Design and Specification of Radar Based Early Warning Systems

Trevor Harvey, formerly Segment Engineering Technical Authority (BP Upstream),
Paul Oram, Chief Engineer, Inst'n Control & Electrical (BP Upstream),
Jonathan Love, Visiting Professor, Imperial College (Independent).

Offshore facilities are vulnerable to collision with errant vessels. A primary means of protection against such collisions is the use of radar based early warning systems (REWS). Presently there is no international standard covering the design of REWS for collision avoidance. To address this gap, BP is developing its own internal engineering technical practice (ETP) GP-59-83. Key to a REWS' fitness for purpose is its reliability or, strictly speaking, its availability. Much of the thinking behind GP-59-83 is inspired by the concepts of IEC 61508. This paper explains the basis of the approach adopted. Two scenarios are considered, one leading to an alert and the other to an emergency shutdown (ESD). The work is on-going.

1 Introduction

Around the world there are many offshore oil and gas facilities such as drilling rigs, production platforms, floating production storage and off-loading (FPSO) vessels, etc. All operators have a responsibility to ensure that the risk of a major incident involving any of those facilities is assessed and managed. Typical risks include:

- process safety
- offshore structural integrity failure
- subsea pipeline integrity failure
- loss of primary containment (LOPC)
- attendant vessel collision
- errant vessel collision
- helicopter incident

The focus of this paper is on errant vessel collisions. There have been various such collisions over the years, throughout the industry, and many more near misses. Therefore, almost every offshore facility has a radar based early warning system (REWS) whose function is to prevent it from being struck by an errant vessel, especially by a large and heavily laden vessel.

In essence, the REWS is used to detect a vessel as it appears over some horizon and, if on collision course or thereabouts, to monitor its direction and speed. The intelligence in the tracking software raises alerts when a realistic risk of collision is determined. Contact with the errant vessel is then attempted by radio or otherwise and a change of course encouraged.

It should be appreciated that REWS is not the only barrier against errant vessel collision. For example:

- carriage of an automatic identification system (AIS) is mandatory for any vessel >500 tonnes: apart from broadcasting identity, position, speed, etc, this also marks any offshore structure on a vessel's navigational displays over a range of 40km.
- most structures are supported by an emergency response and rescue vessel (ERRV) which maintains an anti-collision watch and is equipped with both REWS and AIS.

The use of REWS is not restricted to errant vessel collisions: it can, for example, mitigate against subsea pipeline failures due to errant fishing (trawler) vessels. And the consequences are certainly not restricted: an errant vessel collision can lead to loss of structural integrity, LOPC, etc.

Whilst there is no suggestion that any of the existing REWS are not fit for purpose, there is much variety in design with:

- different types of equipment and technology,
- multiple suppliers,
- alternative hardware configurations,
- various software and display systems,
- different levels of operator involvement, and so on.

There is no international standard on the requirements for the design of REWS used for collision avoidance. Various standards exist which address specific aspects of REWS, such as protocols for ship identification and for ship-to-ship or ship-to-shore communication, but there's nothing about the design of REWS as a complete system. Accordingly, BP has decided to develop an internal engineering technical practice (ETP) GP 59-83 on the design and specification of REWS: this paper outlines some of the underlying work done thus far.

2 Adaptation of IEC Standards to REWS

Much of the thinking behind the development of GP 59-83 to date has been informed (and inspired) by the concepts of the IEC standards 61508 and 61511. Whilst most of the content of both standards concerns the life cycle of protection systems, and their management in particular, the essential functionality is captured by two simple equations:

$$HR = DR \times PFD \quad (1)$$

$$Risk = HR \times VF \times C(E) \quad (2)$$

In the context of collision avoidance, the terms can be defined as follows:

DR the unmitigated demand rate (collisions/year). That is the frequency at which vessels are found to be on collision course with a facility. Unmitigated means the value of DR as if the REWS does not exist.

