AWT420

Universal 4-wire, dual-input transmitter

Additional instructions for
IEC 61508-compliant devices

Measurement made easy

—

AWT420
Universal 4-wire,
dual-input transmitter

Introduction

The purpose of the safety manual is to document the important information required to enable the integration of this product into a safety-related system, in compliance with the requirements of the IEC 61508 and IEC 61511 standards.

This document must be considered in conjunction with related operating instruction.

For more information

Further publications for the AWT420 transmitter are available for free download from:
www.abb.com/measurement
or by scanning this code:

Links and reference numbers for the transmitter publications are also shown below:

	Search for/click on:
AWT420 transmitter – Data Sheet	DS/AWT420
AWT420 transmitter – Commissioning Instruction	CI/AWT420
AWT420 transmitter – Hazardous area information	INF/ANAINST/012
AWT420 transmitter – HART Communications Supplement	COM/AWT420/HART
AWT420 transmitter – HART FDS Communications Supplement	COM/AWT420/HART/FDS
AWT420 transmitter – PROFIBUS Communications Supplement	COM/AWT420/PROFIBUS
AWT420 transmitter – MODBUS Communications Supplement	COM/AWT420/MODBUS
AWT420 transmitter – Ethernet Communications Supplement	COM/AWT420/ETHERNET

Contents

1 Application area

The AWT420 transmitter is a 4 wire device for monitoring of water quality parameters.

Combined with analog or digital EZLink sensors, the AWT420 transmitters become a sensor assembly.

The sensors that can be connected to the AWT420 transmitter for SIL safety applications are:
- Analog pH
- Digital pH
- Analog conductivity
- Dissolved oxygen
- ATS410 turbidity
- ATS430 turbidity and total suspended solids (TSS) sensor
- ACL420 digital chlorine
- ACL410 analog chlorine

Note. SIL is only applicable to build revision “B: Isolated outputs”.

The area of safety applications can be seen in “Table 9 SIL assessment of AWT420” on page 11, with further constraints as stated within this safety manual.

In case of questions and detected safety critical device failures please contact the ABB Customer Service Center by stating the ‘Product Type Designator’ and ‘Functional Safety SIL’ as request headlines.

2 Associated documents

The following product documents must be adhered to in addition to this safety manual:

Table 1 AWT420 documentation

Product designation	Document type	Document name
AWT420	Data sheet	DS/AWT420
AWT420	Commissioning instruction	CI/AWT420
AWT420	Operating instruction	OI/AWT420

The documents can be downloaded in the available languages from the links in Table 1, or from library.abb.com.
In addition, the user of this device is responsible for ensuring compliance with applicable legal regulations and standards.

3 Safety function and safety data overview

This chapter provides information on the safety function and safety integrity data.

Table 2 General safety function

Device designation and permissible types	AWT420	
Safety-related output signal	4 to 20 mA	
Fault current	Current low alarm value ≤ 3.6 mA Current high alarm value ≥ 21.0 mA	
Safety function(s)	Provide appropriate 4 to 20 mA current output based on sensor input within the defined safety deviation	
Device type acc. to IEC 61508-2	☐ Type A (HFT = 0)	☒ Type B (HFT = 0)
Operating mode	☒ Low demand mode	☒ High demand mode
Valid hardware version	Refer to Table 3	
Valid software version	N/A	
Type of evaluation	☐ Complete HW/SW development process evaluation incl. FMEDA and change management acc. to IEC 61508-2,3	
	☐ Evaluation of 'Prior use' performance for HW/SW incl. FMEDA and change management acc. to IEC 61508-2,3	
	☐ Evaluation of HW/SW field data to verify 'prior use' acc. to IEC 61511	
	☒ Evaluation of hardware safety integrity as per 7.4.4 & 7.4.5 of IEC 61508-2 without assessment of systematic capability. **Note**. Only the electronics have been evaluated. The software has not been evaluated.	
Evaluation through - report no.	Technis: FMEDA Report T1062 Iss. 1, 01/09/2022	

Table 3 Hardware versions

PCBA	Hardware version*
Analog isolated OP	2
CPU	5
AC isolated baseboard	3
DC isolated baseboard	5
Analog pH	3
Analog conductivity	3
EZLink HazLoc	2
EZLink	4
Analog turbidity	3
Universal Input Module	3
ATS430	3
Digital pH	3
Digital Cl	3

* SIL is applicable to this hardware version and later.

