Containment Architecture and Failure Response in Pumps for Hazardous-Liquid Service

A liquid-agnostic examination of what happens when primary containment is breached — and how dual-seal, magnetic drive, and canned-motor pumps respond.
Published by Klaus Union GmbH & Co. KG, Bochum Germany. The hybrid double containment shell described in Section 4.4 is a Klaus Union design.

Executive summary

When a pump moves a toxic, flammable, or environmentally damaging liquid, the engineering question is rarely whether the containment boundary can be breached — given the right initiator, every boundary can fail.

The more useful questions that must be answered are:

- How quickly is a breach detected?
- How much time and margin remain before the surroundings are affected?
- How much hazardous material escapes in the meantime?

A consequence of these three questions is a final, fourth question with direct impact on process design and steps to be taken when the primary containment boundary fails:

- Can the current process be reasonably completed, or must the pump be immediately tripped and decontaminated?

This paper sets out one liquid-agnostic framework — a layered defense in depth — and applies it to the three architectures common in hazardous service. Throughout, it separates measures that merely **limit and direct** leakage (**in API terminology: secondary control**) from those that **fully retain** it (**in API terminology: secondary containment**), because that distinction determines the emission outcome after a breach.

The analysis goes from the simplest to the most robust solution: a sealless pump with a double containment system. The solution can be continuously monitored via a simple instrument, which allows continued operation to a controlled shutdown with zero atmospheric leakage, achieved without external utilities and while remaining site-serviceable for those applications where leakage is not an option.

1 Pump safety is a containment-architecture question

Hazardous-liquid duties fall into three consequence classes, each with a different acceptance threshold: **toxic exposure** (acute harm to people), **flammable or explosive release** (fire and overpressure), and **environmental and fugitive emission** (regulated losses to air, soil or water). A single leak can belong to more than one class at once.

One special case requires separate treatment because it breaks a common assumption. A fluid handled **above its autoignition temperature** (common with heat transfer applications) ignites on contact with air **without any external ignition source**. Ignition-source control as per ATEX (Directive 2014/34/EU) — area zoning, equipment categories, surface-temperature classes, etc. — remains necessary, but is **not sufficient** here, because the leak supplies its own ignition. The only robust control is to prevent the leak. For these applications ignition-source management and containment are in essence one and the same, making a strong case for a true zero-leakage architecture.

The organizing idea is **defense in depth** (equivalently, layers of protection): prevention, primary containment, detection, secondary control or containment, and controlled shutdown. Each intact layer reduces the chance that a single boundary breach reaches the surroundings (Figure 1).

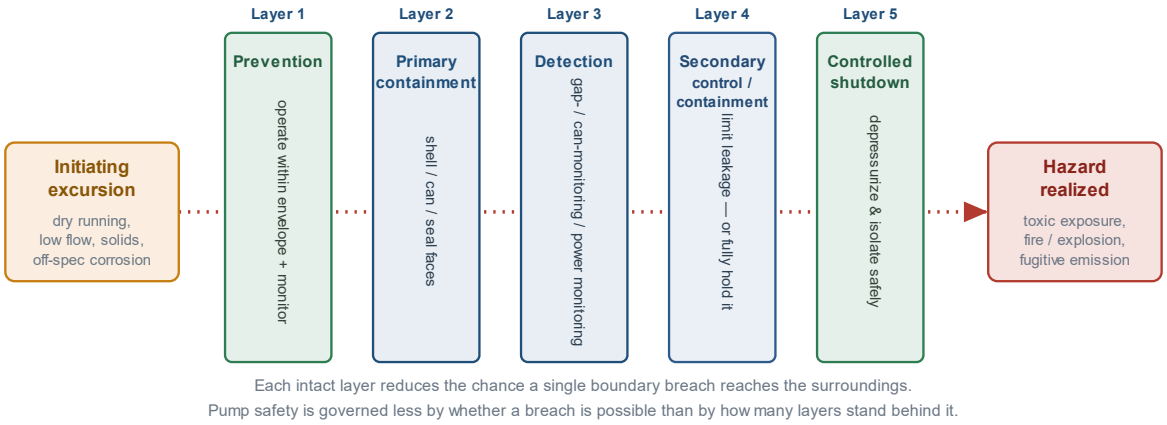

Figure 1. A layered defense in depth. Each vertical bar is a protective layer standing between an initiating excursion and a realized hazard.