DR = fn (shipping traffic density)

PFD the probability of failure on demand of a REWS collision avoidance system. Each REWS is bespoke and its PFD has to be evaluated on an **end-to-end** basis which includes any action taken by the operator. PFD is always based upon dangerous mode failures only. Within IEC 61508 and 61511, PFD is articulated in terms of safety integrity level (SIL) bands.

HR the mitigated hazard rate (collisions/year): that is the DR having been reduced by a factor due to interventions made by means of REWS.

C(E) the consequence of a collision (deaths/collision) if it were to happen. Strictly speaking this is deaths or serious injuries, the difference being a matter of chance.

C(E) = fn (momentum of vessel and manning level of facility).

Note that in determining C(E) no particular account has been taken as to whether the facility is of a gas and/or oil processing nature.

VF the vulnerability factor which, in the context of an offshore facility, is a measure of the operators' ability to escape prior to collision, assuming life rafts available, crew trained, etc.

VF = fn (time available before collision happens).

Risk the tolerable risk which is based upon the principle of as low as reasonably practicable (ALARP). The regulatory bodies have coalesced around an acceptable range for tolerable risk of 10^{-4} to 10^{-6} deaths/year although an upper limit of 10^{-3} may be considered if there is no risk to the public.

Consequence

Assuming a vessel is on collision course with a facility, the consequence C(E) of a collision is a function of the momentum of the vessel and the manning level (occupancy) of the facility. A collision factor (CF) is introduced by definition:

$$C(E) = CF \times Manning \quad (3)$$

Collision factors are banded according to momentum as shown in Table 1 below. Note that the CF thresholds are subject to further calibration against experience.

Momentum (kN s)	$<10^3$	10^3-10^4	10^4-10^5	$>10^5$
Collision factor (CF)	0.0005	0.005	0.05	0.5

Table 1

Vulnerability

The concept of vulnerability was introduced in IEC 61511 to allow for the fact that, in some cases, the operators may be able to avoid the consequences of a hazardous event by, for example, running away from it. In the context of an offshore facility, the avoidance option is to take to the life rafts. It should be appreciated that abandonment is hazardous in itself and not free of risk even in non-emergency circumstances.

The proposed vulnerability factors are given in Table 2. Again, note that the VF thresholds are subject to further calibration against experience.

Shut down mode		PSD	ESD	
Alarm category	Alert	Warning	Abandon	
Distance to collision (km)	<40			
Time to collision (mins)	>30	15-30	5-15	0-5
Vulnerability factor (VF)	0.003	0.01	0.03	0.1

Table 2

Availability Integrity Level

As stated, PFD is normally articulated in SIL bands. However, for REWS purposes, it is proposed that availability integrity level (AIL) bands be introduced. That is in recognition of the IEC 61508 and 61511 standards not applying offshore and most of the equipment used for REWS not being SIL rated.

There is a 1:1 mapping between AIL and SIL bands, assuming demand mode operation (DR < 1.0 collisions/yr) as shown in Table 3 below.

Availability	0.0-0.9	0.9-0.99	0.99-0.999	0.999-0.9999	0.9999-0.99999
AIL level	0	1	2	3	4

Table 3

3 Alert Scenario: Availability Requirement

The following scenario is considered:

- a 50,000 te vessel travelling at 20 km/hr is detected to be 25 km away and on collision course with a platform.
- the platform has 20 personnel aboard.

Tolerable risk is presumed to be within the ALARP range:

$$\text{Risk} = 0.8 \times 10^{-4} \text{ deaths/yr}$$

Consequence of a collision is established from momentum and occupancy:

$$\text{Momentum} = 50{,}000 \text{ te} \times 20 \text{ km/hr}$$

$$\approx 5 \times 10^{7} \text{ kg} \times 5.6 \text{ m/s} = 2.8 \times 10^{8} \text{ N s} = 2.8 \times 10^{5} \text{ kN s.}$$

So, according to Table 1:

$$\text{Collision factor} = 0.5$$

Thus, from Equation 3:

$$C(E) = CF \times \text{Manning} = 0.5 \times 20 = 10 \text{ death/collision.}$$

Note that the manning level excludes the crew of the errant vessel.