Table 4 Safety integrity

Hardware safety integrity	Single-channel use (HFT = 0)	☒ SIL1 capable	☐ SIL2 capable

Table 5 Failure rates and diagnostic data

Data for the Safety Configuration	Data for the transmitter without connected sensor at the environmental conditions listed within chapter "FMEDA failure data" on page 11	
Safety deviation	±2 % (±0.32 mA)	Failure Data incl. sensor combinations, refer to "FMEDA failure data" on page 11
SFF Safe failure fraction	Refer to "FMEDA failure data" on page 11	
Proof-test coverage (PTC)	100 % (in using the procedure described in "Periodic proof-test and maintenance" on page 9)	

4 Terms and definitions

Table 6 Terms and definitions

Term	Definition
IEC 61508	International Standard 'Functional safety of electrical/electronic/programmable electronic safety-related systems'
IEC 61511	International Standard 'Functional safety – safety instrumented systems for the process industry sector'
Safety integrity	Probability of a safety system satisfactorily performing the specified safety functions under the stated conditions
Safety Integrity Level (SIL)	Discrete safety integrity level corresponding to a range of safety integrity values, where level 4 has the highest and level 1 has the lowest
Functional safety	Part of the overall safety relating to the controlled system that depends on the correct functioning of the safety system and other risk reduction measures
Safety function	Function to be implemented by a safety system or other risk reduction measures, that is intended to achieve or maintain a safe state for the controlled system, in respect of a specific hazardous event
Safety deviation (formerly safety accuracy)	Change in the output due to (internal) component failures which was not rated as failure within the failure analysis
Hardware fault tolerance HFT n	Ability to continue to perform a required function in the presence of n hardware faults or errors
Architectural constraints	The highest safety integrity level that can be claimed limited by the hardware constraints (SFF, HFT)
Systematic safety integrity SC	Measure on a scale of SC 1 to SC 4 on the systematic safety integrity when the element is applied in accordance with the instructions specified in the safety manual
Low demand mode	The safety function is only performed on demand with a demand interval no greater than one per year and greater than twice the proof-test interval
High demand mode	The safety function is only performed on demand, and where the frequency of demand is greater than one year
Dangerous failure	Failure that prevents the safety function from operating as expected
Dangerous detected failure	Dangerous failure but detected and forced to alarm state
Dangerous undetected failure	Dangerous failure not being diagnosed
Safe failure	Failure that results in a fail-safe state
No effect, no part failure	Failure without effect above the safety deviation or which are not part on the specified safety function
Annunciation failure	Failure within automatic diagnostics
Common cause failure	Failures from a single cause that affect more than one channel or component
FIT	Failure in Time (1×10^{-9} failures per hour) named λ Lambda
Failure rate	Number of failures per unit time assuming to be a constant value declared as FIT λDD – detected dangerous failures λDU – undetected dangerous failures λSD – detected safe failures λSU – safe failures
PFD_{AVG}	Average probability of dangerous failure on demand
Safe failure fraction (SFF)	Fraction of the overall failure rate that results to a safe failure
Proof-test	Periodic test performed to detect dangerous hidden failures and weaknesses in the mechanical integrity within the final application environment
Proof-test interval	Execution interval of the period proof-test
Proof-test coverage (PTC)	Fraction of detected dangerous failures by the periodic proof-test
Diagnostic coverage (DC)	Fraction of dangerous failures detected by on-line diagnostic tests
Fault detection time	Worst case interval on the transmitter fault detection by on-line tests to output fault reaction
Common cause failure	Failure causing concurrent failures of two or more separate channels in a multiple channel system
Systematic failure	Failure, related in a deterministic way to a certain cause, which can only be eliminated by design, manufacturing, operational procedures, documentation, or other relevant factors
Random hardware failure	Failure, which results from degradation mechanisms in the hardware. For equipment comprising many electrical components those failures occur at predictable rates but at unpredictable random times
Type A element Type B element	An element can be regarded as type A if, the failure modes of all constituent components are well defined; and the behavior of the element under fault conditions can be completely determined; and there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met. Otherwise, the element shall be regarded as type B
MooN architecture	Voting redundancy architecture. e.g., 1oo2: 1 out of 2 redundant channel architecture 2oo3: 2 out of 3 redundant channel architecture
Useful lifetime	Beyond the useful lifetime the probability of failure increases with time and the probabilistic failure rate estimation is invalid
Mission time	Final plant operation time for the safety system. Used for the PFD_{AVG} and Proof-Test Interval calculation

