall be stated and the resulting limits of effectiveness defined.
- 3.4.3.2. If the chosen provision selects a second (back-up) means to realise the vehicle control system objective, the principles of the change-over mechanism, the logic and level of redundancy and any built in back-up checking features shall be explained and the resulting limits of back-up effectiveness defined.
- 3.4.3.3. If the chosen provision selects the removal of the higher level function, all the corresponding output control signals associated with this function shall be inhibited, and in such a manner as to limit the transition disturbance.
- 3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave on the occurrence of any one of those specified faults which will have a bearing on vehicle control performance or safety.

This may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) or any similar process appropriate to system safety considerations.

The chosen analytical approach(es) shall be established and maintained by the manufacturer and shall be made open for inspection by the technical service at the time of the type-approval.

- 3.4.4.1. This documentation shall itemise the parameters being monitored and shall set out, for each fault condition of the type referred to in point 3.4.4, the warning signal to be given to the driver and/or to service/technical inspection personnel.

4. Verification and Test

- 4.1. The functional operation of 'the System', as laid out in the documents required in point 3, shall be tested as follows:

- 4.1.1. Verification of the function of 'the System'

As the means of establishing the normal operational levels, verification of the performance of the vehicle system under non-fault conditions shall be conducted against the manufacturer's basic benchmark specification unless this is subject to a specified performance test as part of the approval procedure set out in this Regulation.

- 4.1.2. Verification of the safety concept referred to in point 3.4

The reaction of 'the System' shall, at the discretion of the approval authority, be checked under the influence of a failure in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal faults within the unit.

Changes to legislation: *There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) [View outstanding changes](#)*

The verification results shall correspond with the documented summary of the failure analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate.

Changes to legislation:

There are outstanding changes not yet made to Commission Regulation (EU) No 347/2012. Any changes that have already been made to the legislation appear in the content and are referenced with annotations.

[View outstanding changes](#)

Changes and effects yet to be applied to the whole legislation item and associated provisions

- Signature words omitted by [S.I. 2022/1273 reg. 69\(7\)](#)
- Annex 2 Appendix 1 omitted by [S.I. 2022/1273 reg. 69\(9\)\(g\)](#)
- Annex 2 Appendix 2 footnotes words omitted by [S.I. 2022/1273 reg. 69\(9\)\(h\)](#)
- Art. 1(4) words substituted by [S.I. 2022/1273 reg. 69\(2\)\(b\)](#)
- Art. 1(5) words substituted by [S.I. 2022/1273 reg. 69\(2\)\(b\)](#)
- Art. 2(3) words substituted by [S.I. 2022/1273 reg. 69\(3\)\(b\)](#)
- Art. 3(5)(a) words omitted by [S.I. 2022/1273 reg. 69\(4\)\(e\)\(ii\)\(bb\)](#)
- Art. 3(5)(a) words substituted by [S.I. 2022/1273 reg. 69\(4\)\(e\)\(ii\)\(aa\)](#)
- Art. 3(5)(c) words omitted by [S.I. 2022/1273 reg. 69\(4\)\(e\)\(ii\)\(bb\)](#)
- Art. 3(5)(c) words substituted by [S.I. 2022/1273 reg. 69\(4\)\(e\)\(ii\)\(aa\)](#)