

Applying a Single Rosemount 5900S 2-in-1 Radar Level Gauge as the Sensor in Two Independent Protection Layers (i.e. BPCS and SIS)



Contents

Section 1: Introduction

1.1 Purpose	1
1.2 Background	1
1.3 Independent protection layers	8
1.4 Technology diversification	11

Section 2: Technical Evaluation

2.1 Independence	14
2.1.1 Putting numbers in perspective	15
2.2 Technology diversification	16

Section 3: Standards Compliance

3.1 API 2350 Edition 4	17
3.2 IEC 61511 Edition 1	17

Section 4: Conclusion

Appendix A: Common cause Failure Assessment of Rosemount 5900 2-in-1 & 2x5900 1-in-1

A.1 Definitions	21
A.2 Methodology	22
A.3 Comparison objects	23
A.4 Beta-calculation technique #1: Random Hardware Failures	24
A.5 Beta-calculation technique #2: Random and Systematic failures	25
A.6 Summary	27

Appendix B: Common Cause Failure Assessment of Rosemount 5900 2-in-1 & 2x5900 1-in-1 Including the Tank

Appendix C: Example Rosemount 5900 2-in-1 Users

Appendix D: Rosemount 5900 2-in-1 SIL 2 IEC 61508 Certificate

Appendix E: Rosemount 5900 2-in-1 Compliance with API 2350 Category 3 Requirements

Appendix F: API 2350 Ed 4 Interpretation

**Appendix G: Rosemount 5900 2-in-1 Compliance with IEC
61511 Requirements**

Section 1 Introduction

Purpose	page 1
Background	page 1
Independent protection layers	page 8
Technology diversification	page 11

1.1 Purpose

The purpose of this document is to provide a technical justification for anybody who wants to use the Rosemount 5900 2-in-1 Radar Level Gauge as both automatic tank gauge (ATG) and independent sensor in an overfill prevention system (OPS). The document specifically addresses requirements related to independence, technology diversification and compliance with the standards IEC 61511 and API 2350.

1.2 Background

Overfills are a major problem to the process industry in general, but especially so for bulk liquid storage tanks where the consequences can be catastrophic. Buncefield, Jaipur, Puerto Rico and West Virginia are just a few of the recent locations where chemical and petroleum overfills have affected thousands of people by for example environmental damage such as water pollution, fires and explosions resulting in asset and property damages, injuries and multiple fatalities.

Figure 1-1. Oil terminal just outside London in Buncefield, U.K. A tank overfill resulted in vapor cloud explosion and formation of the largest smoke cloud in western Europe since WW II. Fortunately there were no fatalities⁽¹⁾



(1) HSE UK Buncefield Investigation, <http://www.buncefieldinvestigation.gov.uk/>

Figure 1-2. Oil spill at a tank terminal in Jaipur, India which resulted in 11 fatalities. Half a million people were evacuated from the area, including 'residents' of a nearby prison⁽¹⁾



Yet accidents still occur. One of the reasons is that there are still considerable amounts of old and not properly maintained storage tanks in service with non-existing, non-functioning or obsolete overfill prevention equipment.

The industry and society in general is currently investing considerable resources to increase the safety at tank farms. Obvious examples of this on-going safety trend is the introduction of a standard for Safety Instrumented Systems (SIS), IEC 61511 Edition 1⁽²⁾, and the release of a new and more stringent overfill prevention standard, API 2350 Edition 4⁽³⁾, created by more than 40 global users and manufacturers in the petroleum industry. But although considerable industry focus it is a gigantic task to revamp all the existing storage tanks to API 2350 compliance, and a task that obviously not will be done overnight (if ever).

(1) *M B Lal Committee Report "IOC Fire accident investigation"*; <http://oisd.nic.in/>

(2) *International Electrotechnical Commission, Standard 61511 "Functional safety - Safety instrumented systems for the process industry sector"*; <http://www.iec.ch/>

(3) *American Petroleum Institute, Standard 2350 "Overfill Protection for Storage Tanks in Petroleum Facilities" Edition 4*; <http://www.api.org/>

Figure 1-3. API 2350 edition 4 is the new global overfill prevention standard for atmospheric petroleum storage tanks aboveground



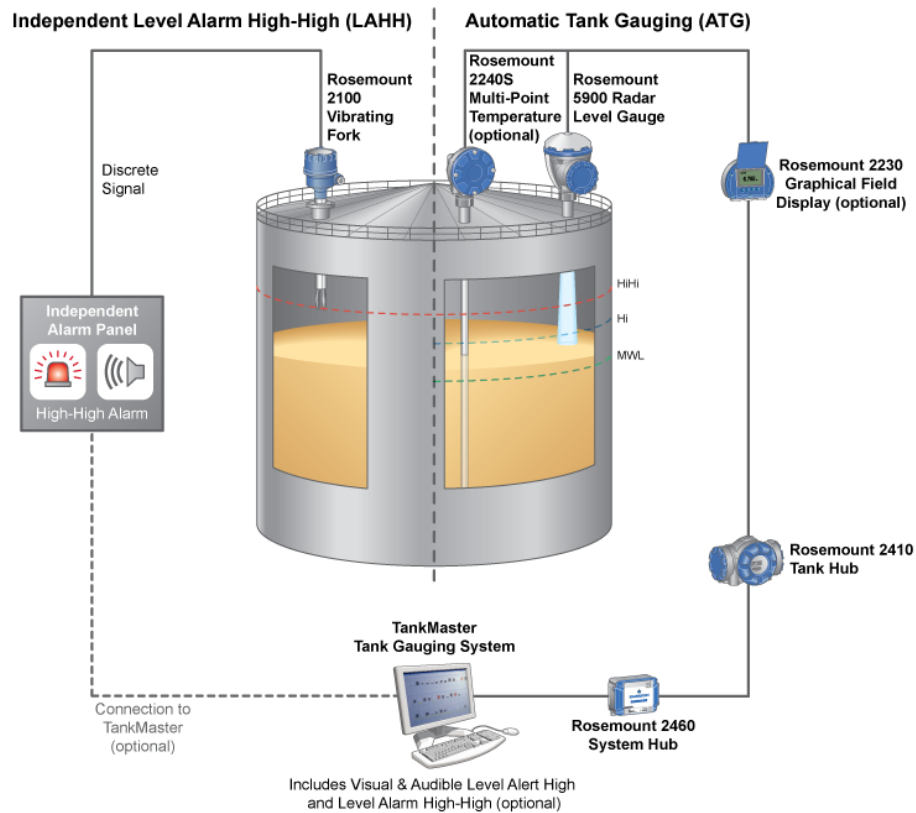
Today the basic overfill prevention technology at many facilities with atmospheric bulk liquid storage tanks has the following principal configuration:

- 1xAutomatic tank gauge (ATG) for continuous hi-accuracy level measurement connected to a DCS or separate tank gauging system and
- 1xSeparate level sensor connected to manual or automatic overfill prevention system (OPS-Sensor)

This is the recommended minimum configuration for most tank operations according to API 2350 and thereby considered as the industry best practice for most petroleum tanks. Today this configuration is typically compliant with any local regulation and external requirements from third parties such as insurance companies.

Level switches are well known and have historically been the typical choice for the OPS-Sensor. An example of a modern point-level configuration is depicted in [Figure 1-4](#). The key advantage with this type of sensor over a continuous level measurement is primarily the lower initial purchasing cost. The largest disadvantage is usually that level switches do not provide any online measurement and it is therefore virtually impossible to really know whether they are functioning correctly or not. As a result, level switches in practice typically require frequent proof-tests, which mean climbing the tanks if properly executed. This dangerous and labor-intensive procedure also results in tank (and possibly also process) downtime.

Figure 1-4. Traditional solution consisting of an automatic tank gauge (ATG) and an independent point-level sensor for the overfill prevention system (OPS-Sensor)



Investment calculations that also include a realistic view of the costs associated to proof-testing usually result in a fairly quick Return On Investment (ROI) for continuous level gauges, especially since they usually are a very small part of the overall project cost. Increased safety while at the same time generating less downtime and lower operational expenditures are some of the key reasons why the industry is rapidly transitioning from level switches to continuous level gauges also for OPS. Additional benefits include for example multiple (Hi and HiHi) and adjustable alarm-points and the capability to use the OPS-sensor to monitor the ATG (online transmitter surveillance) and if necessary act as a hot backup. Also there's a philosophical dimension to it - why use continuous level gauging for the ATG but settle for the second best option for the OPS-Sensor?

The dominant level measurement technology for ATGs being used in bulk liquid storage tanks has for a long time been non-contacting Radar⁽¹⁾. It is a well-proven technology that offers several advantages over traditional mechanical level technologies such as servo and float&tape: no moving parts and therefore very high mean time between failure (MTBF), unaffected by most fluid and tank atmosphere properties, stable custody-transfer grade accuracy, and no re-calibration or need for maintenance.