...4 Terms and definitions

...Table 6 Terms and definitions

Term	Definition
FMEDA	Failure modes, effects and diagnostics analysis
MTBF	Mean time between failure
MTTR	Mean time to repair
MTTF	Mean time to failure
DTM	Device type manager
EDD	Electronic device description
FIM	Field information manager
FDI	Field device integration
DCS	Distributed control system
HMI	Human-machine interface
Multidrop	HART Bus Communication Mode where output-signal is set to 4 mA
Closed coupled	Short connecting lead to the temperature sensor with less than 1 m (39.37 in) in length and connecting leads laid with mechanical protection
Extension wire	Long connecting lead to the temperature sensor with more than 1 m (39.37 in) in length or connecting leads laid without mechanical protection
Low stress	Low stress environment in terms of vibration and temperature cycling The operation is below 67 % maximum rating according to specification
High stress	High vibration environment in terms of vibration and temperature cycling The operation is above 67 % maximum rating according to specification
NAMUR NE43	Standardization of the signal level for the breakdown information of digital 4 to 20 mA transmitters
SIS	Safety instrumented system, e.g., consisting of sensors and transmitter, logic solver, and ESD actuator
LRV	Lower range value (measuring range lower limit)
URV	Upper range value (measuring range upper limit)
Range A...B	Ranges using three dots means running from the value A to the value B inclusively
Sensor redundancy with drift detection	Assembly with two sensors and one transmitter which allows to detect sensor drift failures
Safety assessment	Investigation based on evidence on the achieved safety integrity

5 Safety function

The safety function of the named transmitters is to provide an appropriate 4 to 20 mA output from the sensor input within the safety deviation.

Dangerous failure modes are considered as:
- fail to provide an appropriate 4 to 20 mA output
- spurious response despite no valid change

No other functions are declared and qualified as safety functions.

The safety function refers only to the analog output signal.

The final device assembly consists of the device electronics, and the attached sensor.

Alarm behavior and alarm current output

When a critical error is detected, an alarm current according NAMUR NE 43 is generated, which must be evaluated and processed by the safety logic solver.

Detected failures by internal diagnostics generates the configured alarm current.

The transmitter supports two selectable modes for the alarm current:
- LOW ALARM; this is the factory default setting
- HIGH ALARM

The low alarm current can be configured in a range from 3.5 to 4.0 mA.
The factory default setting is 3.5 mA.
The **low alarm current value** for safety applications shall be configured within **3.5 to 3.6 mA**.

The high alarm current can be configured in a range from 20.0 to 23.6 mA.
The factory default setting is 22 mA.
The **high alarm current value** for safety applications shall be configured **within 21.0 to 23.6 mA**.

The safety-related system (safety logic solver) must be able to safely detect both, the high and the low alarm current state.

In the following cases and by some electrical part failures, an error is forced independently of the configured alarm current to the low alarm current range:
- detected runtime errors by the watchdog monitoring
- detected runtime errors by current readback monitoring
- detected memory errors

Also, failures in some electrical parts force the current into a high alarm current range independent of the configured alarm current.

Safety deviation

The basic accuracy depends on the sensor type and the specified data within in the corresponding data sheets and the final measurement application.

Deviation on the output current by more than **±2 % (±0.32 mA)** is defined as the safety deviation for this transmitter.

…5 Safety function

Safety response time

The transmitter measurement update cycle time is up to 1,000 ms.

Each sensor may have a configurable filter length. This may be configured within “Sensor Setup” for the connected sensors.

It is the responsibility of the end user to consider and validate the impact of the above-mentioned response time behaviors.

Type classification

This transmitter is declared as Type B complex element with HFT = 0 according IEC 61508:2010.

Average probability of dangerous failure on demand PFD_{AVG}

The PFD_{AVG} calculation must be done based on certain important variables including:

1 Failure rates and failure modes.

2 Redundancy architecture including common cause failures.

3 Proof-test coverage, proof-test interval, proof-test duration.

4 Mission time.

5 Operational/maintenance capability.

6 Mean time to repair.

As only item **1** from the list above is under the control of the device manufacturer, it is the responsibility of the SIS designer to perform the PFD_{AVG} calculations for the final assembled SIS in order to determine suitability for the demanded Safety Integrity Level (SIL).