Vulnerability is determined by the estimated time to collision (ETC):

$$\text{ETC} = 25 \text{ km} / 20 \text{ km hr}^{-1} \equiv 75 \text{ mins}$$

So, according to Table 2:

$$VF = 0.003$$

Hazard rate is thus given by Equation 2:

$$\text{Risk} = HR \times VF \times C(E)$$

$$0.8 \times 10^{-4} = HR \times 0.003 \times 10$$

$$HR \approx 2.7 \times 10^{-3} \text{ collisions/yr.}$$

The probability of a vessel being on or very near to collision course is obviously a function of the traffic density and shipping routes.

Data gathered for the UK continental shelf for 1990-2005 revealed that there were 40 collisions (accidents, incidents or near misses) involving passing (as opposed to attendant) vessels. However, that data is for the whole of the continental shelf on which there were situated approx. 50 facilities. Hence, per facility:

DR = 40 / 16 / 50 = 0.05 collisions/yr

The PFD of the protection system is given by Equation 1:

HR = DR x PFD

$2.7 \times 10^{-3} = 0.05 \times PFD$

PFD = 0.054

Thus, to satisfy the requirements, the protection system has to have a PFD of 0.054, corresponding to an availability of 0.946 which, according to Table 3, places it in the middle of the AIL 1 band. The issue, therefore, is whether the design and technology of the REWS system is at least of AIL 1 quality.

4. Decomposition of REWS

There are eight sub systems involved, end-to-end, in a REWS based collision avoidance system as depicted in Figure 1,

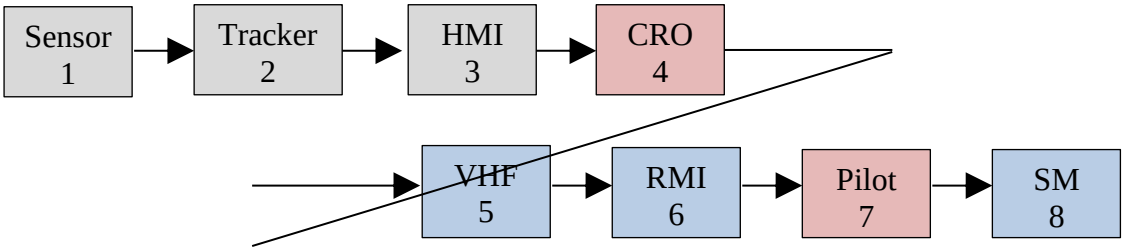

Figure 1

The sub systems, referred to by Box no, are as follows:

1 Sensor: this sub-system comprises the radar sensor, transmitter and receiver.

2 Tracker: the hardware and software of the REWS tracking system.

3 HMI: the operator interface of the REWS in the control room of the facility.

4 CRO: the control room operator.

5 VHF: the means of communication between the CRO and the pilot.

6 RMI: the radio machine interface on the bridge of the vessel on collision course.

7 Pilot: the person steering the vessel.

8 SM: the steerage mechanism, which may be of an electro-mechanical or electro-hydraulic nature.

Some of these sub-systems, especially the tracker, are complex whereas others such as the RMI may be relatively simple. Some may be highly reliable with known failure modes, others less so. To all intents and purposes, these subsystems are in series although each may in itself have some parallelism. Thus, analogous to a convoy, the speed of which is determined by that of the slowest ship, the overall availability is dominated by that of the least reliable sub-systems.

It is worth noting at this stage that the VHF, RMI, Pilot and SM are either partially or wholly beyond the offshore facility operator's control.

5. Alert Scenario: Availability Realised

As stated, there are many designs of REWS. The configuration depicted in Figure 2 below is relatively simple but not untypical.