2 A common failure taxonomy

Rigorous analysis keeps four things apart that are easy to conflate:

- **Initiator (root cause)** — the operating excursion or condition that starts the event.
- **Breach mode** — which boundary element physically fails.
- **Leakage path** — where the hazardous fluid then goes.
- **Mitigation layer** — what catches it.

Applied to the three architectures, the same skeleton produces Table 1.

Aspect	Dual mechanical seal	Magnetic drive (sealless)	Canned motor (sealless)
Primary boundary	Two dynamic sealing faces + barrier / buffer fluid	Stationary containment shell (casing + shell)	Stationary stator liner / can
Characteristic failure type	Wear-out of faces (finite design life by nature)	Conditional failure from an operating excursion	Conditional failure from an operating excursion
A breach releases into	Barrier fluid, then atmosphere	Into the lantern area, then atmosphere	Stator cavity, then atmosphere
Standard backup	Tertiary seal (control) or pressurized tertiary (containment)	Secondary control (single gas seal) or secondary containment (double isolation shell)	Inherent secondary boundary — only if qualified for the fluid, process pressure and process temperature (incl. upset conditions) – including electrical insulations
Governing standard	API 610 + API 682	API 685	API 685

Table 1. The same failure skeleton across the three architectures.

2.1 Root causes of the characteristic failure types

Wear-out versus conditional failure. A mechanical seal seals by relative motion across contacting (or near-contacting) faces; material is consumed as an inherent consequence of doing its job. It therefore has a **wear-out life** — API 682 sets a design objective of three years (25,000 hours) of reliable operation. This means that the lifetime of a seal is limited **even under perfect (i.e. specification compliant) operation**.

The pressure-retaining containment shell of a sealless pump has **no such wear-out mode**.

Corrosion is a materials / fluid-compatibility outcome and can be designed against by using high nickel alloys and / or ceramics as the isolation shell (magnetic drive pump) respectively can (canned motor pump) material.

Erosion is a materials / specification outcome and can be designed against with inline filtration systems and proper selection of liquid gaps as well as by choosing wear-resistant shell materials.

The internal components most vulnerable to off-design operation are the product-lubricated journal bearings. They too do not wear, when properly selected for the operating conditions, but will generally be the first parts that show wear if the pump is not operated as per design.

This gives sealless pumps one clear advantage – provided they are operated within specification, no single component imposes a fixed wear-out life. Conversely that means the user can monitor against excursions from planned operating conditions.

3 Mechanical (dual) seals: the baseline

Considering that most people are far more familiar with mechanically sealed pumps than with sealless designs, it seems prudent to establish these solutions as the baseline.

API 682 classifies seals by **Arrangement**: 1 (single), 2 (dual with an unpressurized buffer fluid, e.g. Plan 52), and 3 (dual with a pressurized barrier fluid, e.g. the Plan 53A/B/C and Plan 54 family). For toxic or zero-tolerance liquids, Arrangement 3 (or a dry-gas variant) is the standard: a clean barrier fluid held **above** process pressure means any face leakage flows inward, and nothing escapes to atmosphere while the system is intact. Three failure modes follow, in increasing severity (Figure 2).

- **Failure Mode 1 — barrier pressurization is lost.** The arrangement silently degrades to an unpressurized dual seal (Plan 52 behavior). Process now migrates into the barrier fluid and — the easily missed part — the zero-emission guarantee that justified the pressurized design has quietly disappeared. A reservoir built for a pressurized Plan 53 may lack the vent / relief or flare connection a Plan 52 needs. (For a Plan 53C, where barrier pressure is referenced to seal-chamber pressure through a piston accumulator, “loss of pressure” is not even a single clean event; degradation is more gradual.)
- **Failure Mode 2 — the outer (atmospheric-side) seal fails.** This leads to a quick loss of the barrier fluid through the now leaking atmospheric side seal. The inner seal, which was selected for the process, continues as a single seal. Some process leaks to atmosphere, but across a face designed for the duty. Zero-emission status is lost, as is the protection of the process side seal by the much more benign barrier fluid, leading to a much quicker degradation of the process-side seal performance than otherwise to be expected.
- **Failure Mode 3 — the inner (process-side) seal fails.** Process floods the barrier chamber and the surviving outer seal becomes the last boundary. But that outer seal was specified for a **benign barrier fluid, not for the process** — its faces, materials and balance may all be wrong for what it is now holding. This makes this mode the most dangerous of the three, even though, like Failure Mode 2, it leaves a single seal in service.

