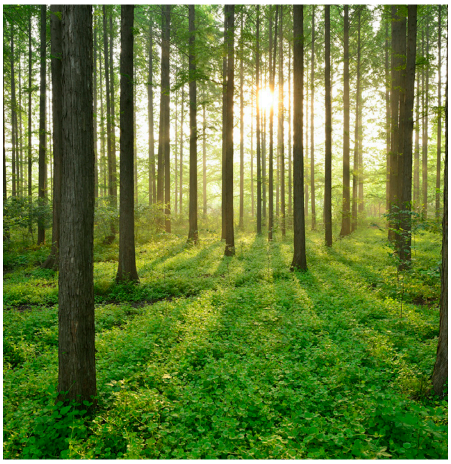
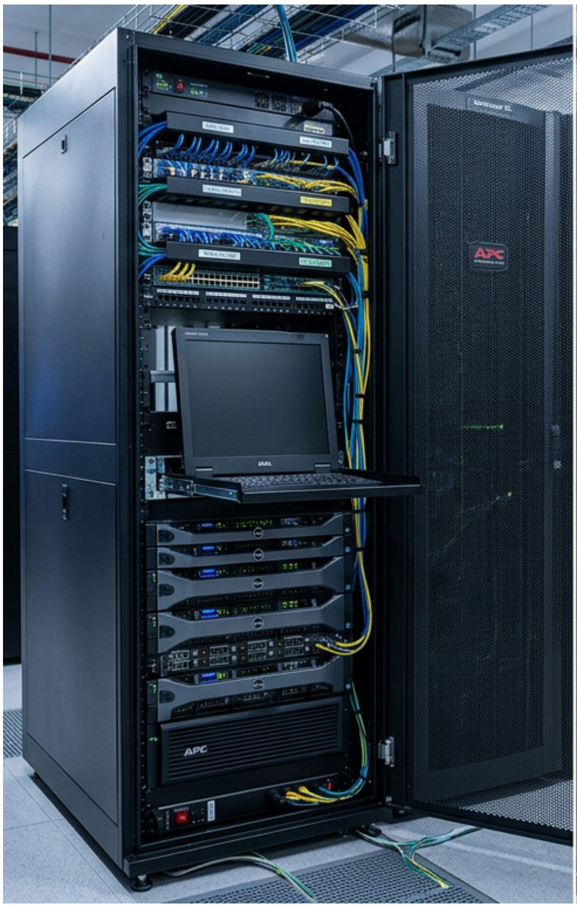
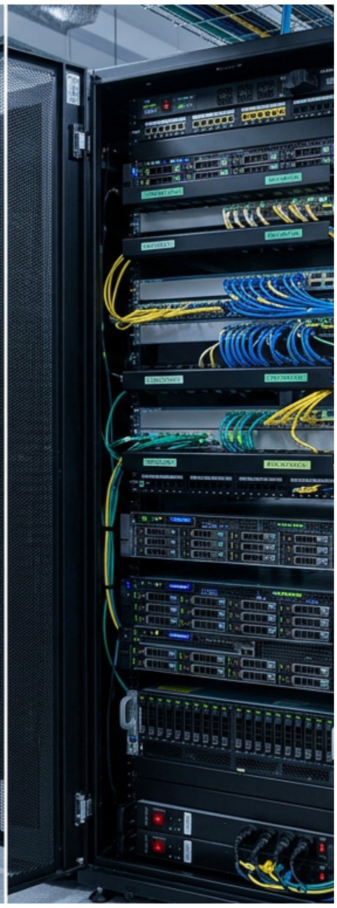
VIRTUALIZATION PLATFORMS COMPARISON

REPORT 2026:1205



ENERGIFORSK NUCLEAR SAFETY RELATED I&C, ENSRIC





Energiforsk

Virtualization platforms comparison

A pre-study to evaluate virtualization platform suitability for the nuclear industry

DANIEL NAGY OCH LISA SAHLIN

ISBN 978-91-89917-48-4| © Energiforsk June 2026

Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

Reliable and maintainable digital systems are essential for the long-term operation of nuclear power plants. Increasing reliance on virtualization introduces opportunities and challenges, particularly regarding stability, offline operation, and preservation of legacy systems in highly regulated environments.

This study evaluates the suitability of different virtualization platforms for Nordic nuclear power plant applications. It provides a structured comparison of available technologies, focusing on key requirements such as legacy support, offline operability, licensing models, and long-term maintainability.

The results of the study shortlists three platforms, but also highlights that no single platform fulfils all requirements and that each nuclear power plant therefore must continue the evaluation based on the individual needs of the specific plant.

This report forms the results of a project performed within the Energiforsk Nuclear Safety Related I&C (ENSRIC) Program, which is financed by Vattenfall, Uniper, Fortum, TVO, Skellefteå Kraft and Karlstads Energi. The Energiforsk Nuclear Safety Related I&C (ENSRIC) Program aims to increase the knowledge of aspects affecting safety, maintenance and development of I&C systems and their components in the Nordic nuclear power plants. Part of this is to investigate possibilities to facilitate and simplify the work that is performed in the nuclear business.