These two trends - continuous level also for the OPS-sensor and Radar technology for the ATG - are now converging and new installations today often consist of two Radar level gauges for both level and independent overfill prevention measurements. Two of the main reasons behind this transition is the high reliability of Radar technology combined with the efficient proof-testing procedure it offers. Because of the online measurement the latest generation of Radar level

(1) Radar Level Transmitters Global Market Research Study - Market Analysis and for Forecast through 2017, Arc Advisory Group, 2013

gauges can offer remote proof-testing capabilities. The test procedure can be initiated from the control- or maintenance room without any need to change the liquid level position and can therefore be completed within a few minutes. This is both safer and reduces the maintenance cost compared with traditional proof-testing procedures used by point-level sensors and less sophisticated continuous level gauges. Additionally, the use of two radar level gauges allows for fewer device types, which equals fewer spare-parts and a reduction in the need for device-specific training.

Figure 1-5. The industry trend is to use two continuous sensors for both level and overfill prevention measurements, here exemplified with Rosemount 5900 Radar Level Gauges



Existing tanks often have practical limitations that make safety upgrades with two separate level gauges cost prohibited:

- No tank opening available
- No measurement pipe available
- Pressurized tank that cannot be opened
- Hot tank work cannot be accepted
- Modifications may require tank to be taken out of service
- Difficult to modify floating roofs
- Tank's Custody Transfer Approval may become invalid
- Restrapping the tank due to modifications
- Tank may not pass a new pressure test

New tank projects may experience similar limitations where adding an extra nozzle or measurement pipe may result in additional costs.

One solution to these problems is the new product developed by Emerson upon request from end-users: Rosemount 5900 2-in-1 Non-contacting Radar Level Gauge. This level gauge consists

of two completely separate and independent electrical-units and a common antenna, as depicted in [Figure 1-6](#).

Figure 1-6. Rosemount 5900 2-in-1 Radar Level Gauge



When connected with the cables separated in different cable trays as illustrated in [Figure 1-7](#) and [Figure 1-8](#), a single Rosemount 5900 2-in-1 Radar Level Gauge can be used for both level (ATG) and separate overfill prevention (OPS-Sensor) measurements. As described in subsequent sections of this paper, this configuration has been verified by 3rd parties to be compliant with the requirements in both API 2350 and IEC 61511. The most obvious benefit is of course that it only requires a single tank opening. This solution allows for cost-efficient safety upgrades of existing tanks by replacing a single existing ATG (or OPS-Sensor) with two continuous level measurements with a minimum of tank modifications. Often Rosemount 5900 2-in-1 fits the antenna of earlier generations of Emerson's Radar Level Gauges and therefore require no tank modifications at all.

Figure 1-7. Rosemount 5900 2-in-1 used as both Automatic Tank Gauge and separate level sensor in a manual overfill prevention system (MOPS)

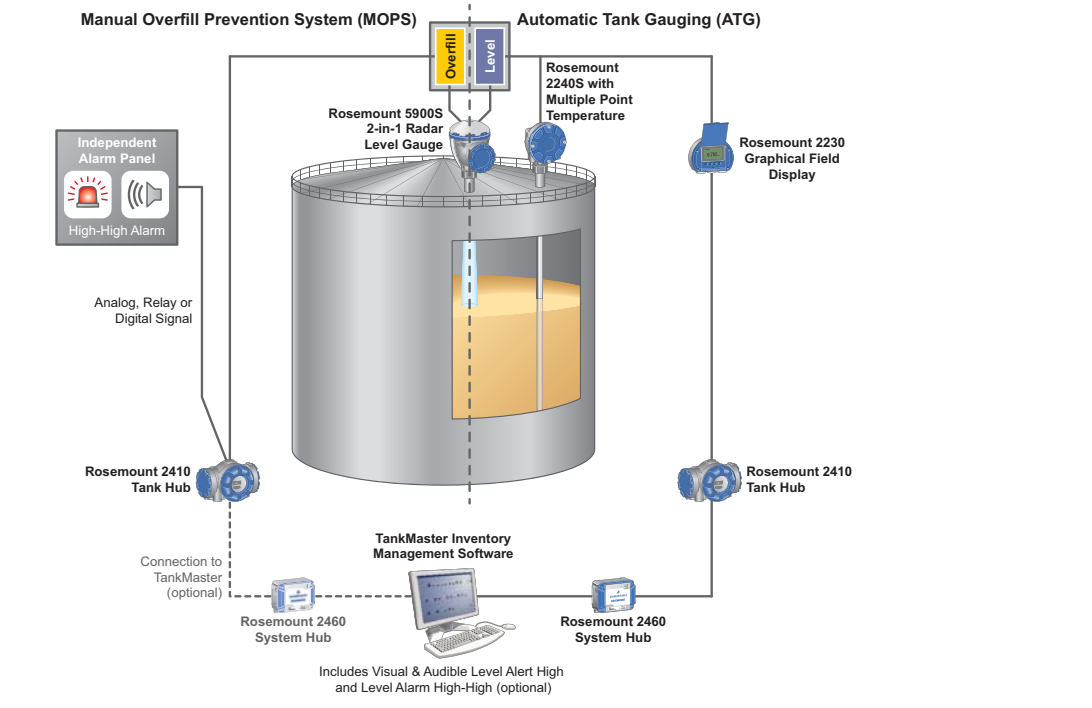
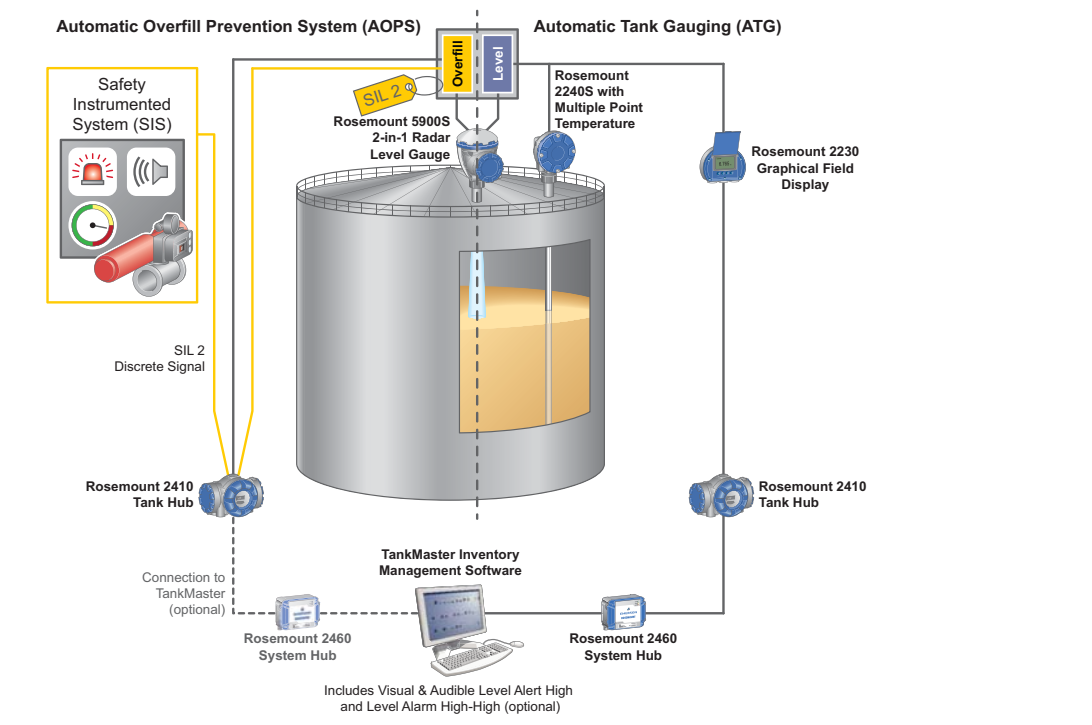


Figure 1-8. Rosemount 5900 2-in-1 used as both Automatic Tank Gauge and separate level sensor in a SIL 2 automatic overfill prevention system (AOPS) designed per IEC 61511

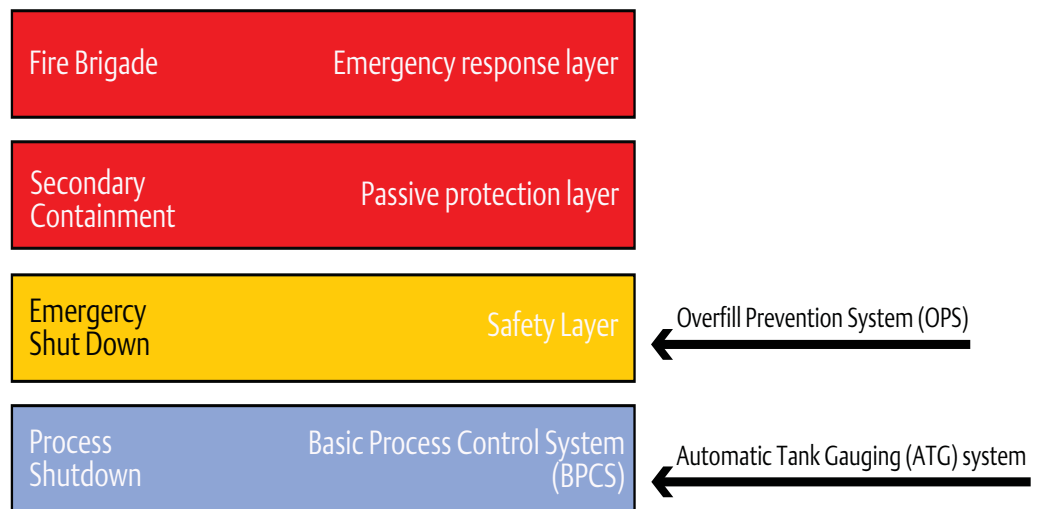


The Rosemount 5900 2-in-1 Radar Level Gauge has a large installed base and is in use by many of the largest global petroleum companies (examples provided in [Appendix A](#)). Nevertheless; it is a new technology and as any novel approach it will require a technical justification wherever relevant. Compared with traditional overfill prevention solutions there are two potential deviations: independence and technology diversification. The remainder of this paper will therefore investigate these two concepts in greater detail and provide a technical justification why this is an acceptable solution that fulfills the requirements of both API 2350 and IEC 61511.