Box 1 has two input channels in parallel, each consisting of a radar sensor, transmitter and receiver. The elements of each channel are in series and their combined failure rate is the sum of the individual failure rates articulated in failures/year (fpy) which are for dangerous mode only. Suppose, for a single input channel:

$$\lambda_{i/p} = \sum \lambda_j = 0.02 \text{ fpy}$$

If each radar channel had 360° coverage, or thereabouts, they could be counted as truly redundant channels in parallel with (maybe very) high availability. However, a more likely scenario is that they will have reduced coverage, say some 180-270° each. Thus to provide 100% coverage it is essential that both channels are working simultaneously.

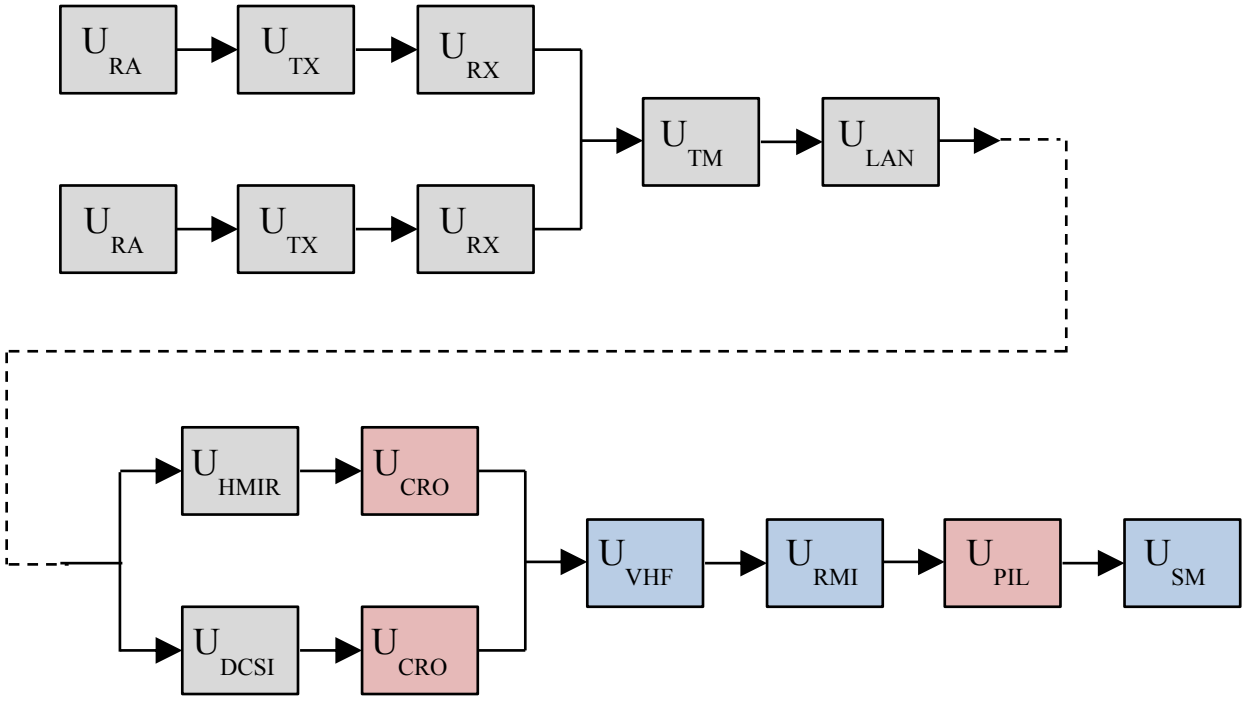

Figure 2

The two radar channels, although physically in parallel, are functionally in series. Thus:

$$\lambda_{Box1} = 2\sum\lambda_{i/p} = 0.04 \text{ fpy}$$

From this the unavailability of the input channels may be calculated:

$$U_{Box1} \simeq PTRT \times \lambda_{Box1}$$

where PTRT is the proof test and repair time for the devices in the channel:

PTRT = PTI/2 + MTTR

Presume that the REWS is in regular but intermittent use such that it is exercised, say, once every 8 hours. Because of various independent means of verification of REWS, such as line-of-sight and visual verification, this period can be taken as being equivalent to the proof test interval PTI. Assume the mean time to repair (MTTR) of any identified fault is 2 days. Thus