The work was performed by Daniel Nagy and Lisa Sahlin with support from Andreas Pihstrand from Rejlers and from Marie-Louise Axenborg and Pontus Ryd from Solvina part of Rejlers.

These are the results and conclusions of a project, which is part of a research programme run by Energiforsk. The author/authors are responsible for the content.

Summary

This pre-study provides a structured and independent assessment of virtualization platforms for use in Nordic nuclear power plant environments, where long-term stability, offline operability, and legacy system support are critical requirements.

The study evaluates a range of platforms representing different virtualization approaches, including traditional enterprise hypervisors (Hyper-V and VMware), open-source alternatives (Proxmox VE), Kubernetes-based virtualization solutions (Red Hat Virtual Datacenter / OpenShift Virtualization and SUSE Harvester), and an OT-focused platform (SEAPATH). The evaluation is based on publicly available documentation and applies a weighted scoring framework to compare different criteria against each other based on their importance to the nuclear industry, aligned with nuclear industry requirements.

Key evaluation criteria include Type-1/bare-metal capability, support for legacy 32-bit systems, offline operability, licensing model, commercial risk, and documentation strength. These criteria reflect the specific constraints of nuclear environments, where systems must operate reliably over long lifecycles with limited external dependencies.

The results indicate that certain platforms demonstrate a stronger overall fit for nuclear industry requirements than others. Proxmox VE, Windows Server Datacenter with Hyper-V emerge as the strongest overall candidates, though for different reasons. Proxmox VE performs well due to its licensing independence, strong offline capabilities, and flexibility for legacy workloads. However, it has weaker formal enterprise documentation and lifecycle guarantees. Hyper-V, by contrast, represents a stable and well-documented enterprise solution with strong vendor support and clear legacy compatibility models, but with greater dependency on commercial licensing.

Other platforms present more specialized strengths. VMware vSphere/ESXi remains technically mature and well documented, but its overall suitability is reduced by subscription-based licensing, increased vendor dependency and lifecycle-related considerations. OpenShift Virtualization and SUSE Harvester are more aligned with modernization and container convergence but introduce additional operational complexity and are less suited for legacy preservation. SEAPATH offers strong alignment with operational technology environments but is less mature as a general-purpose virtualization platform.

The study highlights several critical findings:

Energiforsk

- Support for legacy 32-bit systems is a key requirement and a major differentiator between platforms
- Offline operation is generally possible, but lifecycle management in isolated environments varies significantly
- Licensing models and commercial risk play a central role in long-term suitability
- Strong vendor documentation is essential for regulatory defensibility

Overall, the study concludes that platform selection must balance technical capability, long-term operability, and commercial risk. It is also essential that the evaluation and selection process consider the specific operational, regulatory, and infrastructure requirements of each individual nuclear power plant. While no single platform fully satisfies all requirements, Proxmox VE and Windows Server Datacenter with Hyper-V provide the strongest basis for further plant specific evaluation.

Keywords

Virtualization platforms, Nordic nuclear power plant environments, Offline operation, Legacy system support

Sammanfattning

Denna förstudie presenterar en strukturerad och oberoende utvärdering av virtualiseringsplattformar för användning i nordiska kärnkraftverk, där krav på lång livslängd, offlinekapacitet och stöd för äldre system är centrala.

Studien omfattar flera typer av plattformar, inklusive etablerade enterprise-lösningar (Hyper-V och VMware), open source-alternativ (Proxmox VE), Kubernetes-baserade lösningar (Red Hat Virtual Datacenter / OpenShift Virtualization och SUSE Harvester) samt en OT-anpassad plattform (SEAPATH). Utvärderingen baseras på publikt tillgänglig dokumentation och genomförs med hjälp av en viktad bedömningsmodell som är anpassad till kärnkraftsindustrins krav.

De viktigaste utvärderingskriterierna är stöd för Type-1/bare-metal, hantering av äldre 32-bitars system, offline-funktionalitet, licensmodell, kommersiell risk samt tillgänglighet och kvalitet på dokumentation. Dessa speglar de särskilda förutsättningarna i kärnkraftsmiljöer, där system måste vara stabila över lång tid och kunna drivas utan kontinuerlig extern uppkoppling.

Resultaten visar att Proxmox VE och Windows Server Datacenter med Hyper-V är de starkaste kandidaterna, men med olika styrkor. Proxmox VE utmärker sig genom sin licensoberoende modell, starka offlinefunktionalitet och flexibilitet för äldre system. Samtidigt saknas delvis formell företagsdokumentation och tydliga livscykelgarantier. Hyper-V erbjuder i stället en stabil och väl dokumenterad företagslösning med starkt leverantörsstöd och tydliga modeller för kompatibilitet med äldre system, men med större beroende av kommersiell licensiering.

Övriga plattformar har mer nischade styrkor. VMware är tekniskt mogen men påverkas negativt av förändrade licensmodeller och ökat leverantörsberoende. OpenShift Virtualization och SUSE Harvester är mer inriktade på modernisering och samlad hantering av virtuella maskiner och containrar, men innebär ökad komplexitet och är mindre lämpade för att bevara äldre system. SEAPATH är starkt anpassad för OT-miljöer, men generellt mindre mogen som virtualiseringsplattform.