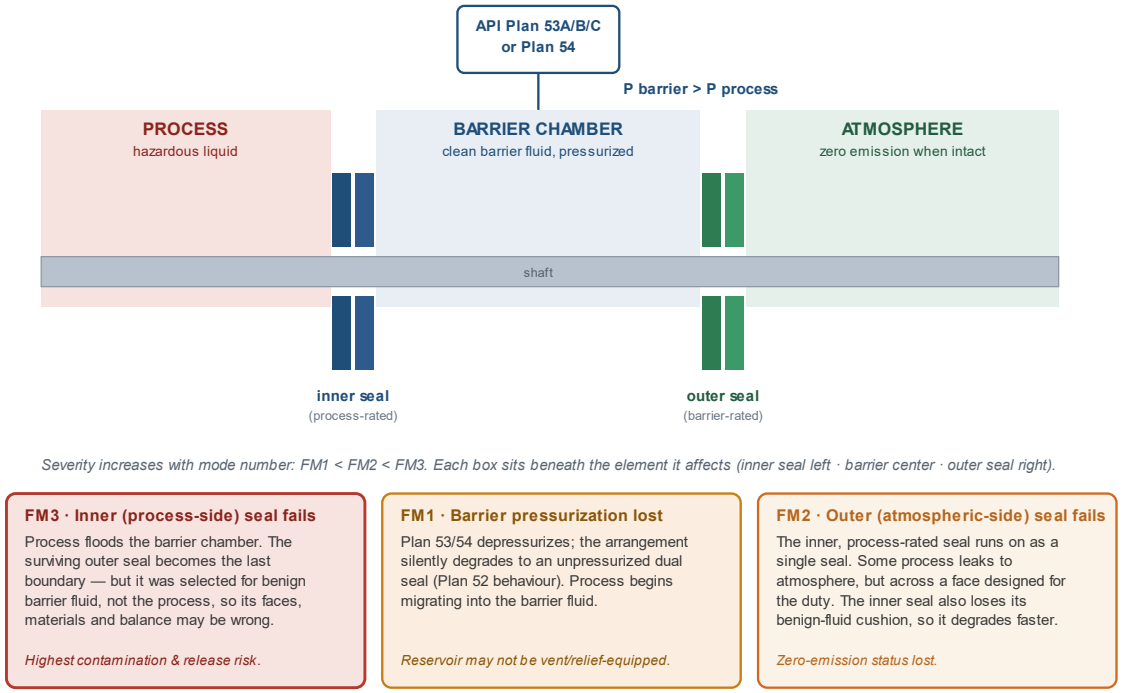

Figure 2. Pressurized dual seal (API Arrangement 3) and its three failure modes

Backups extend the baseline. A **dry-running tertiary seal** with a leakage-collection plan is a **secondary-control** measure: it limits and directs leakage but does not eliminate it. A **pressurized tertiary seal** can eliminate leakage, at the cost of a second barrier system. The challenge remains that **every backup in a sealed pump is itself another dynamic sealing element**, with its own wear-out life and its own support requirements.

4 Sealless pumps: protecting the boundary, not the seal

Both sealless types remove the dynamic shaft seal entirely. In a **magnetic drive pump**, torque crosses a stationary, pressure-retaining **containment shell** that separates the wetted inner magnet assembly from the dry outer magnets; the process fills the rotor chamber and lubricates the internal bearings. In a **canned-motor pump**, the rotor runs in the process inside a thin stator liner (the can), which forms the primary boundary, with the motor stator outside it. Neither has a dynamic element on the containment boundary — which is why, per Section 2, that boundary has no wear-out life.

4.1 What a breach looks like, and what causes it

The dominant real-world initiators are **operational, not material**:

A breach can be caused by direct damage to the containment shell / can or as a secondary effect most typically because of an unrecognized failure of the journal bearings.