PTRT = 8/2 + 48 hr ≈ 0.006 yr

Hence $U_{Box1} = 0.006 \times 0.04 = 2.4 \times 10^{-4}$

Box 2 is the track manager and the local area network (LAN) for communicating with the HMI. The elements are in series. Suppose:

$$\lambda_{Box2} = \sum\lambda_j = 0.01 \text{ fpy}$$

Again, assuming a PTRT of 0.006 yr gives:

$$U_{Box2} = 0.006 \times 0.01 = 6 \times 10^{-5}$$

Boxes 3-4. There are two human machine interfaces (HMI) for REWS. One (HMIR) is a dedicated REWS display system. The other (DCSI) is a shared display supported by the distributed control system (DCS). The no of personnel in the control room is such that each HMI can be presumed to have an independent operator (CRO).

Suppose that the failure rate of both HMIR and of the DCSI is 0.01 fpy. Again, assuming PTRT = 0.006 yr:

$$U_{HMIR} = U_{DCSI} = PTRT \times \lambda_j = 0.006 \times 0.01 = 6 \times 10^{-5}$$

Assume the operators are fully trained and experienced. At best, there is a 95% chance of each operator being available, recognising an alert and responding to it appropriately.

$$U_{CRO} = 0.05$$

Since the operators are in series with the HMIs and the HMIs are in parallel:

$$U_{Box34} = \left(\sum U_j\right)^2 = (6 \times 10^{-5} + 0.05)^2 \simeq 2.5 \times 10^{-3}$$

Boxes 5-8 represent the output channel of the REWS consisting of the VHF system, the ship's radio-machine interface (RMI), its pilot and steerage mechanism (SM). The technology involved is uncertain, potentially ranging from a simple hand-held VHF receiver to an integrated navigation display system and cannot be presumed to be dual redundant.

As a first guess, assume the combined unavailability of the various hardware elements to be substantially worse than for the input channel, say:

$$\lambda_{h/w} = \sum \lambda_j = 0.2 \text{ fpy}$$

Whence: $U_{h/w} \simeq PTRT \times \lambda_{h/w} = 0.006 \times 0.2 = 0.0012$

Ultimately, the REWS is also reliant upon the pilot to take evasive action upon receiving a message from the CRO. Make similar assumptions about the training and experience of the Pilot as for the CRO. However, it has to be assumed that there may well only be one pilot on the bridge of the vessel:

$$U_{Pilot} = 0.05$$

The hardware and pilot of the output channel are in series, so its unavailability is found by summation:

$$U_{Box58} = \sum U_j = 0.0512$$

End to end. The subsystems of the REWS being in series, its overall unavailability is found by summation: Thus, on an end-to-end basis:

$$U_{REWS} = \sum U_j = U_{Box1} + U_{Box2} + U_{Box34} + U_{Box58}$$
$$= 2.4 \times 10^{-4} + 6 \times 10^{-5} + 2.5 \times 10^{-3} + 0.0512 = 0.054$$
$$A_{REWS} = 1 - U_{REWS} = 0.946$$

The overall availability is also in the middle of the AIL 1 band of Table 3 and, amazingly, is exactly the same as the 0.968 target for the alert.

Note that this is dominated by the unavailability of the pilot. Indeed, with a single pilot in the forward path for whom A = 0.95 at best, the AIL 2 design criteria of 0.99 < A < 0.999 can never be satisfied.

6 Shutdown Scenario: Availability Requirement

The scenario is changed such that the same vessel, with the same momentum is still on collision course for the same platform, but it is now only 4 km away from the facility.

The probabilistic analysis is reworked, although the question as to how the vessel managed to get to within 4 km without avoidance action having already been taken is pertinent. If, for example, the pilot has gone to sleep, in which case $A_{Pilot} \approx 0$, a collision is guaranteed.

Risk and consequence are the same as before:

Risk = 0.8 x 10^{-4} deaths/yr.

C(E) = 10 deaths/collision.