Studien drar flera viktiga slutsatser:

- Stöd för 32-bitars legacy-system är en avgörande faktor
- Offline-drift är generellt möjligt, men livscykelhantering skiljer sig mellan plattformar

- Licensmodell och kommersiell risk har stor påverkan på långsiktig användbarhet
- Tydlig dokumentation är avgörande i regulatoriska miljöer

Sammanfattningsvis visar studien att val av plattform kräver en avvägning mellan teknisk flexibilitet, långsiktig stabilitet och kommersiellt oberoende. Det är också avgörande att utvärderings- och urvalsprocessen beaktar de specifika operativa, regulatoriska och infrastrukturrelaterade kraven för varje enskilt kärnkraftverk. Ingen plattform uppfyller alla krav fullt ut, men Proxmox VE och Hyper-V framstår som de mest relevanta alternativen beroende på prioriteringar.

List of content

List of words and abbreviations

Table 1. List of words and abbreviations

Term / abbreviation	Meaning
NPP	Nuclear Power Plant. In this report, the term refers to Nordic nuclear power plant environments.
ENSRIC	Nuclear Safety Related Instrumentation and Control program coordinated by Energiforsk.
Type-1 hypervisor	A hypervisor that runs directly on physical server hardware. Also referred to as a bare-metal hypervisor.
Type-2 hypervisor	A hypervisor that runs on top of a general-purpose operating system.
Bare metal	Physical server hardware without an additional general-purpose operating system layer between the hardware and the virtualization platform.
I&C	Instrumentation and Control. Systems used to monitor, control and protect industrial or nuclear processes.
OT	Operational Technology. Hardware and software used to monitor and control physical processes, equipment and industrial systems.
Virtualization	A technology that allows one physical server to run multiple isolated virtual machines or workloads.
Hypervisor	The software layer that creates and runs virtual machines by abstracting the underlying physical hardware.
VM	Virtual Machine, a software-defined computer that runs its own operating system and applications.
Guest OS	The operating system running inside a virtual machine.
Host	The physical server or virtualization node that runs the hypervisor and virtual machines.
Multilib	A compatibility approach that allows 32-bit software components to run in a 64-bit operating system environment.

Term / abbreviation	Meaning
KVM	Kernel-based Virtual Machine, a Linux-based virtualization technology used by several evaluated platforms.
QEMU	An emulator and virtualization component commonly used together with KVM to run virtual machines.
KubeVirt	A Kubernetes extension that enables virtual machines to be managed within a Kubernetes environment.
Kubernetes	A platform for managing containerized workloads and related infrastructure.
Container	A lightweight application runtime environment that shares the host operating system kernel.
HCI	Hyperconverged Infrastructure, an infrastructure model that combines compute, storage and virtualization in an integrated platform.
Air-gapped environment	An environment that is physically or logically isolated from external networks, including the internet.
HA	High Availability, the ability of a system to maintain or restore service after failure, often through clustering or restart mechanisms.
Live migration	Moving a running virtual machine from one host to another with limited or no downtime.
Snapshot	A point-in-time state of a virtual machine or storage volume, typically used for short-term restore or operational rollback.
Disaster Recovery	Disaster Recovery, processes and capabilities used to restore systems after major failure, such as site or cluster loss.
RBAC	Role-Based Access Control, a method for assigning system permissions based on roles and responsibilities.
Audit logging	Logging of administrative and system actions to support traceability, review and compliance.

Term / abbreviation	Meaning
Hardening	The process of reducing security risk by configuring systems according to security best practices.
Encryption at rest	Protection of stored data through encryption when it is not actively being transmitted or processed.
TPM	Trusted Platform Module. Hardware or virtual hardware used to support secure boot, attestation and cryptographic functions.
HSM	Hardware Security Module, a dedicated device used to protect and manage cryptographic keys.
LTS	Long-Term Support, a support model where a product version receives maintenance and security updates for an extended period.

1 Introduction

1.1 BACKGROUND

Energiforsk, through the ENSRIC (Energiforsk Nuclear Safety Related I&C) program, is initiating a research project to support the long-term operation and modernization of digital systems used in Nordic nuclear power plants. As nuclear facilities increasingly rely on virtualization to extend the lifetime of software-based systems, reduce hardware dependencies, and optimize operational costs, a systematic assessment of available virtualization technologies has become essential. However, nuclear power environments place unique requirements on virtualization platforms such as offline operability, long-term stability, support for legacy 32-bit operating systems, redundancy, and reliable backup solutions. At the same time, vendors are shifting from perpetual licenses to subscription-based models, creating additional challenges for nuclear power plants that cannot rely on continuous connectivity. This pre-study provides an independent, structured, and comprehensive study that maps available platforms, evaluates their suitability, and provides actionable recommendations.