Accordingly, the PFD_{AVG} and the Architectural constraints (in terms of HFT & SFF) must be verified for each application by the end user, and the transmitter must be properly designed into the target safety instrumented function.

6 Safety operation constraints

The following constraints need to be considered when using the transmitter for SIL safety applications:

- only the current output 4 to 20 mA shall be used for safety applications
- the entire valid range of the output signal has been verified by the end user
- the safety parameters are configured as specified within this safety manual
- the correct parameterization in terms of the SIS safety function shall be checked be the end user
- the proof-test specified within this safety manual (or an equivalent test as specified for the final SIS safety function) shall be performed before activating the safety operation and in periodical cycles as demanded by the final PFD_{AVG} demands
- the device is installed per manufacturer’s instructions
- the DCS power supply for the transmitter shall be capable to provide the required voltage level even when the current output is active with the configured high alarm
- the transmitter shall be protected against environmental influences by a suitable installation housing
- the safety-related system (safety logic solver) must be able to safely detect both the high and the low alarm current states
- materials are compatible with the final process conditions
- the robustness against EMC disturbances has been tested to the requirements of NAMUR NE21:2017 which fulfills also the demands of IEC 61326-3-2:2017 Annex B, C, D
- strong surge EMC interference can lead to short-term deviations of up to 1 second in the output signal. If the final application environment offers such interference pulses, a DCS input filtering with a time constant of at least 1 second should be implemented
- the environmental, measurement and application limits must be considered accordingly for the SIL safety application

The transmitter does not meet safety requirements under the following conditions:

- during installation, configuration, repair and simulation
- with deactivated write protection
- during an inspection or proof-test

Before commissioning the transmitter in a safety loop application, the end user must check whether the transmitter setup confirms to the system’s safety function.

The end user must verify also that the correct transmitter has been installed at the correct measuring point.

Whenever the transmitter operating conditions are changed (for instance, if the mounting position is changed or the setup is modified), the safety function of the transmitter must be checked again.

7 Periodic proof-test and maintenance

According IEC 61508 and IEC 61511 proof-testing shall be performed to reveal dangerous faults which are undetected by automatic diagnostic tests.

The end user is responsible for selecting the type and the intervals according the overall safety system demands.

The inspections must be conducted in a manner that enables users to verify the proper function of the safety equipment in combination with all related components.

Recommended proof-test (transmitter and sensor)

The below described proof-test is a recommended variant which should be performed after installation, configuration changes and within the required periodical proof-test interval derived from the safety instrument system engineering demands and related PFD_{AVG} calculations.

This proof-test is assumed to detect 100 % of possible dangerous faults on the related transmitter electronics.

Table 7 Suggested steps for proof-test

Step	Test action (consecutive steps)
1	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2	Power down the transmitter, remove the sensor from the measuring point safely (refer to the sensor OI for further details). Power up the transmitter.
3	Force the transmitter to the high alarm current output by placing the connected sensors into a solution that will trigger a change in process value beyond the configured high alarm current setting, verify that the high alarm current is correct within the stated safety deviation.
4	Force the transmitter to the low alarm current output by placing the connected sensors into a solution that will trigger a change in process value beyond the configured low alarm current setting, verify that the low alarm current is correct within the stated safety deviation.
5	Restore the loop to full operation by restarting, powering down and powering up the device, and placing the sensor back into the measurement point.
6	Remove the bypass from the safety DCS.

Repair and replacement

In case of detected failures, corrective actions may be demanded.
Possible safety-critical failures shall be reported to service. Defective transmitters sent to ABB for repair or failure analysis should include information about the failure effect, hardware and software versions, the safety application and environmental conditions.

8 Installation, commissioning, and configuration

The transmitter must be installed, configured, commissioned and maintained by suitably qualified and experienced personnel.

Any configuration, installation or repair change may affect the safety function of the transmitter.

Therefore, the safety function shall be checked again after configuration, installation or repair change in using the described “Recommended proof-test (transmitter and sensor)” and “Safety parameter configuration”.

The constraints and limitations as provided within the operating instruction and data sheet as referenced within chapter “Associated documents” must be considered by the end user, especially in terms of:

- intended use and improper use
- use in potentially explosive atmospheres
- design and function
- product identification
- transportation and storage
- installation and ambient conditions
- electrical connections
- commissioning and operation
- diagnosis, maintenance, and repair

9 Safety parameter configuration

The transmitter can be configured using the local HMI.