4.1.1 Direct damage to containment shell / can

Causes for direct damage to the containment shell / can are typically:

1. unanticipated solids
2. vaporization in the shell / can area
3. dry running
4. Pressurization of the pump above design pressure.

Note that points 2 and 3 are only applicable to canned motor pumps or magnetic coupled pumps with metallic containment shells, though for the latter the bearings have to be taken separately into consideration.

4.1.2 Damage to journal bearings

A failure of the journal bearings is the more typical cause. The bearing can fail if the pump is operated outside its permissible envelope (low or high flow conditions), with off-spec viscosity, dry run or unanticipated solids.

As all of these conditions are process conditions, the pumps can be largely designed to meet these challenges, if they are known at design stage, or – if not – the operator can generally monitor against them. A journal bearing failure can be easily detected by utilizing power monitoring – still something all too often not implemented in the field.

A primary breach then admits process into the next region —the lantern in a magnetic drive pump, or the stator cavity in a canned-motor pump.

4.2 Secondary control versus secondary containment

Secondary control and secondary containment are often mixed up – but the strategies they implement and their implications for both operational procedures and safety of the equipment are so fundamental that we have to clearly distinguish what we are talking about, when we use either term.

4.2.1 Degrees of safety in control / containment design

Looking at the “Hazard based specification of Control / Containment Guidelines” as per API 685, 3rd Edition, Annex P it appears to classify the following priority of safety, from least to most safe:

1. None – no additional measures taken
2. Secondary Control – a secondary control device is introduced, creating a secondary pressure casing out of the lantern with a dynamic sealing element, but monitoring of the same is not made mandatory
3. Secondary Control System – same as above, but with the secondary pressure casing monitored, to immediately detect a primary containment failure
4. Secondary Containment System – a means to positively contain any leakage into the secondary pressure casing, not allowing any process leakage to the outside, and providing a suitable online monitoring system to verify the integrity of the containment system (both process and standby) to allow the operators to take appropriate action if necessary.

4.2.2 Typical designs and considerations for the safety design

- **Secondary control** limits and safely directs leakage after a breach but is **not** designed to hold the full process indefinitely. Throat and throttle bushings, a backup lip seal, and a single-acting backup mechanical seal all fulfill this requirement nominally, but of course with different leakage rates to atmosphere and different standby as well as operational lives.

  According to API 685 3rd Edition the secondary control device shall by itself still meet local emission guidelines or have a maximum screening value of 1000 ml/m³ (1000 ppmv) whichever is more stringent. To ensure any device implemented meets this specification requires a detailed study of applicable limits depending on process conditions and secondary control device chosen.

  Typical secondary control devices used in the industry are:

  - Labyrinth seal or throat / throttle bushing – as those devices by their very nature are not tight, especially not when pressurized, they are not typically used as

secondary control devices, but API 685 3rd Edition does at least in theory permit them.

  - A backup lip seal of high-performance PTFE which runs on a hardened shaft sleeve (tungsten carbide or chromium carbide coated for example). While API 685 does not allow lip seals, they are a typical industry-accepted, low-cost solution for secondary control devices, especially in typical ASME B73.3 or ISO 15783 application envelopes (which are less than what API 685 aims for)
  - A dry-running backup mechanical seal that does not need any additional auxiliary services such as gas supply to operate in standby mode (i.e. as a dry seal). This is the most robust solution which reliably meets or exceeds the requirement of 24 hours 'wet' and 25,000 hours 'stand by' operation and can exceed these requirements in many cases. However, we must still be clear, that in "wet" condition this is essentially just a single-acting seal that is being relied upon to contain highly toxic liquids.

- **Secondary containment** is a second boundary rated to hold the process at design conditions. A **double-wall (secondary) containment shell** is the clearest example: if the primary shell is breached, the secondary shell retains full process pressure, no process reaches atmosphere, and the pump can keep running until a planned shutdown. A **gas-lubricated dual seal** (used as a backup seal to a single isolation shell) can also deliver zero leakage, at the cost of a reliable gas supply. Most canned motor pumps are considered fulfill all requirements of the double containment classification. However, in their case one must take care that the full secondary containment layers (including for example, but not limited to the electrical feed through barrier) are rated to full process pressure and temperature and have not degraded over prolongated time due to absolute process temperatures or temperature cycles. Additionally, procedures need to be defined and implemented on how the function of these barriers can be monitored while the pump is operating.