1.2 VIRTUALIZATION PLATFORM AND HYPERVISOR TYPES

A virtualization platform is a software layer that enables multiple virtual machines or workloads to run on the same physical server. Each virtual machine can run its own operating system and applications while sharing the underlying hardware. In this study, virtualization is assessed as a way to replace ageing physical hardware while preserving existing software-based systems. A distinction is commonly made between Type-1 and Type-2 hypervisors. A Type-1 hypervisor runs directly on the physical server hardware and is commonly used in enterprise and datacenter environments. A Type-2 hypervisor runs on top of a general-purpose operating system, for example on a desktop or workstation. Virtualization should also be distinguished from emulation. Virtualization allows a guest operating system to run on modern hardware through a hypervisor, while emulation attempts to recreate hardware behavior in software. Emulation can be relevant for specific legacy systems that depend on obsolete hardware, processor architectures or timing behavior that cannot be handled through virtualization. However, emulation is generally more specialized, may introduce performance and supportability constraints, and often requires more extensive validation. For this reason, emulation is treated as a possible special-case approach, but not as a general substitute for 32-bit guest operating system support in the evaluated virtualization platforms.

1.3 PURPOSE AND GOALS

The purpose of the pre-study is to provide an independent comparative analysis of current virtualization platforms and assess their suitability for deployment in Nordic nuclear power plants. The pre-study has the following goals:

- Provide an overview of available virtualization platforms relevant to nuclear industry requirements.
- Define and describe the key features and evaluation criteria including potential licensing models relevant for NPP's, offline capability, redundancy, backup and disaster recovery options, legacy 32-bit OS support, and Type-1 hypervisor capabilities.
- Evaluate selected platforms.
- Deliver a comparative analysis supported by a structured assessment framework.
- Present clear findings, conclusions and recommendations for use in Nordic NPP environments.

2 Methodology

2.1 OVERALL METHODOLOGICAL FRAMEWORK

The project was conducted using a structured and systematic methodology combining data collection and evaluation, comparative analysis, and comprehensive documentation. During the initial phase, project requirements were aligned with the steering group, and the selection of virtual platforms included within the study scope were finalized based on these requirements. This process established a shared understanding of the project objectives, evaluation criteria, and expected deliverables.

The project was planned and executed over an approximate eight-week period, progressing from governance setup and scoping through evaluation, comparative analysis, and final synthesis. All outcomes were documented in this report, prepared in accordance with Energiforsk's reporting standards.

2.2 DATA COLLECTION AND EVALUATION

The platforms were selected to cover the main virtualization approaches considered relevant for Nordic nuclear power plant environments, namely established enterprise hypervisors, open-source oriented virtualization, Kubernetes managed virtualization and OT focused virtualization. Hyper-V and VMware represent established enterprise virtualization, Proxmox VE represents an open KVM-based alternative, OpenShift Virtualization and SUSE Harvester represents VM/container convergence through Kubernetes, and SEAPATH was included due to its OT and energy-sector relevance.

The evaluations were based on publicly available technical documentation from vendors and relevant open-source projects. This includes official product documentation, lifecycle and support policies, licensing information, compatibility guides, security and hardening guidance, release notes, and architecture documentation. The main sources are official documentation from Red Hat, SUSE/Harvester, Microsoft, Proxmox, Broadcom/VMware and SEAPATH/LF Energy. General KVM/QEMU documentation has only been used as technical background for underlying virtualization capabilities, not as proof of vendor-certified support. No vendor-internal, customer-specific or non-public documentation has been used. Since a detailed comparison of virtualization platforms can be challenging, as each vendor determines what information is made publicly available, the assessment is presented at an appropriate level of detail that enables the findings to be efficiently absorbed, interpreted, and applied.

The features in the evaluation matrix were derived from the study scope, the project objectives and the expected comparison areas described in the request from Energiforsk. Additional features were included where they were needed to compare the platforms in a consistent way, for example lifecycle, security, automation and commercial risk. The weighted assessment criteria were identified based on their relevance to long-term operation in NPP environments. These criteria include Type-1/bare-metal support, 32-bit OS/legacy support, offline operability, licensing model, commercial risk and documentation/regulatory defensibility. Type-1/bare-metal support and 32-bit OS/legacy support were given the highest individual weight because they are directly linked to replacing ageing hardware while preserving existing software.

Altogether, the data gathering and evaluation focused on the collection and review of publicly available technical documentation, the definition of relevant functional and technical evaluation criteria, and the assessment of each virtualization platform using a standardized evaluation framework. This ensured a consistent and transparent basis for cross-platform comparison and supported the identification of platform-specific strengths, limitations, risk, constraints, and overall suitability for nuclear power plant environments.

2.3 COMPARATIVE ANALYSIS USING SCORING AND WEIGHTING

To evaluate the features against each other a scoring method was used. The scoring method was developed for this pre-study and is not a formal certification standard. Each platform was scored from 1 to 5 based on its alignment with the selected criteria and the available public documentation. Weighting is often applied to give greater or less emphasis to specific factors when they are considered to differ in importance within the analysis. In this case, weighting was used to account for the fact that certain features were deemed more influential than others, ensuring that their relative importance was appropriately reflected. Bare-metal/Type-1 support and 32-bit legacy support were weighted highest because they relate directly to replacing ageing hardware while preserving existing software. Offline operability, licensing model and lifecycle/commercial risk were also weighted highly due to the need for long service life, controlled changes and limited external dependency. The scoring should be interpreted as a comparative assessment framework, not as a formal qualification result.