1.3 Independent protection layers

Many company specifications, national regulations and industry standards prescribe, or at least recommend, the usage of a separate overfill prevention system independent of the automatic tank gauging system. Knowingly, or unknowingly, this requirement is based on the theoretical “Swiss cheese model” where independent protection layers (IPLs) are used in a layer of protection analysis (LOPA).

Figure 1-9. Example LOPA model for overfills consisting of multiple independent protection layers (IPL)



In the idealized LOPA model each IPL is designed to independently protect against the hazard for which they are designed to safeguard. As a result, the combined risk reduction factor (RRF) can simply be calculated by multiplying the individual IPLs' RRFs:

$$RRF_{Total} = \prod_{i=1}^n RRF_{IPL\# i} \text{ (where n equals the total number of IPLs)}$$

To take advantage of this simple model, industry best practices command each IPL to fulfill at a minimum the following requirements⁽¹⁾⁽²⁾:

- **Effective** in preventing the consequence when it functions as designed
- **Independent** of the initiating event and the components of any other IPL already claimed for the same scenario
- **Auditable**; designed to facilitate regular validation of the protective functions

A traditional overfill solution consisting of an ATG and ‘independent’ point-level sensor was previously presented in [Figure 1-4](#). Most people will intuitively believe that this configuration fulfills the requirements for two IPLs consisting of a basic process control system (BPCS) and a safety layer. If designed properly, the protection layers can obviously be made effective and auditable as required by an IPL. However, when the requirement for independence is investigated more carefully, the two layers will not fulfill a literal interpretation. A meteorite, earthquake, tsunami, flooding, aircraft crash, fire, explosion, power loss or tank failure will probably affect both layers and are examples of common cause failures (CCF).

Independence is a theoretical construct with a definite yes or no answer. The real world is however grey and in practice there exist no such thing as ‘full independence’. Modern safety standards such as IEC 61511 have therefore moved away from this digital interpretation of independence. Instead the existence of CCFs are recognized and as described in [Appendix A](#) typically quantified as a beta-factor (β). Rather than pretending that this problem does not exist this allows for an engineering approach to minimize the CCFs and places the focus on a much more important performance metric: the achieved risk reduction. The following comparison explains why ([Figure 1-10](#)):

- **Example Configuration #1** (idealized): BPCS with a fully independent safety instrumented function rated to safety integrity level (SIL) 2. Using the risk reduction numbers in IEC 61511, the achieved risk reduction for this configuration will be:

$$RRF_{BPCS+SIL2} = RRF_{BPCS} \cdot RRF_{SIL2} = 10 \cdot 100 = 1,000$$

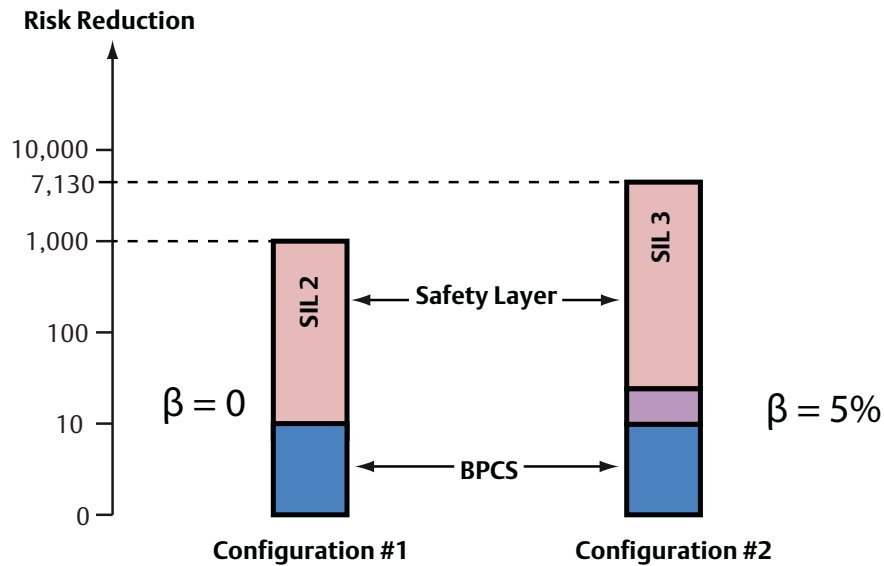
- **Example Configuration #2**: BPCS with non-independent safety instrumented function rated to safety integrity level (SIL) 3. The dependence between the BPCS and safety function has been estimated to 5%. Using the risk reduction numbers in IEC 61511, the achieved risk reduction for this configuration will be:

$$RRF_{BPCS + SIL3 + \beta = 5\%} = \frac{1}{\frac{(1 - \beta)^2}{RRF_{BPCS} \cdot RRF_{SIL3}} + \beta \cdot \frac{1}{RRF_{SIL3}}} = \frac{1}{\frac{(1 - 5\%)^2}{10 \cdot 1000} + 5\% \cdot \frac{1}{1000}} = 7130$$

(1) *Layer of Protection Analysis, Simplified Process Risk Assessment, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2001*

(2) *IEC 61511-3 Annex C*

Figure 1-10. Comparison of the achieved risk reduction with two example configurations:
 - Configuration #1: BPCS with SIL 2 safety layer and $\beta = 0$
 - Configuration #2: BPCS with SIL 3 safety layer and $\beta = 5\%$



From a risk reduction perspective, this example visualizes why example configuration #2 (lower likelihood to fail but non-independent) is preferable over configuration #1 (independent, but higher likelihood to fail). Obviously the reliability of a protection layer needs to be considered in parallel with the evaluation of its independence.

Traditionally the concept of independence has frequently been used in the process industry, although with a literal interpretation it is practically impossible to fulfill. Instead, the underlying intention of the requirement must be understood: to minimize the common cause failures to maximize the total risk reduction. When interpreted this way, the requirement provides some value that can actually be fulfilled.

The evolution in the interpretation of independence is an indication of the ongoing development in the process industry. The original intention is fulfilled while at the same time being more practical and also possible to implement in practice. It still requires consideration of the common cause failures but put these in perspective to an even more important performance metric, the risk reduction factor (RRF). This change in focus has been critical for the development of increased safety in the process industry because it has allowed equipment manufacturers to develop new novel solutions that actually focus on risk reduction - rather than fulfilling an impossible theoretical requirement.

1.4 Technology diversification

Failures can be split into two basic categories:⁽¹⁾

- **Systematic failures:** produced by human error during system development and operation. Will always appear when the circumstances are exactly the same. Examples include, but are not limited to, software bugs, incorrectly designed products and misapplications.
- **Random failures:** the result of corrosion, thermal stressing and wear-out that apply to simple hardware components within a system. Appear randomly and can be described with a probabilistic model.

Random failures are typically addressed by using hardware fault tolerance (redundancy) whereas systematic failures are the result of human errors and therefore need to be addressed differently.

A commonly employed technique to minimize the likelihood of systematic failures is product and technology diversification. This is however only one of several methods. For example IEC 61511 uses a life-cycle approach where some of the key components to minimize the likelihood of systematic failures are qualified personnel, written and agreed procedures and specifications, proper planning, thorough reviews, management of change and testing. The measures that have been undertaken to avoid systematic failures is described as 'systematic capability' and is quantified according to IEC 61511 in safety integrity levels (SIL) 0 - 4, just as random hardware failures.

(1) John Robert Taylor (1999). *An Introduction to Error Analysis: The Study of Uncertainties in Physical Measurements*. University Science Books. p. 94, §4.1. ISBN 0-935702-75-X.

Section 2 Technical Evaluation

Independence	page 14
Technology diversification	page 16

This entire section assumes that the Rosemount 5900 2-in-1 Radar Level Gauge has been connected as depicted in [Figure 1-7](#) or [Figure 1-8](#).