But, because the vessel is much closer, vulnerability is much higher.

ETC = 4 km / 20 km hr^{-1} ≡ 12 min

VF = 0.03

The hazard rate is again given by Equation 2:

Risk = HR x VF x C(E)

0.8 x 10^{-4} = HR x 0.03 x 10

HR ≈ 2.7 x 10^{-4} collisions/yr.

The demand rate is essentially the same.

DR = 0.05 collisions/yr.

The PFD of the protection system is again given by Equation 1:

HR = DR x PFD

$2.7 \times 10^{-4} = 0.05 \times PFD$

$PFD = 5.4 \times 10^{-3}$.

Thus, to satisfy the requirements, the protection system has to have a PFD of 0.0054. That corresponds to an availability of 0.9946 which, according to Table 3, places it in the middle of the AIL 2 band. This is a much more stringent criterion.

7 Shutdown Scenario: Availability Realised

The REWS configuration now to be considered is as depicted in Figure 3. The essential difference is that, whilst still attempting to contact the errant vessel, the modus operandi has changed to shutdown mode. Subject to whatever local/higher authority is required, the control room operators (CRO) trigger the emergency shutdown (ESD) system. In effect, the REWS is an input to the ESD, albeit through the CRO. Thus the entire system, end to end, is now wholly under the offshore facility operator's control.

The unavailability for Boxes 1-4 are exactly the same as for the alert scenario, that is:

$$U_{Box1} = 2.4 \times 10^{-4} \qquad U_{Box2} = 6 \times 10^{-5} \qquad U_{Box34} \simeq 2.5 \times 10^{-3}$$

Presume that the ESD is a high integrity logic solver with a discrete input channel from the DCS. It can be assumed that the channel and solver will have very low failure rates so a combined failure rate of 0.001 fpy or less is realistic. Assume quarterly proof testing of the ESD so its PTRT is approx. 0.25 yr. Thus:

$$U_{ESD} \simeq PTRT \times \lambda_{ESD} = 0.25 \times 0.001 = 2.5 \times 10^{-4}$$

The action of an ESD is obviously context dependant but presume that, not untypically, it has three primary output channels:

- one de-energises a fail-open solenoid which in turn causes the well/main riser shutdown valve to close,
- one de-energises another fail-open solenoid valve which depressurises the fail-open gas inventory vent valve, and
- the other de-energises a fail-open relay which in turn de-powers a fail-off mains supply isolator common to various items of electrical plant/equipment.