2.4 LIMITATIONS

The pre-study includes several limitations in order to maintain focus on the most relevant aspects of virtualization platforms for nuclear power plant environments. The selected scope is based on relevance, applicability, and the specific requirements associated with safety-critical industrial systems.

Type-2 hypervisors were excluded from the detailed evaluation. The study focuses on platforms suitable for long-term, server-based and offline operation, including native Type-1 hypervisors and bare-metal-capable virtualization platforms. Type-2 hypervisors run on top of a general-purpose operating system and are therefore less aligned with the intended use case, where controlled infrastructure, reduced operational complexity and long-term maintainability are important.

The study does not include hands-on testing, proof-of-concept deployment or laboratory validation. Compatibility with specific legacy operating systems, application stacks, hardware configurations, drivers, backup workflows, offline update procedures and security configurations would need to be verified in the target environment before any deployment decision is made.

The study does not include a full cybersecurity assessment. Cybersecurity-related features such as patching, access control, audit logging, hardening guidance and encryption are considered as part of this platform comparison, but detailed threat modelling, vulnerability assessment, penetration testing and security architecture review are outside the scope of this pre-study.

The study does not include a detailed cost or total cost of ownership analysis. Licensing model, commercial risk and vendor dependency are considered at a comparative level, but detailed pricing, procurement conditions, support agreements, migration costs, internal staffing costs and long-term operational costs would need to be assessed separately.

3 Included platforms

Below, the platforms included in the pre-study are listed and briefly described.

3.1 RED HAT VIRTUAL DATACENTER / OPENSHIFT VIRTUALIZATION

Table 2. Information about Red Hat Virtual Datacenter / Openshift Virtualization

Parameter	Description
General profile	Enterprise Kubernetes platform with virtualization capabilities through OpenShift Virtualization.
Market position / maturity	Mature enterprise platform in the Kubernetes and container platform market; virtualization use case is newer than traditional hypervisor platforms.
Typical use cases	Container platforms, hybrid cloud, application modernization and mixed VM/container environments.
Workload model	Supports containerized workloads and virtual machines.
License model	Commercial Red Hat subscription model.
Offline relevance	Supports disconnected operation, but requires controlled management of registries, images, operators and update artifacts.
Reason for inclusion	Included to represent VM/container convergence and Kubernetes-managed virtualization.

3.2 SUSE HARVESTER

Table 3. Information about Suse Harvester

Parameter	Description
General profile	Open-source-based HCI and virtualization platform built around Kubernetes and KubeVirt/KVM.
Market position / maturity	Newer and less broadly established than the largest enterprise hypervisor platforms.

Parameter	Description
Typical use cases	Hyperconverged infrastructure, open-source virtualization and edge or isolated environments.
Workload model	Primarily virtual machine workloads, with Kubernetes-based platform integration.
License model	Open-source-based platform with commercial support options through SUSE.
Offline relevance	Air-gapped installation and operation are documented.
Reason for inclusion	Included to represent an open-source-based HCI alternative with air-gap capability.

3.3 WINDOWS SERVER DATACENTER WITH HYPER-V

Table 4. Information about Windows Server Datacenter with Hyper-V

Parameter	Description
General profile	Microsoft enterprise virtualization platform included with Windows Server.
Market position / maturity	Mature and established enterprise platform, particularly in Windows-based environments.
Typical use cases	Enterprise server virtualization, Windows infrastructure, private cloud and controlled datacenter environments.
Workload model	Primarily virtual machines. Container support exists in the broader Windows ecosystem but is not the main focus of this evaluation.
License model	Commercial Microsoft Windows Server licensing.
Offline relevance	Supports established enterprise patterns for local activation and controlled update distribution.
Reason for inclusion	Included as a conservative enterprise baseline with strong vendor documentation and predictable lifecycle handling.

3.4 PROXMOX

Table 5. Information about Proxmox

Parameter	Description
General profile	Open-source-based virtualization platform using KVM/QEMU.
Market position / maturity	Established in open-source, SMB, hosting and technically oriented environments; less formal enterprise positioning than Microsoft or VMware.
Typical use cases	Server virtualization, self-managed infrastructure, hosting, lab environments and cost-sensitive deployments.
Workload model	Supports virtual machines and Linux containers.
License model	Open-source-based platform with optional commercial subscriptions and enterprise repository access.
Offline relevance	Provides documented mechanisms for repository mirroring and offline subscription handling.
Reason for inclusion	Included as an open, offline-oriented and licensing-independent virtualization alternative.

3.5 VMWARE

Table 6. Information about VMware

Parameter	Description
General profile	Enterprise virtualization platform based on VMware ESXi and vSphere management.
Market position / maturity	Mature and widely established enterprise virtualization platform.
Typical use cases	Large enterprise virtualization, datacenter consolidation, high availability, migration and integration with enterprise infrastructure tooling.
Workload model	Primarily virtual machines, with broad ecosystem integration.
License model	Commercial Broadcom/VMware subscription-based licensing model.

Parameter	Description
Offline relevance	Can operate offline, but downloads, update artifacts and entitlement workflows depend on vendor-controlled processes.
Reason for inclusion	Included as a mature enterprise virtualization benchmark.

