Document Title	Requirements on Synchronized Time-Base Manager
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	420
Document Classification	Auxiliary

Document Version	1.0.0
Document Status	Final
Part of Release	4.0
Revision	1

Document Change History

Date	Version	Changed by	Change Description
30.11.2009	1.0.0	AUTOSAR Administration	Initial Release

Disclaimer

Advice for users

AUTOSAR Specification Documents may contain exemplary items (exemplary reference models, "use cases", and/or references to exemplary technical solutions, devices, processes or software).

Any such exemplary items are contained in the Specification Documents for illustration purposes only, and they themselves are not part of the AUTOSAR Standard. Neither their presence in such Specification Documents, nor any later documentation of AUTOSAR conformance of products actually implementing such exemplary items, imply that intellectual property rights covering such exemplary items are licensed under the same rules as applicable to the AUTOSAR Standard.

Table of Contents

1 Scope of Document

The basic purpose of the Synchronized Time-Base Manager (StbM) is to provide a "global time" to other BSW modules or to the application. Global time means, that different entities within the system have the same definition of time[1]. In the system, multiple "global times" can exist simultaneously (e.g. the FlexRay time definition, the TTCAN time definition …). It is the task of the Synchronized Time-Base Manager to access those global times (e.g. by calling the FlexRay Interface) and providing them to the customers.
In the following, required terms and definitions are described which are important for the later chapters.

1.1 Overview

1.1.1 Synchronized Time-Base Manager as broker

Basically, the Synchronized Time-Base Manager is interacting with two different roles, as Figure 1 shows:

1) **Provider**
   The StbM requires information from other modules (e.g. receiving the global time defined by the FlexRay Interface). So far, the *provider* has the task to deliver a "synchronized time-base".

2) **Customer**
   The StbM collects information about time. This functionality can be used by several *customers*: either other BSW modules or application SW-Cs.

[1] Definition of time: Each system node has its own definition of time (time-base). When several nodes have the same definition of time, then we denote this as "synchronized time-base". In the following, the terms "definition of time" and "time-base" are used equivalently.