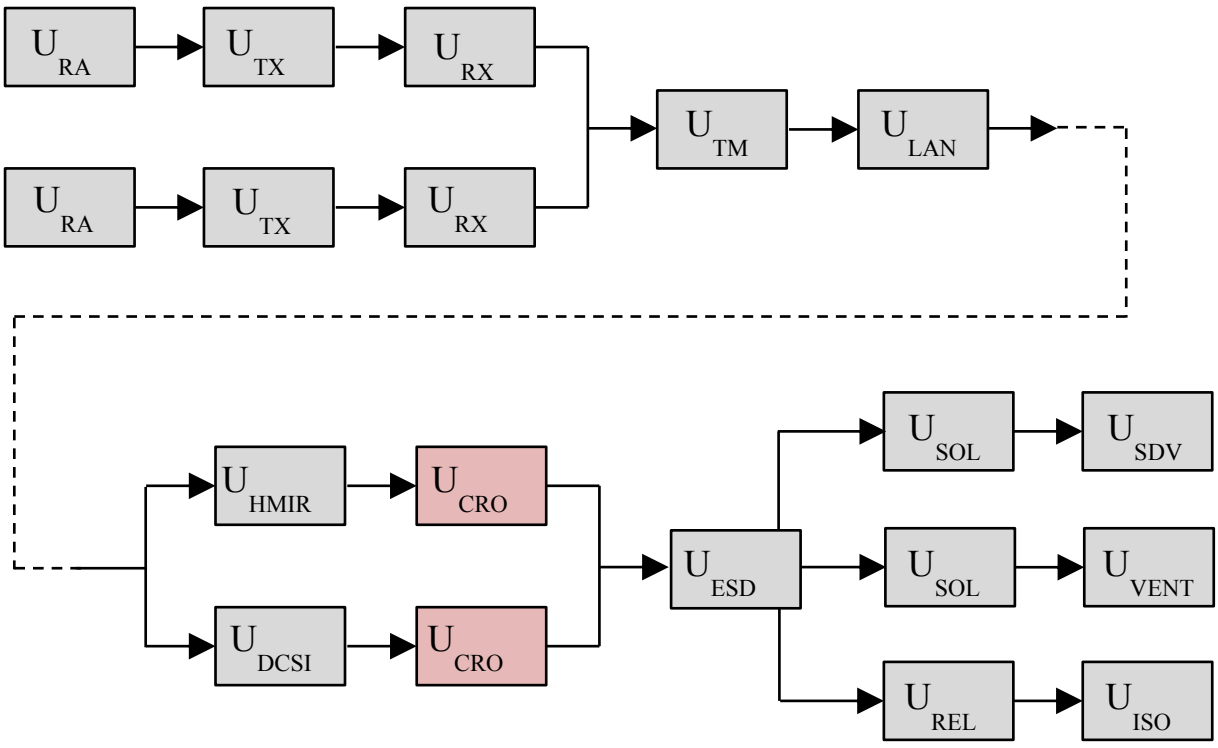

Figure 3

It is recognised that additional redundancy would be required to achieve the necessary reliability of the output channels. Redundancy of the riser shutdown valves, for example, has been omitted in the interest of brevity for this paper.

For the ESD to function correctly, the riser shutdown valve must close and both the gas vent valve and the supply isolator must open. Thus, whilst these channels are physically in parallel as depicted in Figure 3, functionally they are in series.

$$U_{OUTS} = \sum U_j = U_{SOL} + U_{SDV} + U_{SOL} + U_{VENT} + U_{REL} + U_{ISOL}$$

Assume the sum of the dangerous mode failure rates for the solenoids, relay, isolator shutdown and vent valves is 0.004 fpy and presume the same proof testing regime as for the ESD itself. Thus:

$$U_{OUTS} = PTRT \times \sum \lambda_j = 0.25 \times 0.004 = 0.001$$

Thus, on an end-to-end basis:

$$\begin{aligned} U_{REWS} &= \sum U_j = U_{Box1} + U_{Box2} + U_{Box34} + U_{ESD} + U_{OUTS} \\ &= 2.4 \times 10^{-4} + 6 \times 10^{-5} + 0.0025 + 2.5 \times 10^{-4} + 0.001 \\ &= 0.00405 \\ A_{REWS} &= 1 - U_{REWS} \approx 0.9969 \end{aligned}$$

The overall availability is within the AIL 2 band and not far short of the 0.9946 target. Given the various presumptions and approximations made and the values assumed that is probably close enough.

Comment

This paper has explained some of the work done to date in developing BP ETP GP-59-63 for the design and specification of REWS. The standard is not prescriptive as to the technology deployed or configuration used: there is plenty of scope for sensible interpretation of requirements and engineering judgement of the proposed solution.

The paper has provided insight into some of the challenges in applying the concepts of IEC 61508 and 61511 to the design of REWS on an end-to-end basis. In particular it has provided a credible basis for taking into account the momentum of an errant vessel as well as the distance/time to collision and the consequences of such. Two worked examples have been provided.

The work is on-going. A suite of model calculations to determine overall availability for different system configurations is being developed for reference purposes. Relevant incident frequency and failure rate data continues to be gathered. The collision and vulnerability scaling factors are subject to calibration against experience.

Caution

The values assumed throughout this paper for failure rates (fpy) are for dangerous mode failures and are indicative only for illustrative purposes: they should not be presumed to be appropriate for any particular application.

Reference

Love J, Process Automation Handbook, Chapters 53 & 56, Springer, 2007.