3.6 SEAPATH

Table 7. Information about Seapath

Parameter	Description
General profile	OT-focused open-source virtualization platform developed for digital substations and critical energy infrastructure.
Market position / maturity	Niche and emerging compared with established enterprise virtualization platforms.
Typical use cases	Digital substations, IEC 61850 environments, real-time OT workloads and virtualized protection, automation and control systems.
Workload model	Focused on virtualized OT workloads rather than general enterprise IT workloads.
License model	Open-source-based LF Energy project; commercial support depends on ecosystem and implementation model.
Offline relevance	Conceptually aligned with isolated OT environments, although public documentation on long-term offline lifecycle management is less extensive.
Reason for inclusion	Included as an OT- and energy-sector-oriented virtualization candidate.

4 Evaluation criteria and features

4.1 FEATURE SELECTION AND CATEGORIZATION

The selected features were included to compare the platforms from the perspective of long-term use in nuclear power plant environments. The features cover technical suitability, offline operation, lifecycle, licensing, recovery, security, documentation and market risk. To make the evaluation transparent, the features were grouped into three categories: weighted assessment criteria, operational assessment criteria, and supporting context criteria. Weighted assessment criteria are the criteria used directly in the final scoring model. These criteria were selected because they have the strongest influence on platform suitability in the intended use case. They include Type-1/bare-metal support, 32-bit OS/legacy support, offline operability, licensing model, commercial risk and documentation/regulatory defensibility. Operational assessment criteria are important sub-criteria that inform one or more weighted criteria but are not scored separately in the final weighted table. For example, air-gapped environment support, internet dependency, and offline licensing inform the assessment of offline operability and licensing. This avoids double-counting closely related aspects while still preserving the technical details needed to explain the scores. Supporting context criteria provide additional background on architecture, security, maturity, ecosystem, and operational complexity. These criteria do not determine the final score on their own, but they help explain platform-specific strengths, limitations, and implementation risks. Cybersecurity is treated as a cross-cutting consideration in the evaluation. In offline or air-gapped environments, reduced external connectivity may reduce some external exposure, but it does not remove the need for controlled patching, vulnerability management, access control, audit logging, hardening, secure configuration and recovery procedures. In this study, cybersecurity is therefore mainly assessed through features that affect secure long-term operation in isolated environments. These include security patch frequency, role-based access control, audit logging, hardening guidance, encryption at rest, TPM/HSM support, lifecycle documentation and offline update handling. These features inform the assessment of documentation/regulatory defensibility, offline operability and operational risk rather than being scored as one separate cybersecurity criterion.

4.2 FEATURE OVERVIEW

Table 8 summarizes the features considered in the study including their priority and an explanation of each.

Table 8. Feature overview and description.

Category	Feature	Explanation	Supports assessment of
Weighted assessment	Type-1 / bare-metal support	Assesses whether the platform can run directly on physical hardware and is suitable for bare-metal virtualization.	Scored directly in the weighted result.
Weighted assessment	32-bit OS / legacy support	Assesses whether the platform can preserve legacy 32-bit operating systems or software environments on modern hardware, primarily through virtual machines and, where relevant, multilib compatibility.	Scored directly in the weighted result.
Weighted assessment	Offline operability	Assesses whether the platform can run, be maintained and updated without internet access.	Scored directly in the weighted result.
Weighted assessment	License model	Assesses whether the platform uses subscription, perpetual, open-source or optional support models.	Scored directly in the weighted result.
Weighted assessment	Commercial risk	Assesses risk related to licensing changes, vendor dependency, support model, product packaging and long-term cost predictability.	Scored directly in the weighted result.
Weighted assessment	Documentation / regulatory defensibility	Assesses how clearly platform capabilities, lifecycle, support and operational requirements are documented in publicly available sources.	Scored directly in the weighted result.
Operational assessment	Air-gapped environment support	Assesses whether the platform has documented support for disconnected or isolated environments.	Offline operability
Operational assessment	Internet dependency	Assesses whether runtime, updates, activation or support processes depend on external connectivity.	Offline operability / Commercial risk
Operational assessment	Long-term stability / lifecycle	Assesses whether the platform has a lifecycle model suitable for long-term operation in conservative environments.	Commercial risk / Documentation
Operational assessment	LTS support length	Assesses the documented support duration for platform versions or underlying components.	Commercial risk / Documentation