Measure	Type	Leakage outcome after a primary breach	Basis
Labyrinth seal or throat / throttle bushing	**Control**	Restricts flow; leakage continues at a reduced rate	*API 685 provided it meets emission guidelines*
Backup lip seal	**Control**	Contains modest leakage in the lantern; not tight	*Industry practice*
Single-acting backup mechanical seal	**Control**	24h run-down (acc. API 685) with some leakage to atmosphere	*API 685 secondary control*
Double (secondary) containment shell	**Containment**	Full process held; zero atmospheric leakage	*API 685 secondary containment*
Gas-lubricated dual seal	**Containment**	Zero leakage; requires a reliable gas supply	*API 685 secondary containment*

Table 2. Secondary measures, classified by whether they control or contain

4.3 Detection is the layer that makes the others real

No backup is worth its rating without the instrumentation that triggers its use. The gap between a double containment shell's two walls is **monitored** — typically held at vacuum and watched by a pressure transmitter — so it is at once a containment volume **and** a leak detector: the first trace of process across the primary shell registers immediately.

This arrangement provides an additional functionality that is important for those most critical applications: The ability to ensure and monitor online, without the need to shutdown the pump to verify the integrity of the secondary pressure casing. The pressure transmitter will read one of three possible cases (see table 3).

Pressure Transmitter Reading	Status of Double Shell	Explanation / Reaction
Vacuum	**Everything ok**	No actions necessary. Both primary shell and secondary shell are tight, secondary containment system is available.
Atmospheric Pressure	**Atmospheric Side Compromised**	Either the atmospheric side shell, or the atmospheric side seal has been damaged. The pump no longer works with a secondary containment system, but no process liquid is exposed to atmosphere or into the secondary pressure casing.
Process Pressure	**Process Side Compromised**	The process side shell has been compromised. Process liquid has leaked into the secondary pressure casing. The pump is now operating without a secondary containment system and measures should be taken to shut down and decontaminate the pump in line with hazard analysis. No leakage to atmosphere has occurred.

Table 3. Pressure Transmitter Readings and their implication

Canned-motor pumps add stator-cavity moisture / leak detection as part of their secondary containment system. Though these systems typically only check for primary containment failure, they do not confirm that the secondary barrier integrity is still present.

Across both canned motor pumps and magnetic drive pumps, motor power, temperature and vibration monitoring catch the operational excursions of Section 4.2 **before** they reach the boundary; API 682's 4th edition made the same shift on the sealed side, defaulting to continuous transmitters rather than switches.

A full-pressure secondary boundary, plus continuous detection, plus a defined safe-shutdown response, is what converts a primary breach from an incident into a managed event (Figure 3).