Table 2-1. Overview Rosemount 5900 2-in-1

Property	Specification
Description	Rosemount 5900 2-in-1 Non-contacting Radar Level Gauge
Principal components	Two electrical-units which are physically and electrically separated through galvanic isolation. One antenna which is shared between the two electrical units.
Accuracy	Two independent level measurements with 0.5 mm custody-transfer certified accuracy per OIMLR85:2008.
Measurement technology	Each electrical-unit transmits and receives a linear FMCW Radar signal (9.25 -10.75 GHz) @ 3 times / second. The two electrical-units can detect and disregard the interference from each other which statistically occurs once every 1 million measurements (approx once every 5 days).
Cabling (including Power)	Complete separation between the two electrical-units with galvanic isolation and separate cable outlets.
Quality Approvals (example)	ISO 9001:2008, ISO 14001:2004
Overfill Prevention Certificates (examples)	<ul style="list-style-type: none"> ■ IEC 61508 Certificate (Appendix D)⁽¹⁾: <ul style="list-style-type: none"> □ Random Hardware Integrity: SIL 2 □ Systematic Capability: SIL 3 ■ API 2350 Ed 4: Compliant with category 3 requirements (Appendix F) ■ Germany: TÜV/DIBt WHG ■ Switzerland: SVTI ■ US: Florida Department of Environmental Protection's (FDEP) ■ Belgium: Vlare 2
Failure Rates	<p>Mean time between failure (MTBF) according to Table A-1 is 97 years for the complete unit including two electrical-units and the antenna. Additional failure data (e.g. segmented into dangerous undetected failures) can be found in the IEC 61508 Certificate (Appendix D).</p> <p>The MTBF for the individual parts:</p> <ul style="list-style-type: none"> ■ Antenna: 45,400 years ■ Electrical-unit: 194 years

(1) The Rosemount 5900 2-in-1 is also available in a configuration for dedicated service in the safety layer where a single non-redundant fulfills the random hardware integrity requirements of SIL 3. Refer to Exida IEC 61508 certificate 'ROS 1312032 C001' for further details.

Figure 2-1. Scope of the Rosemount 5900 2-in-1 SIL 2 IEC 61508 Certificate (Appendix D)



2.1 Independence

A comparison of the Rosemount 5900 2-in-1 against the basic requirements for an IPL generates the following result:

IPL Requirement	Rosemount 5900 2-in-1 Compliant?	Comments
Effective	Yes	Provides level measurement data to BPCS and Safety layers, both which can be designed to prevent an overflow
Independent	$\beta = 0.4\%$ or 2% depending on assessment technique (Table 2-2)	Owner/Operator to determine if this is acceptable. Detailed information available in subsequent paragraphs.
Auditable	Yes	Proof-test procedure available in the safety manual

Appendix A contains quantitative assessments of the beta-factor for Rosemount 5900 2-in-1 using two different techniques. The result is presented in Table 2-2. The essential difference between the two techniques is that one is a quantitative method that only evaluates the random hardware failures, whereas other is a qualitative method that also takes the systematic failures into account.

Table 2-2. Rosemount 5900 2-in-1 Beta factors according to Appendix A

Assessment Method	β
Random Hardware Failures	0.4%
IEC61508-6 model for Systematic and Random Hardware Failures	2%

The resulting effect of the beta-factors on the risk reduction factor (RRF) is presented in Table 2-3.

Table 2-3. Comparison of the achieved risk reduction including BPCS with SIL 2 safety layer and varying beta factor. This corresponds to a Rosemount 5900 2-in-1 as described in Figure 1-8

Assessment Method	Beta-factor (β) ⁽¹⁾	Risk Reduction ⁽²⁾
Random Hardware Failures	$\beta=0.4\%$	970
IEC61508-6 model for Systematic and Random Hardware Failures	$\beta=2\%$	860

(1) Rosemount 5900 2-in-1 Beta factors according to Appendix A

(2) Assumptions: BPCS risk reduction factor equals 10, and the SIS risk reduction factor equals 100 (SIL 2 lower limit).

An idealized overfill prevention solution with zero CCF ($\beta=0\%$) between the BPCS and safety SIL 2 safety layer will have RRF of 1,000. Consequently; under a worst-case assumption that the beta-factor equals 2% the following question emerges: is a decrease in the risk reduction to 860 acceptable? This is ultimately a question for the owner/operator of the tank facility to decide.

2.1.1 Putting numbers in perspective

When evaluating the common cause failures associated with the Rosemount 5900 2-in-1 it needs to be put in perspective and compared with the alternatives. A configuration that is commonly acceptable is the usage of two separate Rosemount 5900 as the ATG and independent OPS-sensor as depicted in Figure B-1. However this solution does not fulfill a literal interpretation of the requirement independence since the solution uses a single tank, tank roof and potentially also a single tank connection or flange.

Appendix B presents an assessment of the CCF based on random hardware failures when also the tank integrity has been taken into consideration. A comparison of the achieved risk reduction for a Rosemount 5900 2-in-1 compared to two separate Rosemount 5900 1-in-1 is presented in Table 2-4.

Table 2-4. Comparison of the achieved risk reduction including BPCS with SIL 2 safety layer and beta factor according to Appendix B

Components	Beta-factor (β)	Risk Reduction
2xRosemount 5900 1-in-1 Radar Level Gauges 1xAtmospheric Storage Tank (Figure B-1)	1.9%	870
1xRosemount 5900 2-in-1 Radar Level Gauge 1xAtmospheric Storage Tank (Figure B-2)	2.3%	840

In this context it is relevant to apply the British principle of as low as reasonably practicable (ALARP). Investigations that were a consequence to the Buncefield-accident have showed that the overfill risk associated with a typical tank farm equipped with a level gauge and independent overfill prevention system falls into the ALARP-category⁽¹⁾. According to the U.K. legislation risk reduction measures in this category shall be decided based on proportionality. For example, installing an additional pipe in a floating roof tank to switch from a Rosemount 5900 2-in-1 to two separate Rosemount 5900 to achieve an increase in RRF from 840 to 870 would obviously be considered as a disproportionate measure that is not required. But ultimately this is a question for the local owner/operator of the tank facility to decide.

(1) Illustrative model of a risk based land use planning system around petroleum storage sites, Buncefield Major Incident Investigation Board, Rev 0, June 2008

2.2 Technology diversification

Diversification is not a requirement according to any of the recognized global standards for overfill prevention, API 2350 and IEC 61511. Nevertheless; extensive measures have been taken during the design of the Rosemount 5900 2-in-1 to minimize systematic failures and to ensure compliance with this (non-existing) requirement:

- **The parts with redundancy (the electrical units) employ diverse technologies.**
 - Rosemount 5900 2-in-1 contains different circuit boards, internal signal paths, firmware and signal processing algorithms for the two electrical-units used for ATG and SIL high/low-alarm output signal.
- **The common parts (the antenna) have been thoroughly evaluated and designed in such a way to minimize the probability of systematic failures.**
 - **Verification:** The Rosemount 5900 has been installed on more than 10,000 tanks. Every product return undergoes a root-cause failure analysis and corrective action according to a strict quality procedure fulfilling ISO 9001 and IEC 61508 requirements.
 - **Certification:** Rosemount 5900 has been designed according to IEC 61508. The 'systematic capability' fulfills safety integrity level (SIL) 3, which equals a higher risk reduction factor (1,000) than any of the claimed total risk reduction factors when using the Rosemount 5900 2-in-1 for both BPCS and SIS layers (Table 2-3).

Section 3 Standards Compliance

API 2350 Edition 4	page 17
IEC 61511 Edition 1	page 17

3.1 API 2350 Edition 4

API 2350 separates overfill prevention solutions into three different categories. None of the categories require any technology diversification and category #1 and #2 do not require any independent overfill prevention sensor. For category #3 solutions this is however a requirement (4.4.5.4.1):

A Category 3 overfill prevention system uses both an ATG and an independent level alarm high-high sensor (LAHH)

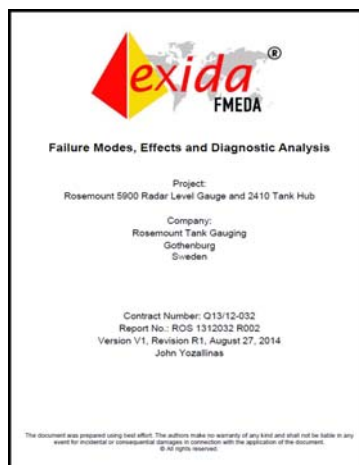
API 2350 defines 'independent sensor' as (3.26)

A sensor that is not used in the ATG system

This definition is explained in further detail along with the standard's intent by Philip E. Myers, the API 2350 Edition 4 committee chairman, in [Appendix F](#). According to Mr Myers' letter in [Appendix E](#), the Rosemount 5900 2-in-1 fulfills the category #3 requirements for ATG and independent OPS-Sensor.