Category	Feature	Explanation	Supports assessment of
Operational assessment	Offline licensing	Assesses whether licensing, activation and entitlement can be handled in disconnected environments.	Offline operability / License model
Operational assessment	High Availability	Assesses whether the platform can maintain or restore service after host or node failures.	Documentation / Operational suitability
Operational assessment	Failover support	Assesses whether workloads can be restarted or failed over after host, cluster or site failure.	Documentation / Operational suitability
Operational assessment	Backup integration	Assesses whether the platform has built-in or well-supported backup mechanisms.	Backup / Recovery / Operational suitability
Operational assessment	Disaster recovery support	Assesses whether the platform supports recovery after larger failures, including site or cluster loss.	Documentation / Operational suitability / Backup
Operational assessment	Legacy system compatibility	Provides a broader assessment of suitability for older systems beyond only 32-bit support.	32-bit OS / legacy support
Operational assessment	3-2-1 backup suitability	Assesses whether the platform can support backup strategies aligned with the 3-2-1 principle through built-in tools, ecosystem integrations or documented backup architecture.	Backup integration / Disaster recovery support
Operational assessment	Security patch frequency	Assesses how security updates are released and whether the model is predictable.	Offline operability / Documentation
Operational assessment	Storage architecture / diskless node support	Assesses whether the platform can support resilient storage architectures, including external/shared storage, distributed storage, diskless node concepts or witness/quorum mechanisms where relevant.	Offline operability / Documentation / Operational suitability
Operational assessment	Container support	Assesses whether the platform supports containerized workloads or integrates virtualization with container platform capabilities.	Type-1 / bare-metal support / Operational suitability

Category	Feature	Explanation	Supports assessment of
Supporting context	GPU / hardware pass-through	Assesses whether physical hardware devices can be assigned directly to virtual machines.	Technical suitability
Supporting context	Automation & APIs	Assesses how well the platform can be automated and integrated into controlled operational processes.	Operational complexity
Supporting context	Vendor lock-in risk	Assesses dependency on a specific vendor, ecosystem, licensing model or proprietary tooling.	License model / Commercial risk
Supporting context	Deterministic behavior	Assesses whether the platform is suitable for predictable or low-latency operation.	Technical suitability
Supporting context	Hypervisor type	Describes the underlying virtualization technology, for example KVM, Hyper-V or ESXi.	Type-1 / bare-metal support
Supporting context	Roadmap transparency	Assesses how clearly the vendor communicates lifecycle, release and roadmap information.	Commercial risk / Documentation
Supporting context	Cost level	Assesses general cost exposure based on available public information.	License model / Commercial risk
Supporting context	Live migration	Assesses whether running virtual machines can be moved between hosts with limited or no downtime.	Operational suitability
Supporting context	Snapshot handling	Assesses how the platform handles restore points and VM snapshots.	Backup / recovery
Supporting context	Role-based access control	Assesses whether access can be controlled by roles and responsibilities.	Security / Documentation
Supporting context	Audit logging	Assesses whether administrative and system actions can be logged and reviewed.	Security / Documentation
Supporting context	Hardening guidance	Assesses whether the vendor provides security hardening guidance or benchmark alignment.	Cybersecurity / Regulatory defensibility
Supporting context	Encryption at rest	Assesses whether stored data can be encrypted through native or storage-layer mechanisms.	Security suitability

Category	Feature	Explanation	Supports assessment of
Supporting context	TPM / HSM support	Assesses support for trusted platform modules, virtual TPMs or external key management.	Security suitability
Supporting context	IEC / nuclear standards alignment	Assesses whether the platform has explicit or indirect alignment with industrial, IEC or nuclear-related requirements.	Regulatory context
Supporting context	Market maturity	Assesses how well established the platform is in enterprise or industrial environments.	Commercial risk
Supporting context	Community / ecosystem strength	Assesses the size and maturity of the vendor, partner, support and open-source ecosystem.	Commercial risk / Maintainability
Supporting context	Technical risk	Assesses technical complexity, maturity and implementation risk.	Overall suitability

5 Results

The results of the study show how each platform scored across the respective features as well as their overall weighted score. Table 9 defines the requirements for each performance level, while Table 10 presents the scoring of each platform based on the extent to which those requirements are fulfilled.

5.1 SCORING FRAMEWORK

The results are presented using a scoring framework that consolidates the findings derived from the applied methodology. Each criterion is evaluated on a five-point scale, where 1 represents the weakest fit and 5 represents the strongest fit with respect to the assessed features. Table 9 outlines the criteria required to achieve each level for the weighted assessment criteria.

Table 9. Description and requirements of each level.

Feature/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Type-1 / bare metal	No clear bare-metal or Type 1 suitability	Indirect or unclear support	Capable but with added abstraction	Strong capability but not a classic standalone Type-1 hypervisor	Native Type-1 hypervisor or clearly documented bare-metal virtualization platform
32-bit legacy	No relevant evidence of 32-bit legacy suitability	Technically plausible, but not a documented product focus and requires validation	Possible support, but dependent on specific OS/version and support classification	Strong technical or documented legacy capability, but still requires OS-specific validation	Clearly documented and strong legacy support for the relevant 32-bit use case
Offline	No clear offline or air-gapped operating model	Runtime may be offline, but lifecycle/update process is unclear or weakly documented	Supported, but requires significant manual process or architecture	Strong offline operation model with documented update or servicing process	Strong and practical offline lifecycle model, including documented repository/mirror/update handling

Feature/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Licensing	Mandatory subscription or licensing model poorly aligned with long-term offline use	Commercial/proprietary model with significant dependency on vendor entitlement	Commercial licensing, but relatively established and predictable	Open or flexible model with optional support/subscription	Open-source or no mandatory runtime license dependency
Commercial risk	High uncertainty around pricing, packaging, lifecycle or vendor terms	Significant vendor dependency or commercial uncertainty	Manageable commercial risk, but with clear vendor or support dependency	Low commercial risk, though some support or operational dependency remains	Low license-related risk and high long-term commercial flexibility
Documentation	Limited public documentation, claims are difficult to verify	Some documentation exists, but several important claims rely on inference	Adequate documentation, but key areas require interpretation or validation	Strong documentation for most relevant capabilities	Strong, product-level, vendor documentation with clear lifecycle/support evidence