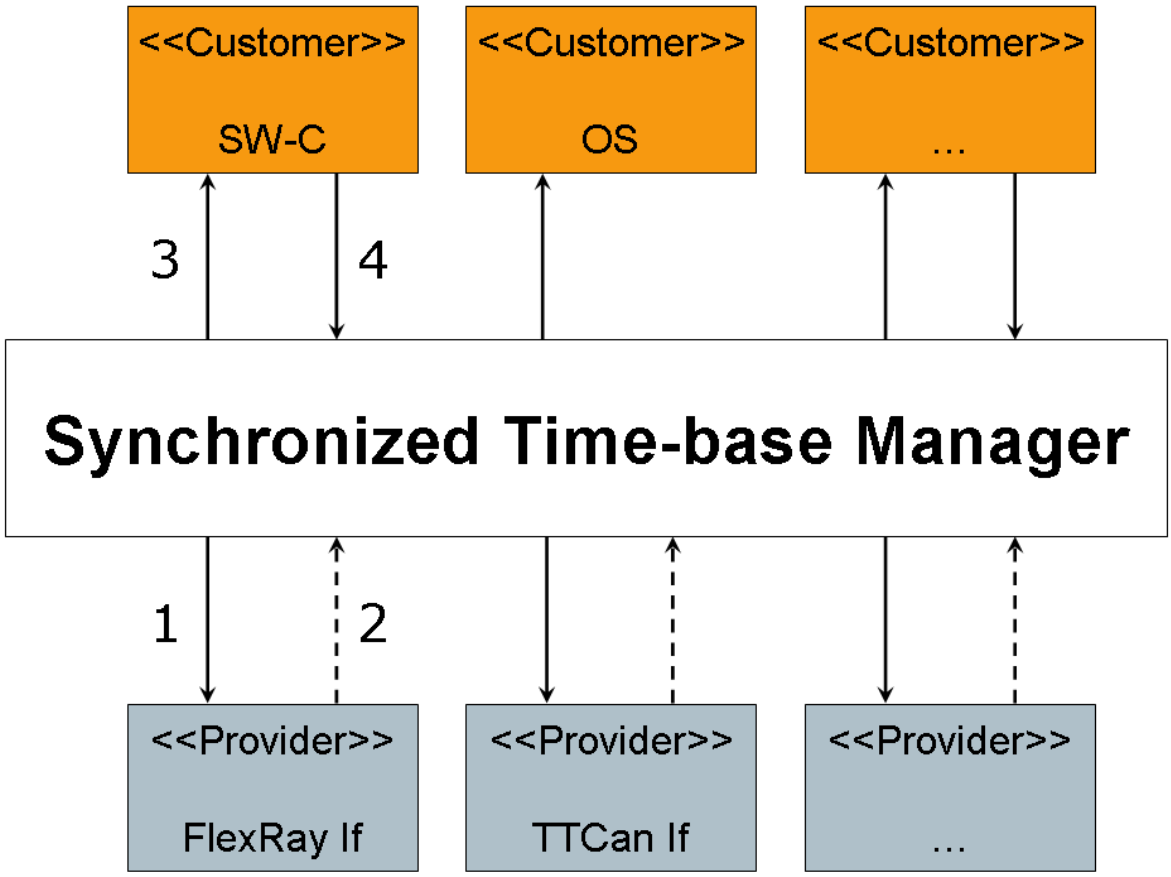

Figure 1: Synchronized Time-Base Manager as consumer and provider

So to say, the Synchronized Time-Base Manager acts as **time-base broker** by offering the customers access to synchronized time-bases. Doing this, the Synchronized Time-Base Manager abstracts from the “real” time-base provider.

In the following, the different providers and customers and the meaning of the several arrows in the figure above are described in a more detailed way.

1.1.2 Provider

The Synchronized Time-Base Manager itself does not provide any facility (e.g. protocols) for establishing a synchronized time among multiple nodes. Thus, the service requires other modules within the AUTOSAR BSW stack, which can provide this functionality. The FlexRay Interface and the TTCAN Interface are examples of modules which provide the definition of a synchronized time-base.

Calling the provider (arrow “1” in Figure 1) or getting called by the provider (arrow “2” in Figure 1) are the possible ways how to communicate with the provider.

1.1.3 Customer

The Synchronized Time-Base Manager has the requirement of satisfying the customers need in regard to time and passage of time. This section describes the different classes of customers and how they access the functionality.

Note: The classes are not completely disjoint. Thus, one specific customer can potentially be mapped to different classes of customers.

a) **Triggered customer**
This kind of customer is triggered by the Synchronized Time-Base Manager. Thus, the module itself is aware of the required functionality of the customer, and uses the defined interface of the customer to access it (e.g. accessing the Os SyncScheduleTable() API for synchronizing the respective ScheduleTable with the global time).

b) **Active customer**
This kind of customer autonomously calls the Synchronized Time-Base Manager, getting knowledge about the global time value (e.g. asking for the actual date and time).

c) **Notification customer**
This kind of customer is interested in the current state of the Synchronized Time-Base Manager and wants to get informed about state changes and/or error occurrences (e.g. loss of global time).

Customers a) and c) are triggered by the Synchronized Time-Base Manager (arrow “3” in Figure 1). Customer b) accesses itself the Synchronized Time-Base Manager (arrow “4” in Figure 1).

1.2 Terminology

In this section, a more precise definition of the term “global time” is given.

Important note: we avoid the use of the term “global time” for the rest of this specification, as there is no single “global time”. Instead, we use the term “synchronized time-base”.

For the purposes of this specification, we use the terms “physical time-base”, “software time-base”, “synchronized time-base” and “Epoch (reference date)” as follows:

1.2.1 Physical Time-Base

Definition: A physical time-base is a physical device which allows obtaining knowledge about the passage of time based on its physical properties (e.g. oscillation of a quartz crystal with a known frequency, atomic clock, earth rotation).

1.2.2 Software Time-Base

Definition: A software time-base is a software-provided measure of time derived from one or more physical time-bases. A time-base can be realized as

- an event source (e.g. a regular interrupt or alarm)
- a clock value data entity (e.g. a hardware or software counter representing time)

A software time-base is a means for customers to be triggered based on the passage of time and/or to obtain knowledge about the passage of time.

