Document Title	Demonstrator Design of Functional Cluster Platform Health Management
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	924

Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R20-11

Document Change History

Date	Release	Changed by	Description
2020-11-30	R20-11	AUTOSAR Release Management	• Implementation of PHM Daemon • Implementation of APIs for Recovery and Health Channel to SM has been introduced • Health Monitoring (i.e. Chapter 7) from ASWS_HM is moved to SWS_PHM
2019-11-28	R19-11	AUTOSAR Release Management	• Implementation of dynamic read of config from Manifest • Implementation of syntax update to match current specification (ReportCheckpoint and ReportHealthStatus) • Implementation to replace standard types with ara::core types • Unit Tests for the new features • Removed generated API tables • Changed Document Status from Final to published

2019-03-29	19-03	AUTOSAR Release Management	• Implementation of Alive and Deadline Supervision (including boost timers) • Implementation of Logical Supervision (with supervision graph) • Implementation of Local Supervision Status (state machine for every supervised entity) • Unit Tests for the new features
2018-11-02	18-10	AUTOSAR Release Management	• Initial release

Disclaimer

Table of Contents

1 Introduction 5
1.1 Known limitations 5
2 Overview on architecture 8
2.1 Design approach / Design principles 9

1 Introduction

This document describes the design (approach and decisions) of the functional cluster Platform Health Management for AUTOSAR's Adaptive Platform Demonstrator (APD).

The decisions taken for the AUTOSAR Adaptive Platform Demonstrator may not apply to other implementations as the standard is defined by the specifications. Nevertheless, the Demonstrator may supplement and ease the understanding of the specifications.

This implementation of Platform Health Management software provides a complete and well-documented reference implementation that is meant to be used in prototype projects as well as a basis for production-grade implementations. The main goal for development of the Platform Health Management demonstrator code is to provide a proof of concept for Platform Health Management features specified in AUTOSAR Adaptive Platform. Optimization for memory consumption and speed have been considered but they haven't played a major role in overall software design and implementation. Furthermore, no static or dynamic code analysis has been performed. Therefore, any series production project deriving from this implementation will have to further fulfill the safety constraints described in the industry standards.

1.1 Known limitations

Limitations of the demonstrator implementation of the functional cluster.

- Not all of the SWS requirements are implemented and they are listed here:

Feature	Requirement ID	Implementation status
Health Monitoring reports	SWS_PHM_01140	not implemented.
supervision errors	SWS_PHM_01141	not implemented.
	SWS_PHM_01142	not implemented.
	SWS_PHM_01143	not implemented.
	SWS_PHM_01144	not implemented.
	SWS_PHM_01146	not implemented.
	SWS_PHM_01147	not implemented.
	SWS_PHM_01148	not implemented.
Health Monitoring provides an inte-	SWS_PHM_00112	not implemented.
face to Supervised Entities about	SWS_PHM_01134	Partially implementedd.
their Supervision State	SWS_PHM_01135	Partially implementedd.
	SWS_PHM_01136	Partially implementedd.
	SWS_PHM_01137	Partially implementedd.
Health Monitoring shall support	SWS_PHM_00457	implemented.
multiple occurrences of the same	SWS_PHM_01116	not implemented.

▽

△

Supervised Entity	SWS_PHM_01120	not implemented.
	SWS_PHM_01121	not implemented.
	SWS_PHM_01123	implemented.
	SWS_PHM_01133	not implemented.
Health Monitoring shall support	SWS_PHM_01116	not implemented.
multiple instances of Checkpoints	SWS_PHM_01120	not implemented.
in a Supervised Entity occurrence	SWS_PHM_01133	not implemented.
Health Monitoring shall support	SWS_PHM_00111	not implemented.
mode-dependent behavior of		
Supervised Entities and it shall		
support the supervision on the		
transitions between Checkpoints		
belonging different Supervision		
Health Monitoring shall provide an	SWS_PHM_00321	implemented.
interface to Supervised Entities	SWS_PHM_00424	not implemented.
to report the currently reached	SWS_PHM_00425	not implemented.
Checkpoint.	SWS_PHM_00458	implemented.
	SWS_PHM_01010	implemented.
	SWS_PHM_01123	implemented.
	SWS_PHM_01124	implemented.
	SWS_PHM_01125	Partially implemented.
	SWS_PHM_01126	Partially implemented.
	SWS_PHM_01127	implemented.
	SWS_PHM_01131	implemented.
	SWS_PHM_01132	implemented.
	SWS_PHM_01138	not implemented.
Health Monitoring shall provide an	SWS_PHM_00321	implemented.
interface to Supervised Entities to	SWS_PHM_00457	implemented.
report their health status.	SWS_PHM_00458	implemented.
	SWS_PHM_01010	implemented.
	SWS_PHM_01118	not implemented.
	SWS_PHM_01119	not implemented.
	SWS_PHM_01122	implemented.
	SWS_PHM_01124	implemented.
	SWS_PHM_01128	implemented.
	SWS_PHM_01131	implemented
	SWS_PHM_01139	not implemented.
Platform Health Management shall	SWS_PHM_00457	implemented.
provide a standardized header file	SWS_PHM_01005	not implemented.
structure for each service	SWS_PHM_01018	not implemented.
	SWS_PHM_01113	not implemented.
	SWS_PHM_01122	implemented.
	SWS_PHM_01123	implemented.
	SWS_PHM_01127	implemented
	SWS_PHM_01128	implemented.