3.2 IEC 61511 Edition 1

The Rosemount 5900 2-in-1 has been certified to IEC 61508 by the accredited 3rd party assessor Exida ([Appendix D](#)). The overfill prevention sensor fulfills the requirements up to safety integrity level (SIL) 2 when the Rosemount 5900 2-in-1 is used as two level sensors connected to a BPCS and independent overfill prevention system simultaneously as depicted in [Figure 1-8](#). According to Exida⁽¹⁾:



“There is no requirement for diverse separation according to IEC 61511 and the safety architecture option “SIL 2 2-in-1” may therefore be used simultaneously for service in both BPCS layers and Safety layers. However any potential systematic and common cause failures must be taken under consideration and the risk reduction factor of the safely layer must be de-rated appropriately”

Exida has also issued a separate letter confirming that the Rosemount 5900 2-in-1 can be used as a BPCS and SIL 2 safety sensor simultaneously ([Appendix G](#)).

Common cause failures can be taken into account using the beta-factor model and the values presented in [Table 2-2](#).

Consequently the Rosemount 5900 2-in-1 fulfills the requirement of IEC 61511 to serve as the level sensor in two independent protection layers (i.e. BPCS and SIS).

(1) John Yozallinas, Exida, Results of the IEC 61508 Functional Safety Assessment, Rosemount 5900 Radar Level Gauge and 2410 Tank Hub, ROS 1312032 R001, 2014

Section 4 Conclusion

Rosemount 5900 2-in-1 Radar Level Gauge is a new technology that allows a single tank opening to be used for both level (ATG) and separate overfill prevention (OPS-Sensor) measurements. This solution offers substantial cost savings compared to using two separate level sensors.

The Rosemount 5900 2-in-1 has been verified by a third part ([Appendix F](#)) to be compliant with the category 3 requirements in the global overfill prevention standard API 2350 if connected properly with the cables separated in different cable trays ([Figure 1-8](#)). A third party has also verified that the Rosemount 5900 2-in-1 fulfills the requirements of IEC 61511 to be used simultaneously as a BPCS and SIL 2 AOPS ([Appendix D](#)).

This novel technology that the Rosemount 5900 2-in-1 offers is based on a single antenna which theoretically is a source of CCF. Consequently, it is better to use two separate Rosemount 5900 if possible ([Table 2-4](#)). However, the likelihood of the antenna failing is very low and the influence on the overall risk for an overfill is usually negligible. An estimation of the exact figures has been presented in this document and whether to apply this solution as two independent protection layers for BPCS and SIS is ultimately the responsibility of the owner/operator of the facility. However, the experience so far is that Rosemount 5900 2-in-1 fulfills any practically viable definition of independence and the risk associated with the common antenna is smaller than the risk associated with most atmospheric storage tanks themselves. As shown in this document, according to British law the small gain in risk reduction that can be obtained by exchanging a Rosemount 5900 2-in-1 to two Rosemount 5900 is considered disproportionate.

For any practical purpose it can be concluded that the Rosemount 5900 2-in-1 Radar Level Gauge technically qualifies to be used as the sensor in two independent protection layers (i.e. BPCS and SIS) if connected properly.

Appendix A Common cause Failure Assessment of Rosemount 5900 2-in-1 & 2x5900 1-in-1

Definitions	page 21
Methodology	page 22
Comparison objects	page 23
Summary	page 27

A.1 Definitions

Common Cause Failure (CCF) is according to IEC 61511-1 Edition 1 defined as a

“failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure”

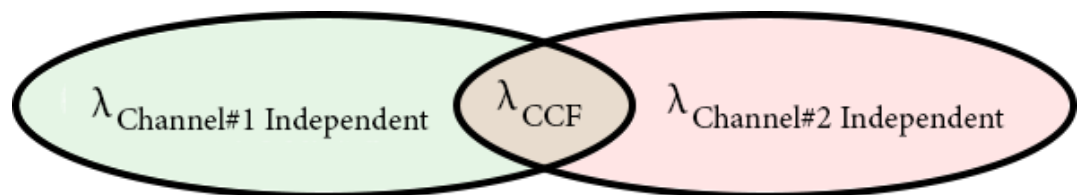
It is commonly quantified using the “beta-factor model”⁽¹⁾ where failures are separated into two categories: independent and common cause. According to this model, the failure-rate λ for a two channel system can be described as

$$\lambda_{\text{Channel\#1}} = \lambda_{\text{Channel\#1 Independent}} + \lambda_{\text{CCF}} \text{ (Equation \#1)}$$

$$\lambda_{\text{Channel\#2}} = \lambda_{\text{Channel\#2 Independent}} + \lambda_{\text{CCF}} \text{ (Equation \#2)}$$

The failure-rates can then be visualized as depicted in Figure A-1.

Figure A-1. Failure-rate segmentation according to the beta-factor model in a two-channel system.



(1) Probabilistic Risk Analysis: Foundations and Methods, Tim Bedford, Roger Cooke, 2001

In the case of identical redundancy the total failure rate for one channel can be denoted

$$\lambda_{\text{Channel}} = \lambda_{\text{Channel\#1}} = \lambda_{\text{Channel\#2}} \text{ (Equation \#3)}$$

and as a consequence the independent failures must also be equal

$$\lambda_{\text{Independent}} = \lambda_{\text{Channel\#1 Independent}} = \lambda_{\text{Channel\#2 Independent}} \text{ (Equation \#4)}$$

and then finally the beta-factor can be defined as

$$\beta := \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Channel}}} = \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Independent}} + \lambda_{\text{CCF}}} \text{ (Equation \#5)}$$

A.2 Methodology

The total failure rate, which consists of both random and systematic failures, is virtually impossible to obtain in practice and it is consequently not possible to calculate the ‘true’ beta-factor. However, two techniques commonly used to estimate the beta-factor are:

1. Probabilistic calculation based on Random Hardware Failures
2. IEC61508-6 checklist for assessment of systematic and random common cause failures

The major difference between the two techniques is that the IEC61508-6 method uses a qualitative method that also includes the effects of systematic failures. Consequently this method generally generates higher estimates of the beta-factor than the quantitative method based purely on random hardware failures. Both techniques have been employed in this report and are presented separately.

A.3 Comparison objects

To simplify the interpretation of the beta-factor it will be calculated for two typical configurations, as depicted in configurations A1 and A2 below. External factors such as cabling and the tank itself are excluded.

Figure A-2. Configuration A1: Two independent Rosemount 5900 1-in-1 Radar Level Gauges



Figure A-3. Configuration A2: Single Rosemount 5900 2-in-1 Radar Level Gauge

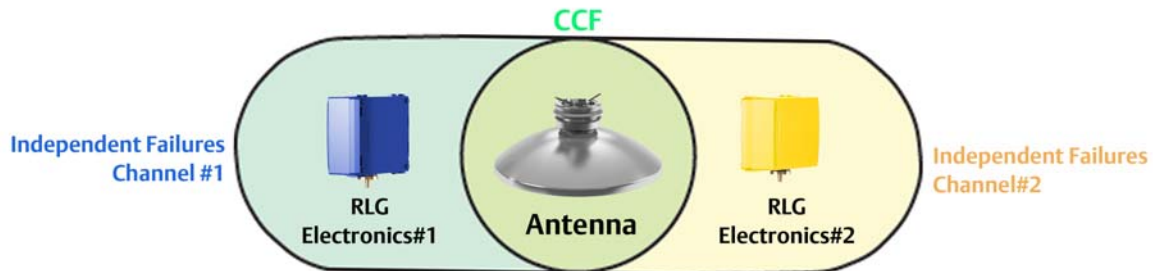


A.4 Beta-calculation technique #1: Random Hardware Failures

Configuration A1 consists of two independent radar level gauges which have no common hardware components. Consequently from a random hardware failure perspective the beta-factor is zero.

Configuration A2 consists of a single 2-in-1 radar level gauge which principally consists of three components: two electronic units and one antenna. The two electronic units are completely separated and can therefore be considered to be independent from a random hardware failures perspective. The antenna is however shared, and an obvious source of common cause failures. The result is visualized in Figure A-3.

Figure A-4. Failure-rate segmentation Rosemount 5900 2-in-1 (configuration A2)



Using the definition of the beta-factor (Equation #5) and the failure rate data in Table A-1 combined with the fact that $\lambda=1/\text{MTBF}$ provide the following results:

$$\beta_{\text{ConfigurationA1}} := \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Independent}} + \lambda_{\text{CCF}}} = \frac{0}{\lambda_{\text{Independent}} + \lambda_{\text{CCF}}} = 0\% \text{ (Equation \#6)}$$

$$\beta_{\text{ConfigurationA2}} := \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Independent}} + \lambda_{\text{CCF}}} = \frac{\frac{1}{45,400}}{\frac{1}{194} + \frac{1}{45,400}} = 0.4\% \text{ (Equation \#7)}$$

Table A-1. Random Hardware Failure Data

Item	MTBF (years)	Source
RLG 1-in-1	193	Rosemount 5900 1-in-1 MTBF according to document 502020en revision AA. MTBF RLG 2-in-1 can be estimated to $1/(1/193+1/193+1/45,400)=97$ years.
Antenna	45,400	Field-experienced MTBF according to Saab Ericsson Space report D-LR-REP-5077-SE "Reliability Analysis of Parabolic Antenna" Revision 2.
RLG Electronics	194	Calculated based on RLG and Antenna failure data: $1/(1/193-1/45,400)$.