The impact of damping and EMC filtering as described within chapter “Safety function” shall be considered.

10 Identification

Table 8 Device

Type	Description	Hardware version	Software version
AWT420	Transmitter	Refer to Table 3 on page 4	N/A

11 Notes on cybersecurity

This product and the EZLink Connect app is designed to be connected to and to communicate information and data via a digital communication interface.

It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the application of authentication measures etc.) to protect the product, the EZLink Connect app, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB Ltd. and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.

Communication protocol-specific security
The HART protocol is an unsecured protocol, as such the intended application should be assessed to ensure that these protocols are suitable before implementation.

The Modbus protocol is an unsecured protocol, as such the intended application should be assessed to ensure that these protocols are suitable before implementation.

The PROFIBUS PA protocol is an unsecured protocol, as such the intended application should be assessed to ensure that these protocols are suitable before implementation.

The PROFIBUS DP protocol is an unsecured protocol, as such the intended application should be assessed to ensure that these protocols are suitable before implementation.

12 FMEDA failure data

This chapter provides the summary of the probabilistic estimation on failure data according to:
Technis FMEDA Report T1062 Iss. 1, 01/09/2022.

The assessment is according to route 1H of IEC 61508-2 2010.

Electronics – AWT420

The FMEDA carried out on the worst-case configuration leads under the assumptions and constraints described in this manual to the following failure rate data.

Table 9 SIL assessment of AWT420

Configuration[1]	Type	Failure rate (FITS)[2]			SFF (%)	PFD_{avg} [3]	Hardware SIL low demand mode[3]	Hardware SIL high demand mode
		λDD	λDU	λS				
Analog pH with sensor[4]	B	816	532	1223	79.3	2.38E-03	SIL1	SIL1
Analog pH without sensor	B	316	32	223	94.5	1.52E-04	SIL2	SIL2
Digital pH with sensor[4]	B	936	566	1275	79.6	2.53E-03	SIL1	SIL1
Digital pH without sensor	B	436	66	275	91.5	3.06E-04	SIL2	SIL2
Conductivity with sensor[4]	B	914	595	1297	78.8	2.66E-03	SIL1	SIL1
Conductivity without sensor	B	414	95	297	88.2	4.32E-04	SIL1	SIL1
Dissolved oxygen with sensor[4]	B	858	539	1243	79.6	2.41E-03	SIL1	SIL1
Dissolved oxygen without sensor	B	358	39	243	93.9	1.86E-04	SIL2	SIL2
Analog turbidity with sensor[4]	A	852	531	1234	79.7	2.38E-03	SIL2	SIL1
Analog turbidity without sensor	A	352	31	234	94.9	1.51E-04	SIL2	SIL2
Digital turbidity with sensor[4]	B	914	566	1260	79.3	2.53E-03	SIL1	SIL1
Digital turbidity without sensor	B	414	66	260	91.1	3.06E-04	SIL2	SIL2
Digital chlorine with sensor[4]	B	856	549	1241	79.3	2.45E-03	SIL1	SIL1
Digital chlorine without sensor	B	356	49	241	92.4	2.28E-04	SIL2	SIL2
Analog chlorine with sensor[4]	B	873	551	1268	79.5	2.46E-03	SIL1	SIL1
Analog chlorine without sensor	B	373	51	268	92.7	2.37E-04	SIL2	SIL2

1 Assessments without sensor include failure rate of AWT420 transmitter and appropriate sensor interface card only. This is provided as sensor element failure rate is highly dependent upon process parameters and as such a generic sensor failure rate is better established by collecting data in-process.
2 Failure rates stated in FITS, or failures per billion hours.
3 PFD_{avg} calculation assumes proof test interval of 8,760 hours (1 year), MTTR of 24 hours, HFT = 0, and recommended proof test undertaken as per “7 Periodic proof-test and maintenance” on page 9.
4 Sensor failure rates should be validated in final application. Sensor failure rate has been assumed to be 2000 FITS for FMEDA data above.

Acknowledgments

- EZLink is a trademark of ABB Ltd.
- HART is a registered trademark of the FieldComm Group
- Modbus is a registered trademark of Schneider Electric USA Inc.
- PROFIBUS is a registered trademark of PROFIBUS organization

ABB Measurement & Analytics

For your local ABB contact, visit:
www.abb.com/contacts

For more product information, visit:
www.abb.com/measurement

SI/AWT420-EN Rev. A 01.2023