▽

△

	SWS_PHM_01132	implemented
	SWS_PHM_01134	Partially implemented.
	SWS_PHM_01135	Partially implemented.
	SWS_PHM_01138	not implemented.
	SWS_PHM_01139	not implemented.
The service header files shall	SWS_PHM_00457	implemented.
define the namespace for the	SWS_PHM_01005	not implemented.
respective service	SWS_PHM_01018	not implemented.
	SWS_PHM_01113	not implemented.
	SWS_PHM_01122	implemented.
	SWS_PHM_01123	implemented.
	SWS_PHM_01127	implemented
	SWS_PHM_01128	implemented.
	SWS_PHM_01132	implemented
	SWS_PHM_01134	Partially implemented.
	SWS_PHM_01135	Partially implemented.
	SWS_PHM_01138	not implemented.
	SWS_PHM_01139	not implemented.
Platform Health Management shall	SWS_PHM_00424	not implemented.
define how language specific data	SWS_PHM_00425	not implemented.
types are derived from modeled	SWS_PHM_01116	not implemented.
data types.	SWS_PHM_01118	not implemented.
	SWS_PHM_01119	not implemented.
	SWS_PHM_01120	not implemented.
	SWS_PHM_01121	not implemented.
	SWS_PHM_01122	implemented.
	SWS_PHM_01132	implemented
	SWS_PHM_01133	not implemented.
	SWS_PHM_01140	not implemented.
	SWS_PHM_01141	not implemented.
	SWS_PHM_01142	not implemented.
	SWS_PHM_01143	not implemented.
	SWS_PHM_01144	not implemented.
	SWS_PHM_01146	not implemented.
	SWS_PHM_01147	not implemented.
	SWS_PHM_01148	not implemented.
Platform Health Management shall	SWS_PHM_00321	implemented.
provide a standardized C++ interfa-	SWS_PHM_00424	not implemented.
ce for the reporting of Checkpoints	SWS_PHM_00425	not implemented.
	SWS_PHM_00458	implemented.
	SWS_PHM_01010	implemented.
	SWS_PHM_01123	implemented.
	SWS_PHM_01124	implemented.
	SWS_PHM_01125	Partially implemented.
	SWS_PHM_01127	implemented

▽

△

	SWS_PHM_01131	implemented
	SWS_PHM_01132	implemented
	SWS_PHM_01134	Partially implemented.
	SWS_PHM_01135	Partially implemented.
	SWS_PHM_01138	not implemented.
Platform Health Management shall	SWS_PHM_00321	implemented.
provide a standardized C++	SWS_PHM_00457	implemented.
interface for the reporting of	SWS_PHM_00458	implemented.
Health Channel	SWS_PHM_01010	implemented.
	SWS_PHM_01118	not implemented.
	SWS_PHM_01119	not implemented.
	SWS_PHM_01124	implemented.
	SWS_PHM_01126	Partially implemented.
	SWS_PHM_01128	implemented.
	SWS_PHM_01131	implemented.
	SWS_PHM_01139	not implemented.
Platform Health Management shall	SWS_PHM_00111	not implemented.
realize the Supervision Mode as tu-		
ple of Execution Management states		
Platform Health Management shall	SWS_PHM_00110	not implemented.
provide a standardized interface	SWS_PHM_NA	not implemented.
between Platform Health Management		
components used in a daisy chain		
Platform Health Management shall	SWS_PHM_00110	not implemented.
provide the Daisy chaining	SWS_PHM_NA	
interface over ara:com		

2 Overview on architecture

The Platform Health Management (PHM) supervises the applications and could trigger a recovery action in case any supervised entity fails. The recovery actions are defined by the integrator based on the software architecture requirements for the Platform Health Management and configured in the manifests.

The Platform Health Management functional cluster provides following supervision to supervise the execution of software:

1. Alive supervision
2. Deadline supervision
3. Logical supervision
4. Health channel supervision

2.1 Design approach / Design principles

The current implementation of PHM is in form of library and runs in context of the application. Multiple instances of same supervised entity is not supported in the current implementation.

In order to implement PHM that can be used in prototype projects as well as a basis for production-grade implementations, ara::phm is provided in the demonstrator. Current ara::phm implementaion provides following demonstrator artifacts:

1. PHM provides an interface to supervised entities about their supervision status and health status.
2. It provides an interface to report the currently reached checkpoint and reporting of health channel.
3. PHM configuration related to supervision modes is partially supported.

The interfaces of Platform Health Management to other functional clusters are only informative and are not standardized.