A.5 Beta-calculation technique #2: Random and Systematic failures

A completely different approach to estimating the beta-factor is provided in IEC61508-6 Edition 2 Annex D: “A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems”. It is a qualitative method based on industry experience that takes both random hardware and systematic failures into account.

According to the results in Table A-2 combined with IEC 61508-6 Table D4 the beta-factor can using this method be estimated to

$$\beta_{ConfigurationA1} = 2\% \text{ (Equation \#8)}$$

$$\beta_{ConfigurationA2} = 2\% \text{ (Equation \#9)}$$

Table A-2. Scoring according to IEC61508-6 table D1

Item	Configuration A1		Configuration A2	
	Yes / No	Score	Yes / No	Score
Are all signal cables for the channels routed separately at all positions?	Yes	3	Yes	3
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	Yes	4	Yes	4
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?	Yes	3	No	0
Do the devices employ different physical principles for the sensing elements, e.g., pressure and temperature, vane anemometer and Doppler transducer, etc?	No	0	No	0
Do the devices employ different electrical principles/designs, e.g., digital and analogue, different manufacturer (not re-badged) or different technology?	No	0	No	0
Are separate test methods and people used for each channel during commissioning?	No	0	No	0
Is maintenance on each channel carried out by different people at different times?	No	0	No	0
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	Yes	1	Yes	1
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	Yes	2	Yes	2
Is there more than 5 years experience with the same hardware used in similar environments?	Yes	3	Yes	3
Are inputs and outputs protected from potential levels of over-voltage and over-current?	Yes	2	Yes	2
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	Yes	2	Yes	2
Have the results of the FMEA or FTA been examined to establish sources of CCF and have predetermined sources of CCF been eliminated by design?	Yes	3	Yes	3

Table A-2. Scoring according to IEC61508-6 table D1

Item	Configuration A1		Configuration A2	
	Yes / No	Score	Yes / No	Score
Were CC failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)	Yes	3	Yes	3
Are all field failures fully analysed with feedback into the design? (Documentary evidence of the procedure is required.)	Yes	4	Yes	4
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?	Yes	2	Yes	2
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	Yes	3	Yes	0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.), intended to be independent of each other, are not to be relocated?	Yes	1	Yes	1
Is all maintenance of printed-circuit boards, etc. carried out off site at a qualified repair center and have all the repaired items gone through a full pre-installation testing?	Yes	2	Yes	2
Does the system diagnostic tests report failures to the level of a field-replaceable module?	Yes	2	Yes	2
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	Yes	5	Yes	5
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	Yes	5	Yes	5
Is personnel access limited (for example locked cabinets, inaccessible position)?	Yes	3	Yes	3
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	Yes	4	Yes	4
Are all signal and power cables separate at all positions?	Yes	3	Yes	3
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognised standards?	Yes	20	Yes	20
Total		80		74

For sensors, a score of 70 to 120 corresponds to a beta-factor of 2% according to IEC 61508-6 Table D4.

A.6 Summary

Table A-3. Estimate of Rosemount 5900 Beta-factors

Assessment technique	Configuration A1 (2xRosemount 5900 1-in-1 RLG)	Configuration A2 (1xRosemount 5900 2-in-1 RLG)
Random Hardware Failures	0%	0.4%
IEC61508-6 model for Systematic and Random Hardware Failures	2%	2%

Appendix B Common Cause Failure Assessment of Rosemount 5900 2-in-1 & 2x5900 1-in-1 Including the Tank

In this section the beta-factor (refer to [Appendix A](#) for definition) will be calculated based on the random hardware failures for two typical system layouts, as depicted below.

Figure B-1. System layout B1: Tank with two independent Rosemount 5900 1-in-1 Radar Level Gauges

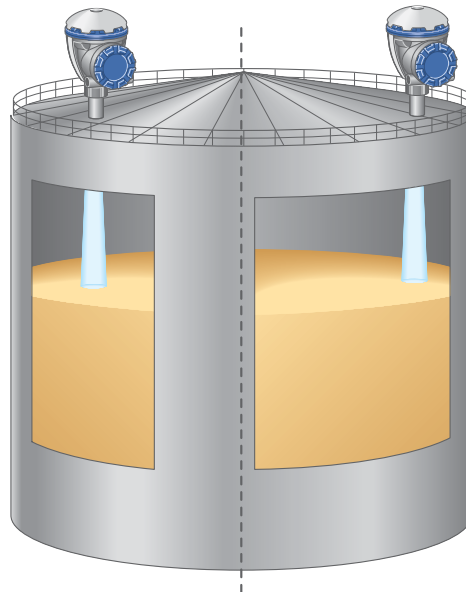
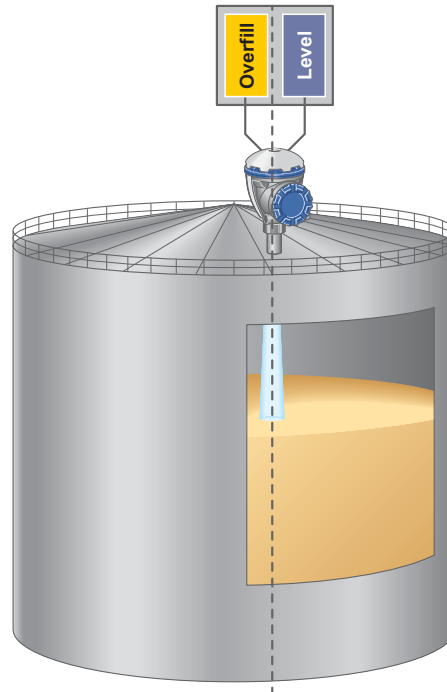
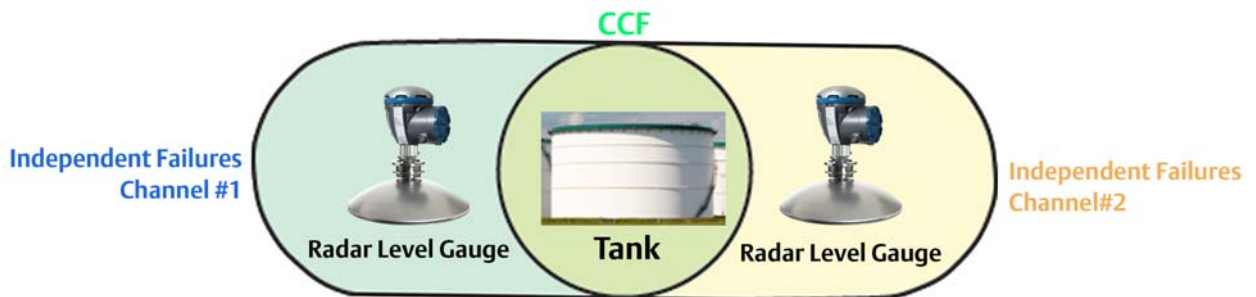


Figure B-2. System layout B2: Tank with single Rosemount 5900 2-in-1 Radar Level Gauge



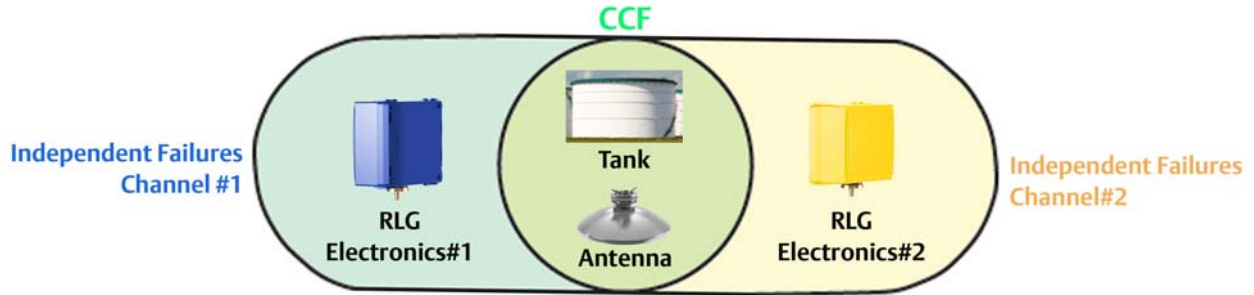
System Layout B1 consists of three principal components: Radar Level Gauge (RLG) #1, Radar Level Gauge (RLG) #2 and the tank. The two Radar Level Gauges can be assumed to be independent from a random hardware failure perspective and the only source of common cause failures is therefore the tank, which is visualized in Figure B-3.

Figure B-3. Failure-rate segmentation System Layout B1



System Layout B2 also consists of a single tank which is an obvious source of common cause failures. Additionally it consists of a 2-in-1 Radar Level Gauge that has two independent electronic-units and a common antenna, which is another source of common cause failures. The result is visualized in Figure B-4.