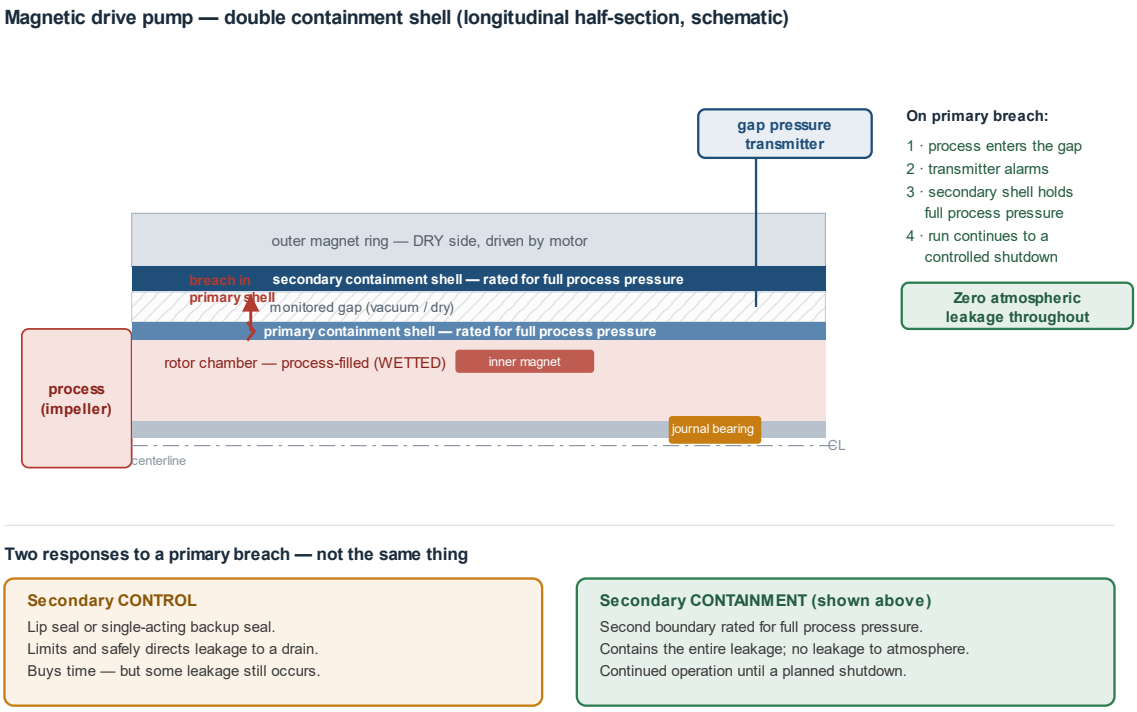

Figure 3. Magnetic drive pump with a double containment shell and a monitored gap, and the contrast between secondary control and secondary containment.

The most advanced example of this approach is a true hybrid double containment shell. It consists of a primary metallic containment shell and a secondary non-metallic containment shell made of heavy-duty industrial ceramics. Between both shells is a vacuum barrier, which is continuously monitored using a pressure transmitter.

Both shells can be independently pressure tested during production and are each rated for full pump design pressure. The pressure transmitter can be used to verify the integrity of both shells independently as shown in Table 3. The advantage of the hybrid metallic / non-metallic construction is that this shell has a comparable efficiency to a traditional single metallic shell, providing far superior efficiency than the classic double metallic shells without compromising on reliability.

5 Canned-motor specifics

A canned-motor pump is sometimes presented as **inherently** providing secondary containment, because the pressure-retaining outer housing sits behind the stator can, and API 685 recognizes this. But the inherent boundary only counts as secondary containment if it is actually **qualified for the duty**: rated for full process pressure and — the point most easily overlooked — compatible with the process fluid's chemistry **and temperature**.

A secondary boundary not verified against the actual liquid (a hot heat-transfer fluid, or an acid that would attack the housing material or a gasket) is not containment in any meaningful sense; it is an unproven assumption.

The same is true if the secondary containment integrity cannot be continuously monitored without shutting down the pump.

The other practical difference is **serviceability**: a breached canned-motor primary boundary generally requires motor disassembly to address, whereas a magnetic drive containment shell is typically a site-serviceable component.

6 Selection guidance

There is no single correct architecture; the right choice follows from consequence severity, the value placed on continued operation, and utility availability. Table 4 maps severity to the **minimum** architecture that matches it — a floor, not a ceiling.

Consequence severity (example)	Minimum architecture that matches it
Low — low toxicity, easily detected, tolerant of minor emission	Single seal (Arrangement 1), or a basic sealless pump
Moderate — flammable or moderately toxic, emission-regulated	Dual unpressurized seal (Arrangement 2), or sealless with secondary control
High — acutely toxic, atmospheric release unacceptable	Dual pressurized seal (Arrangement 3), or sealless with secondary containment + monitoring
Extreme — acutely toxic and / or above autoignition temperature, zero acceptable release	Sealless with full secondary containment + continuous monitoring: magnetic drive double shell, a qualified canned motor with suitable monitoring of both primary and secondary integrity, or a gas-lubricated dual seal where utilities exist

Table 4. Matching architecture to consequence severity.

For the most demanding services — acutely toxic liquids, fluids handled above their autoignition temperature, and any duty where atmospheric release is simply unacceptable — the strongest readily-available combination is a **magnetic drive sealless pump with a hybrid double containment shell and gap monitoring**. It provides **full-pressure secondary containment** (not merely secondary control), continued operation to a controlled shutdown, and **zero atmospheric leakage** after a primary breach — without depending on an external gas or barrier-fluid supply, and while remaining site-serviceable and most importantly while being continuously monitorable for both primary and secondary containment integrity.