1.2.3 Synchronized Time-Base

Definition: A synchronized time-base is a software time-base existing at a processing entity (actor / processor / node of a distributed system) that is synchronized with software time-bases at different processing entities. A synchronized time-base can be achieved by time protocols or time agreement protocols that derive the synchronized time-base in a defined way from one or more physical time-bases. Examples are the network time protocol (NTP) and FlexRay or TTCAN time agreement protocol.

The synchronization will apply to the clock rate and/or to the clock absolute value (offset correction).

A synchronized time-base allows synchronized action of the processing units. Synchronized time-bases are often called “global time”, like the so called “FlexRay global time”. We do not use the term “global time” here because it is an important feature of the module specified in this document that it can cope with different synchronized time-bases which may vary in terms of rate and absolute value.

More than one synchronized time-base can exist at one processing unit, e.g. a FlexRay node will have the synchronized time-base achieved from the FlexRay time agreement protocol in the network cluster but might also have a global time-base derived from the time provided by a UTC time server (which is based on a set of atomic clocks). Both synchronized time-bases will probably have slightly different rate, and there is no relationship defined between their absolute values.

Note: A synchronized time-base is derived in a defined way (time protocol or time agreement protocol) from a defined set of physical time-bases.

2 Conventions to be used

- In requirements, the following specific semantics shall be used (based on the Internet Engineering Task Force IETF).

  The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as:

  - SHALL: This word means that the definition is an absolute requirement of the specification.
  - SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
  - MUST: This word means that the definition is an absolute requirement of the specification due to legal issues.
  - MUST NOT: This phrase means that the definition is an absolute prohibition of the specification due to legal constraints.
  - SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
  - SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
  - MAY: This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

3 Related Documentation

3.1 Input Documents

The following input documents have been used in the development of these requirements:

[1] Glossary
AUTOSAR_TR_Glossary.pdf

[2] Specification of Timing Extensions
AUTOSAR_TPS_TimingExtensions.pdf

3.2 Related standards and norms

[3] IEC 7498-1 The Basic Model, IEC Norm, 1994
[4] ISO WD 26262: Functional Safety

4 Requirements

This chapter describes all requirements driving the specification of the Synchronized Time-Base Manager. Most of them originate from the Time Determinism concept paper (AUTOSAR internal document). Also, some of them have strong links to the Technical Safety Concept (AUTOSAR internal document). These links are given (when possible) in the "supporting material" field.

Limitations

The concept is targeted at supporting time-critical and safety-related automotive applications such as airbag systems and braking systems. This doesn't mean that the concept has all that is required by such systems though, but crucial timing-related features that cannot be deferred to implementation are considered.

In addition, the current solution of the Synchronized Time-Base Manager does not provide its own time agreement protocol. Thus, the Synchronized Time-Base Manager shall use the functionality of time-base providers as defined in 1.1.2[2].

For simplicity, only ECUs in the same network cluster are considered. A vehicle-wide definition of time can be achieved by introducing time gateways between clusters but this is left to the implementer.

4.1 [BSW420001] Deal with different customer types

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	06.11.2008
Short Description:	Deal with different customer types
Type:	New
Importance:	High
Description:	The configuration of the Synchronized Time-Base Manager shall allow the interaction with different types of customers. The Synchronized Time-Base Manager is a service that should provide a time-base (if requested) in such a way : a) it triggers interfaced SW-C and BSW b) it provides the time-base on demand when the customer asks for it The customer shall have the possibility to choose the desired interaction with the Synchronized Time-Base Manager.
Rationale:	It is necessary to have a configurable interface which allows the application of the Synchronized Time-Base Manager in different architectures (e.g. safety-related or not).
Use Case:	There exist applications (e.g. with safety-related background) that need to be triggered by the Synchronized Time-Base Manager in order to fulfil the functional requirement (e.g. the OS ScheduleTable must be synchronized by the Synchronized Time-Base Manager actively). However, in many other applications (e.g. DEM functionality), the Synchronized Time-Base Manager reacts on demand.

[2] This limitation is only required for distributed global time needs. Obviously, when only a single ECU is considered (e.g. when the whole functionality is deployed to only one ECU), a global time is not explicitly required.