Figure B-4. Failure-rate segmentation System Layout B2



Using the definition of the beta-factor (Equation #5) and the failure rate data in Table B-2 combined with the fact that $\lambda = 1/\text{MTBF}$ provide the following results:

$$\beta_{\text{System Layout B1}} = \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Channel}}} = \frac{\lambda_{\text{Tank}}}{\lambda_{\text{RLG}} + \lambda_{\text{Tank}}} = 1.9\%$$

$$\beta_{\text{System Layout B2}} = \frac{\lambda_{\text{CCF}}}{\lambda_{\text{Channel}}} = \frac{\lambda_{\text{Tank}} + \lambda_{\text{Antenna}}}{\lambda_{\text{RLG Electronics}} + \lambda_{\text{Antenna}} + \lambda_{\text{Tank}}} = 2.3\%$$

Table B-1. Random Hardware Failure Data

Item	MTBF (years)	Source
Tank	10,000	HSE-report "Failure Rate and Event Data refers to major releases and for use within Land Use Planning Risk Assessments". Data assumes fixed position, single walled vessels with a capacity greater than 450m3, which operate at ambient temperature and pressure.
RLG	193	Rosemount 5900 1-in-1 MTBF according to document 502020en revision AA.
Antenna	45,400	Field-experienced MTBF according to Saab Ericsson Space report D-LR-REP-5077-SE "Reliability Analysis of Parabolic Antenna" Revision 2.
RLG Electronics	194	Calculated based on RLG and Antenna failure data: $1/(1/193-1/45,400)$.

Table B-2. Beta-factor estimate based on random hardware failures

System Layout	Components	Beta-factor (β)
B1	2xRosemount 5900 1-in-1 Radar Level Gauges 1xAtmospheric Storage Tank	1.9%
B2	1xRosemount 5900 2-in-1 Radar Level Gauge 1xAtmospheric Storage Tank	2.3%

Preliminary Rev 02

**Common Cause Failure Assessment of Rosemount 5900S 2-in-1 &
2x5900S 1-in-1 including the Tank**

April 2016

White Paper

00870-0100-5900, Rev AA

Appendix C Example Rosemount 5900 2-in-1 Users



SIL 3 certified

Example of Tank Gauging installations
Rosemount 5900S 2-in-1 radar units

5900S 2-in-1
Two radar gauges in one housing – independent level measurement and overfill alarm. SIL 2 and SIL 3 certified.

End user	Country	Units
Caltex Ref. Kurnell /Ampol	Australia	53
Pacific Terminals (Australia) Pty	Australia	24
Origin Energy LPG Limited	Australia	19
Shell Pinkenba Bitumen	Australia	3
Caltex Refineries Ltd	Australia	2
Caltex/Ampol Terminal Banksmeadow	Australia	1
Pacific Terminals Devonport	Australia	1
Puma Energy Holdings Pty Ltd	Australia	1
OMV Refining &Marketing GMBH	Austria	9
Raizen	Brazil	2
Shell Canada	Canada	15
Gibsons	Canada	4
Keyera Partnership	Canada	3
Pembina Pipeline	Canada	3
Gibson Energy - Edmonton	Canada	1
Ultramar	Canada	1
Shell Huabei Petroleum Group Co.	China	13
Anqing Kaimeite Gas Co Ltd	China	3
Solmico Oil S.A.S	Colombia	6
RECOPE Refinery	Costa Rica	12
Cepro Loukov	Czech Republic	4
Statoil Kalundborg Dk.	Denmark	3
Alba Petroleos	El Salvador	8
Valero Pembroke	Great Britain, UK	7
BP Exploration Grangemouth	Great Britain, UK	6
Indian Oil Corp Ltd - Panipat	India	10
IOCL Haldia Refinery	India	4
Reliance Ind Ltd JNPT Terminal	India	3
CPCL	India	2
CTTL Chemical Terminal Trombay	India	1
Pertamina Upms III	Indonesia	16
Basrah Gas Company	Iraq	2
Conocco Phillips	Ireland	1
Esso Italiana Srl, Vado Ligure	Italy	3
Oryx Energie	Ivory Coast	1
Kuwait Oil Company (KOC)	Kuwait	1
Waha Oil Company	Libya	19
Sirte Oil Company	Libya	1
Shell Malaysia Trading, West Port	Malaysia	11
Gas de Calidad	Mexico	16
Mexichem CID SA de CV	Mexico	1
Pemex Refinacion	Mexico	1
Vivo Energy Maroc	Morocco	5
Independant Petroleum Terminal SARL	Mozambique	9
Refineria Panama	Panama	14
Chevron, Panama	Panama	12
Decal Panama, S.A.	Panama	12



Page 1(3)





5900S (2-in-1)
Two radar gauges in one housing – independent level measurement and overflow alarm. SIL 2 and SIL 3 certified.

Example of Tank Gauging installations Rosemount 5900S 2-in-1 radar units

End user	Country	Units
Teixeira Duarte SA	Portugal	6
Luberef	Saudi Arabia	52
SADARA Chemical CO	Saudi Arabia	20
Saudi Aramco Ras Tanura Refinery	Saudi Arabia	20
GFPC, Gulf Farabi Petrochemical Co Ld	Saudi Arabia	13
Saudi Electric Co	Saudi Arabia	4
Saudi Aramco Dhahran Bulk plant	Saudi Arabia	1
NIS-Naftagas Promet	Serbia	1
Chevron Oronite Pte Ltd	Singapore	25
Shell Malaysia Trading, West Port	Singapore	4
PetroSA Voorbaai Mossel Bay	South Africa	6
SASOL	South Africa	6
Aveng Manufacturing	South Africa	1
Ulsan Aromatics Co Ltd	South Korea	3
Hyosung Tank Terminal CO., LTD.	South Korea	1
Samsung Total Petrochemicals	South Korea	1
CLH Algeciras	Spain	9
BP Oil Refineria De Castellon, SAU	Spain	4
CEPSA Ertoil Huelva	Spain	2
NYNÄS REFINING AB	Sweden	25
Preem AB	Sweden	17
Karlshamns Kraft AB	Sweden	7
Nynas AB	Sweden	1
CPC Tao Yuan Plant	Taiwan	1
Formosa Plastics	Taiwan	1
Star Petroleum Refining Co.Ltd	Thailand	6
Thai Lube Base Public Co. Ltd.	Thailand	2
PTT Chemical Public Company LTD.	Thailand	1
Tüpras, TürkiyePetroRafinerileri A.S	Turkey	2
New York Terminals	United States	36
Buckeye Terminals LLC	United States	35
Tesoro Refinery	United States	25
EF 90 LLC	United States	24
Chevron	United States	20
Shell Oil Products Martinez	United States	18
Catlettsburg Refining	United States	11
Tesoro	United States	10
Tesoro Hawaii Corporation	United States	10
Shell Oil Products	United States	9
BP Products	United States	6
Tesoro Alaska	United States	6
Phillips 66 Co.	United States	5
ConocoPhillips, Linden	United States	4
Flint Hills Resources	United States	4
Enbridge Energy	United States	3
Koch Pipeline Company	United States	3
Phillips 66 Co. - Arroyo Grande	United States	3

Example of Tank Gauging installations Rosemount 5900S 2-in-1 radar units



**SIL 3
certified**

5900S (2-in-1)
Two radar gauges in one housing – independent level measurement and overfill alarm. SIL 2 and SIL 3 certified.

End user	Country	Units
Huntsman Corp	United States	2
Nustar Asphalt Refining	United States	2
Chevron Products Co	United States	1
Marathon Ashland Petroleum	United States	1
Oiltanking Texas City	United States	1
Phillips 66	United States	1
Valero Benicia	United States	1
PV Gas ThiVai LPG terminal	Vietnam	14

© Rosemount Tank Radar AB, June 2014.

www.rosemount-tg.com

ROSEMOUNT
Tank Gauging

Page 3(3)


EMERSON
Process Management

Preliminary Rev 02

Example Rosemount 5900S 2-in-1 Users
April 2016

White Paper
00870-0100-5900, Rev AA

Appendix D Rosemount 5900 2-in-1 SIL 2 IEC 61508 Certificate



The manufacturer may use the mark:



Valid until September 1, 2017
Revision 1.1 Aug 27, 2014



ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat Zertifikat / 合格証

ROS 1312032 C003

exida hereby confirms that the:

**5900 Radar Level Gauge and 2410 Tank Hub
(Rosemount Tank Gauging System)
SIL 2 2-in-1 (1oo1) Option**

**Rosemount Tank Gauging
Gothenburg, Sweden**

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

**Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element
SIL 2 @ HFT = 0; Route 1_H
PFH / PFD_{AVG} and Architecture Constraints
must be verified for each application**

Safety Function:
The level transmitter will de-energize a safety critical output when exceeding any of the configured alarm limits within the stated accuracy and within the specified demand response time.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.