That conclusion is bounded by honest trade-offs. Magnetic drive pumps – just as other sealless pumps – are sensitive to unexpected solids and to low-flow / NPSH excursions, and metallic containment shells carry an eddy-current power loss. Where a clean gas supply is reliably available, a gas-lubricated dual seal reaches a comparable zero-leakage outcome by a different route, though at much higher operational cost. A canned-motor pump can match the containment claim where its secondary boundary is properly qualified for the fluid and where site serviceability matters less.

The framework, not the verdict, is the real deliverable: **specify the layers the consequence demands, label control and containment clearly, and make sure something is always watching the boundary.**

7 References and further information

Hybrid double containment shells:

https:/ www.klaus-union.com/wp-content/uploads/PI_Klaus_Union_Hybrid-Double-Containment-Shell.pdf

Secondary mechanical seal (secondary control):

https://www.klaus-union.com/wp-content/uploads/PI_Klaus_Union_Secondary-Mechanical-Seal.pdf

NoVisco® bearings for extremely low viscosity applications:

https://www.klaus-union.com/wp-content/uploads/PI_Klaus_Union_NoVisco_Bearings.pdf

Handling liquids containing solids with magnetic coupled pumps – possible approaches:

https://www.klaus-union.com/wp-content/uploads/PI_Klaus_Union_Handling-Liquids-Containing-Solids.pdf

Appendix A Specifying checklist for the buyer

Information to be provided by buyer:

When specifying a pump for hazardous service, the following information should be made available to the vendor:

- ☐ What are the operating conditions? Not only at rated point, but also startup and transient conditions?
- ☐ What liquid data should be expected? The complete range of viscosity, density, vapor pressure and temperature is important, again keeping in mind transient conditions, special commissioning conditions, etc.
- ☐ What kind of solids should be expected? Amount, size, hardness, but also any other properties, such as polymerizing, ferromagnetic etc.

Information to be provided by the vendor:

These are the questions to put to **any** vendor, of any architecture, before a hazardous-liquid pump is specified. They follow the layers of Figure 1 and are deliberately answerable in writing; a confident supplier will answer each one with evidence rather than category labels.

A.1 Primary containment boundary

- ☐ Is the shell or can material qualified for the process chemistry and for the full temperature range, including credible upset, not only normal operation?
- ☐ Is the boundary rated for the maximum process pressure plus credible upset/settle-out pressure, rather than for normal operating pressure alone?
- ☐ Is the thermal-cycling and start/stop envelope defined, and does the intended duty remain inside it?

A.2 Internal bearings

- ☐ What is the product-lubricated bearing-life basis, and which fluid properties (viscosity, lubricity, vapor margin) does it depend on?
- ☐ What is the minimum continuous flow, the NPSH margin, and the dry-running / low-flow tolerances?

A.3 Detection

- ☐ What is monitored: containment-gap pressure, stator-cavity moisture, motor power, temperature, vibration? Which of these apply to this design?
- ☐ Are continuous transmitters used rather than simple switches, are alarm and trip setpoints defined, and is the protection independent of the basic control system?

A.4 Secondary measure — control or containment?

- ☐ Is the secondary measure secondary CONTROL (it limits and directs leakage) or secondary CONTAINMENT (it holds the full process)?
- ☐ If secondary containment is claimed: is the second boundary rated for FULL process pressure at design temperature, and separately qualified against the actual fluid — chemistry and temperature?
- ☐ If secondary containment is claimed: is the integrity of the secondary boundary continuously monitorable without the needing to shutdown the pump?
- ☐ After a primary breach, for how long can the pump operate safely, and is leakage to atmosphere genuinely zero or merely limited? On what test evidence does the answer rest?

A.5 Safe shutdown (this should be a joined discussion with vendor, considering process requirements)

- □ Is there a defined response on a containment alarm — alarm, controlled shutdown, isolation — and what is the run-down behavior until the pump is safe?

A.6 Serviceability and evidence

- □ Is the containment boundary site-serviceable, or does repair require motor / stator disassembly?
- □ Can the vendor supply an API 685 (3rd edition) conformance statement, ATEX certification with the temperature class for this duty, material certificates, type-test or qualification evidence, and reference installations in comparable service?