Dependencies:	[BRF00124] Usage of ECU local time for scheduling of communication [BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

4.2 [BSW420002] Synchronize triggered customer

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	11.06.2008
Short Description:	Synchronize triggered customer
Type:	New
Importance:	High
Description:	The Synchronized Time-Base Manager shall trigger registered customers. As described in [BSW420001, the Synchronized Time-Base Manager can be configured to trigger customers or to provide the definition of time on demand. For the first case, the module triggers registered customers periodically (within the MainFunction() of the Synchronized Time-Base Manager) by synchronizing their definition of time with the associated time-base.
Rationale:	The Synchronized Time-Base Manager offers the option of synchronizing the customer with the definition of time. In this case, the customer does not require any additional algorithm for synchronization, and reacts on time-base synchronization by the StbM.
Use Case:	An arbitrary number of RunnableEntities must be executed synchronously. Synchronous means, that they shall start with a well defined and guaranteed relative offset (e.g. relative offset “0”, means the execution shall occur at the same point in time).
Dependencies:	[BRF00124] Usage of ECU local time for scheduling of communication [BRF00126] Services for synchronization of SW-Cs
Conflicts:	None identified.
Supporting Material:	

4.3 [BSW420009] Configuration of triggered customers

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	05.02.09
Short Description:	Configuration of triggered customers
Type:	New
Importance:	Medium
Description:	The module should provide configuration parameters for each triggered customer. At least, the following configuration issues must be satisfied: i) During runtime, a possible state of a synchronized time-base is the loss of synchronization (e.g. currently no FlexRay global time has been established). In this case, it should be possible to specify for each triggered customer whether he wants to be synchronized by the Synchronized Time-Base Manager or not. ii) Triggering period: For each customer, the required synchronization period should be configurable.
Rationale:	The customer should have the possibility of configuration its synchronization request.
Use Case:	OS ScheduleTable should be synchronized every 20ms only when the global time definition is available
Dependencies:	[BRF00124] Usage of ECU local time for scheduling of communication

	[BRF00126] Services for synchronization of SW-Cs
Conflicts:	None identified.
Supporting Material:	

4.4 [BSW420003] Access to time-base value

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	06.11.08
Short Description:	Access to time-base value
Type:	New
Importance:	High
Description:	The Synchronized Time-Base Manager shall allow customers to have access to the synchronized time-base. As described in [BSW420001, the Synchronized Time-Base Manager can be configured to trigger customers or to provide the definition of time on demand. For the second case, the module should provide an appropriate interface, allowing the customer to access the time-base.
Rationale:	The Synchronized Time-Base Manager offers the possibility to the customers to access the definition of time if required.
Use Case:	The DEM wants to know the current definition of time in order to clock the error logging.
Dependencies:	[BRF00120] Synchronization of ECUs local time within a cluster [BRF00124] Usage of ECU local time for scheduling of communication [BRF00125] Monitoring of local time [BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

4.5 [BSW420005] Perform access to time-base provider

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	13.01.2009
Short Description:	Perform access to time-base provider
Type:	New
Importance:	High
Description:	The Synchronized Time-Base Manager shall access the time-base provider/providers (e.g. the FlexRay Interface or the TTCAN Interface) for getting its/their definition of time. The Synchronized Time-Base Manager can use this information and forward it to its customers.
Rationale:	The Synchronized Time-Base Manager does not provide its own time agreement protocol and thus he must access entities which provide him the definition of time. The provider has the task to deliver a “synchronized time-base”. This way, there is no need for the Synchronized Time-Base Manager to implement its own agreement protocol. Instead, the module uses existing functionality. Of course, system cluster, where no time-base provider is available, have the possibility to access their local time (e.g. µC clock). However, in this case it is not possible for the Synchronized Time-Base Manager to establish a common definition of time among multiple nodes
Use Case:	A distributed definition of time is needed for safety related applications.
Dependencies:	[BRF00120] Synchronization of ECUs local time within a cluster [BRF00124] Usage of ECU local time for scheduling of communication

	[BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

4.6 [BSW420006] Dependable provision of time

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	13.01.09
Short Description:	Dependable provision of time
Type:	New
Importance:	Medium
Description:	The Synchronized Time-Base Manager shall continuously provide the definition of time. If synchronization is not specified or temporarily not established, the local time shall be provided (but without relation to a distributed definition of time). Thus, the module provides permanently a definition of time to the customer. Among the status information, the customer can get knowledge about the quality of the gathered time definition.
Rationale:	Existing systems today should not be influenced negatively when introducing the new Synchronized Time-Base Manager. It is important that the system doesn't suspend when a distributed definition of time isn't available.
Use Case:	Important for hybrid systems where a synchronized definition of time is important for a certain part of the application.
Dependencies:	[BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