Evaluating Assessor



Certifying Assessor

Page 1 of 2

37

Appendix E Rosemount 5900 2-in-1 Compliance with API 2350 Category 3 Requirements



PEMY Consulting

Report

925-356-1294

RE: Compliance with API 2350 Category 3 requirements

After reviewing the principal design of the Rosemount Tank Gauging System described in figure 1 I hereby testify that it is compliant with the category 3 requirements in API2350 edition 4.

Philip E. Myers;
API2350 Committee Chairman

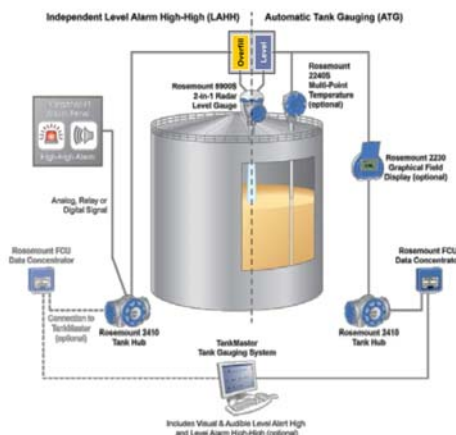


Figure 1: Rosemount Tank Gauging System

About the author



Philip E. Myers, API2350 Committee Chairman

Myers has chaired numerous task groups for the American Petroleum Institute, including API2350. Currently, he is the director of PEMY Consulting. He has also worked at Chevron Corporation where he was a mechanical integrity specialist for tanks, piping and pressure vessels specializing in safety and risk. Myers holds a BS in Chemical Engineering from UC Berkeley and an MS in Theoretical and Applied Statistics from California State University.

Philip E. Myers

phil@pemyconsulting.com

Appendix F API 2350 Ed 4 Interpretation



PEMY Consulting

Report

925-356-1294

RE: Interpretation of the wording “Independence” in API2350:4

Below is an excerpt from the informative Annex A in API2350 Edition 4:

A.3 Independence

The term “independent” means that the AOPS shall be separate from any device or method used to measure, calculate or monitor tank receipts. The independent AOPS shall be designed and installed such that no fault in the ATG gauging/monitoring system is capable of causing a fault in the AOPS.

On first reading, one might be led to the conclusion that two identical level gauges cannot be used where one is for the tank level gauging function and the other is for the purpose of initiating the AOPS system (or an independent alarm system), as it says that that independent means separate devices and methods. If the devices are using the same method of measurement then one might conclude that such use of instrumentation is prohibited by this language. However, this was not the intent of the committee. It might be clearer to read the particular sentence this way, “The term “independent” means that the AOPS shall be separate from any device or method used to measure, calculate or monitor tank receipts.” If the bold underscore wording is read to mean automatic tank gauge or gauging system, then the sentence reads, “independent means that the AOPS shall be separate from any automatic tank gauge or gauging system.” Clearly, two automated tank gauges may independently serve the function of ATG and AOPS sensor. Alternatively, two automated tank gauges may interdependently serve the function of ATG and alarm. It was this interpretation that the committee intended when drafting language regarding independence

Philip E. Myers;
API2350 Committee Chairman

About the author



Philip E. Myers, API2350 Committee Chairman

Myers has chaired numerous task groups for the American Petroleum Institute, including API2350. Currently, he is the director of PEMY Consulting. He has also worked at Chevron Corporation where he was a mechanical integrity specialist for tanks, piping and pressure vessels specializing in safety and risk. Myers holds a BS in Chemical Engineering from UC Berkeley and an MS in Theoretical and Applied Statistics from California State University.

Philip E. Myers

phil@pemyconsulting.com

Appendix G Rosemount 5900 2-in-1 Compliance with IEC 61511 Requirements



To: To whom it may concern **Issue:** 1 (Feb 2015)

From: Dr. William Goble, CFSE, Principle Partner, exida

Subject: Clarification that a single Rosemount 5900 2-in-1 can serve as level sensors in two independent protection layers (i.e. BPCS and SIS)

exida has collaborated with Emerson to assess the Rosemount 5900 Radar Level Gauge for compliance with IEC 61508:2010 and the result has been documented in certificates ROS 1312032 C001/2/3. These are publicly posted on the Safety Automation Equipment List (www.sael-online.com).

As with all assessments, exida has developed a thorough technical understanding of the product. As a result of this, we can testify that a single Rosemount 5900 with option "SIL 2 2-in-1" (ROS 1312032 C003) connected as figure 1 can simultaneously serve as both the level sensor in a BPCS and as the level sensor in a SIL 2 safety instrumented function (SIF) designed per IEC 61511.

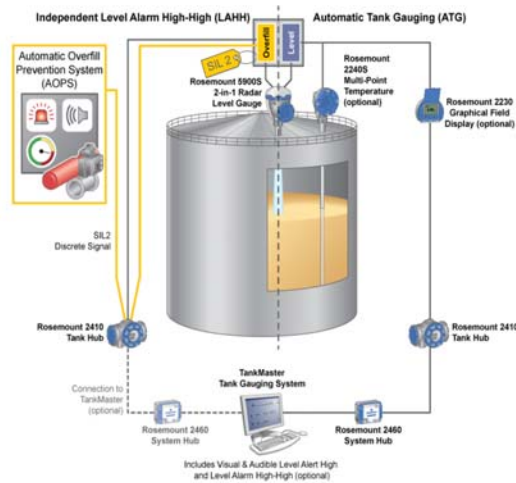


Figure 1: Rosemount 5900 2-in-1 SIL 2 Radar Level Gauge in a configuration suitable to serve as the level sensors in two independent protection layers (i.e. BPCS and SIS)



Public Letter
Page 2 of 2

In practice, this means that according to IEC 61511 a single Rosemount 5900 with option "SIL 2 2-in-1" can be used as the level sensor in both the 'Tank Gauging System' and an independent emergency shutdown system for e.g. overfill prevention (category #3 per API 2350 Edition 4 classification).

William Goble
CFSE, Ph. D, President
Exida
carl-johan.roos@emerson.com
+46-733-336700



exida is ANSI accredited to Guide 65, the general requirements for bodies operating product certification systems.



Dr. Goble has over 30 years of professional experience. He is widely recognized as an expert in programmable electronic systems analysis, safety and high availability automation systems, automation systems new product development and market analysis. He developed many of the techniques used for probabilistic evaluation of safety and high availability automation systems. He was formerly Director, Critical Systems at a successful North American safety company. His principle work responsibilities included strategic planning, market analysis, promotion and business management. Dr. Goble previously held positions in research and development including computer design, software design and development and engineering project management. Dr. Goble also teaches reliability engineering at the University of Pennsylvania. He has written two

widely used books on topics of safety and reliability modeling including "Control Systems Safety Evaluation and Reliability." He teaches many of the exida.com courses and ES35, an ISA professional course on safety and reliability. He is a fellow member of ISA. He has published many papers and magazine articles. Dr. Goble has a BSEE from Penn State, a MSEE from Villanova and a PhD from Eindhoven University of Technology in Eindhoven, Netherlands.

Preliminary Rev 02

Global Headquarters and Europe Regional Office Tank Gauging

Emerson Process Management

Box 150

(Visiting address: Layoutvägen 1)

SE-435 23 Mölnlycke

+46 31 337 00 00

+46 31 25 30 22

sales.rtg@emerson.com

North America Regional Office Tank Gauging

Emerson Process Management

6005 Rogerdale Road

Mail Stop NC 136

Houston, TX 77072, USA

+1 281 988 4000 or +1 800 722 2865

sales.rtg.hou@emerson.com

Latin America Regional Office

Emerson Process Management

1300 Concord Terrace, Suite 400

Sunrise, FL 33323, USA

+1 954 846 5030

+1 954 846 5121

RFQ.RMD-RCC@EmersonProcess.com

Asia Pacific Regional Office

Emerson Process Management Asia Pacific Pte Ltd

1 Pandan Crescent

Singapore 128461

+65 6777 8211

+65 6777 0947

Enquiries@AP.EmersonProcess.com

Middle East and Africa Regional Office Tank Gauging

Emerson Process Management

P.O. Box 20048

Manama

Bahrain

+973 1722 6610

+973 1722 7771

rtgmea.sales@emerson.com



[Linkedin.com/company/Emerson-Process-Management](https://www.linkedin.com/company/Emerson-Process-Management)



[Twitter.com/Rosemount_News](https://twitter.com/Rosemount_News)



[Facebook.com/Rosemount](https://www.facebook.com/Rosemount)



[Youtube.com/user/RosemountMeasurement](https://www.youtube.com/user/RosemountMeasurement)



[Google.com/+RosemountMeasurement](https://plus.google.com/+RosemountMeasurement)

Standard Terms and Conditions of Sale can be found at:
www.Emerson.com/en-us/pages/Terms-of-Use.aspx
The Emerson logo is a trademark and service mark of Emerson Electric Co.
Rosemount and Rosemount logotype are trademarks of Rosemount Inc.
All other marks are the property of their respective owners.
© 2015 Emerson Process Management. All rights reserved.