4.7 [BSW420007] Fault detection

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	13.01.09
Short Description:	Fault detection
Type:	New
Importance:	High
Description:	The Synchronized Time-Base Manager shall provide fault detection mechanism. It must detect the following state changes: • Loss/Re-Establishment of synchronized time-bases • Errors during customer call It shall be configurable whether the customer wants to get informed about those state changes or if the customer itself calls the Synchronized Time-Base Manager to get this information. It is out of the scope of Synchronized Time-Base Manager to define 1) How to manage the failed synchronization (if necessary) 2) How to manage the time recovery value in case of failed synchronization
Rationale:	Certain software parts may require a deep knowledge about the status of the distributed time definition to successfully perform their functionality.
Use Case:	Part of the vehicle dynamic subsystem must guarantee a concurrent execution of their distributed functionality. If a synchronization loss is detected, the subsystem must trigger appropriate counteractions.
Dependencies:	[BRF00125] Monitoring of local time [BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.

Supporting Material:	

4.8 [BSW420008] Notification mechanism

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	13.01.09
Short Description:	Notification mechanism
Type:	New
Importance:	Medium
Description:	The Synchronized Time-Base Manager shall provide the functionality of notifying customers in case a state change of the synchronized time-base(s) has been detected. In addition, the module should allow for periodical notification of the customers about the state.
Rationale:	Certain software parts may require a deep knowledge about the status of the distributed time definition to successfully perform their functionality.
Use Case:	Part of the vehicle dynamic subsystem must guarantee a concurrent execution of their distributed functionality. If a synchronization loss is detected, the subsystem must trigger appropriate counteractions.
Dependencies:	[BRF00125] Monitoring of local time [BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

4.9 [BSW420010] System service interface

Initiator:	WP Functional Safety and Processes | Magneti Marelli Powertrain S.p.A.
Date:	05.02.09
Short Description:	System service interface
Type:	New
Importance:	Medium
Description:	As SW-C are potential customers of the Synchronized Time-Base Manager, a communication among the RTE must be performed. Thus, a respective System Service interface must be defined for the StbM.
Rationale:	The Synchronized Time-Base Manager must be able to communication with SW-C as customers.
Use Case:	An application SW-C wants to get informed about the current value of a time-base (e.g. FlexRay global time).
Dependencies:	[BRF00124] Usage of ECU local time for scheduling of communication [BRF00126] Services for synchronization of SW-Cs [BRF00127] Services for accessing to both local and global time
Conflicts:	None identified.
Supporting Material:	

5 Use Cases

5.1 Synchronization of RunnableEntities

An arbitrary number of RunnableEntities must be executed synchronously. Synchronous means, that they shall start with a well defined and guaranteed relative offset (e.g. relative offset “0”, means the execution shall occur at the same point in time).

Such a requirement can be specified by the AUTOSAR Timing Extensions [2] and must be fulfilled independently of the actual deployment of the software components. However, as the limitations in chapter 4 indicate, only ECUs in the same network cluster are considered for the establishment of a synchronized time-base. Thus, the fulfilment of the requirement described above can only be guaranteed by deploying the related software components within the same cluster (e.g. FlexRay or TTCAN).

A classical application of this use cases is the sensor data read out or synchronous actuator triggering by different RunnableEntities.

5.2 Time provision

The application (and other BSW modules) shall have a central module which is responsible for the provision of information about the absolute time and passage of time.

A classical application of this use case is the access to synchronized calendar time by the application, e.g. for diagnostic events storage.

Other possible scenarios:

- Measuring the passage of time between two tagged system states (e.g. start and end of a RunnableEntity, deadline monitoring for timing-relevant functions).
- Guaranteeing the accurate triggering of OS alarms every (well-defined) interval.

5.3 Notification mechanism

The application (and other BSW modules) shall have the possibility of getting informed about the current status of the definition of time within the cluster. Thus, some kind of notification mechanism is required, which informs the application (and other BSW modules) upon state changes or error occurrences.