5.2 WEIGHTED SCORING RESULT

Table 9 was used as a tool to determine the score of each platform regarding the different features. To reflect the relative importance of the weighted assessment criteria for a nuclear power plant context, the individual criteria were weighed. The highest priority is assigned to requirements deemed critical for this use case, namely Type-1 (bare-metal) support, 32-bit legacy support, offline operability, licensing model, commercial risk, documentation and regulatory defensibility.

The applied weighting is as follows: Type-1/bare-metal support (20%), 32-bit legacy support (20%), offline operability (15%), licensing model (15%), commercial risk position (10%), and documentation and regulatory defensibility (20%). A higher score for commercial risk corresponds to a lower level of perceived commercial risk.

Table 10. Summary of weighted feature scoring.

Platform	Type-1 / bare metal	32-bit legacy	Offline	Licensing	Commercial risk	Documentation	Weighted score
Proxmox VE	5	4	5	5	4	3	4.3 / 5
Windows Server Datacenter with Hyper-V	5	4	4	3	3	5	4.15 / 5
VMware vSphere / ESXi	5	3	3	1	2	5	3.4 / 5
SUSE Harvester / SUSE Virtualization	4	2	3	5	3	3	3.3 / 5
SEAPATH	4	2	3	5	2	2	3.0 / 5
Red Hat Virtual Datacenter / OpenShift Virtualization	4	2	4	1	2	4	2.95 / 5

6 Analysis

The following sections present an analysis of each platform, examining and interpreting the results shown in Table 10.

6.1 RESULT INTERPRETATION

As shown in Table 10, Proxmox VE and Windows Server Datacenter with Hyper-V receive the highest weighted scores. The difference between them is small, and they should therefore be interpreted as the two strongest candidates rather than as a clear first and second place. Proxmox VE receives the highest weighted score because it combines strong offline operability, low licensing dependency and broad KVM/QEMU-based flexibility for legacy workloads. However, this result should be interpreted together with its lower score for formal enterprise lifecycle and regulatory documentation depth. Successful use in an NPP environment would therefore require strong internal governance, validation and support arrangements. Windows Server Datacenter with Hyper-V scores almost equally high and represents the strongest conservative enterprise baseline. It provides native Type-1 virtualization, documented Generation 1 VM legacy capability, established offline activation and update models, and strong vendor documentation. Its lower score in licensing reflects dependency on Microsoft's commercial licensing and ecosystem.

6.2 HYPER-V

Windows Server Datacenter with Hyper-V is assessed as the strongest conservative enterprise option in this comparison. It is a native Type-1 hypervisor, has a clear relationship with the Windows Server lifecycle, supports established enterprise patterns for local activation and controlled update distribution, and provides documented legacy compatibility through Generation 1 virtual machines. This makes Hyper-V well aligned with environments where predictability, vendor documentation and long-term enterprise support are prioritized. Its main limitation is dependency on Microsoft licensing, activation models and the broader Microsoft ecosystem. This dependency does not make the platform unsuitable, but it should be treated as a relevant long-term consideration.

6.3 PROXMOX VE

Proxmox VE is assessed as the strongest open and offline-oriented alternative. It is based on KVM/QEMU, runs directly on bare metal, provides a practical model for offline repository handling and does not require a mandatory subscription for runtime operation, although enterprise support and access to enterprise repositories are subscription-based. Proxmox VE is particularly well aligned with requirements related to licensing independence, offline lifecycle control and technical flexibility for legacy workloads. For 32-bit legacy systems, Proxmox VE should be interpreted as technically flexible rather than formally guaranteed. Its KVM/QEMU foundation makes 32-bit guest operation technically plausible, and its traditional virtualization model gives operators broad control over virtual machine configuration. However, public Proxmox documentation does not provide a formal long-term support guarantee for specific legacy 32-bit guest operating systems. The score for 32-bit legacy support therefore reflects technical flexibility and practical plausibility, not vendor-certified support for every legacy operating system or assurance that such systems will remain unaffected by future platform updates. Its main limitation is that it does not provide the same formal vendor-style long-term enterprise lifecycle or regulatory documentation depth as Microsoft or VMware. This means that successful use in an NPP environment would depend on strong internal governance, configuration control, validation and support arrangements.

6.4 VMWARE VSPHERE / ESXI

VMware vSphere/ESXi remains one of the most technically mature platforms out of the ones included in the study. It has a long enterprise track record and strong capabilities for high availability, live migration, backup integration and operational tooling. However, its overall suitability is reduced by commercial and lifecycle-related factors rather than by core virtualization capability. The transition to subscription-based licensing, release-specific lifecycle management and dependency on vendor entitlement and portal-based workflows make VMware less attractive for long-lived offline environments. VMware remains technically strong and may remain suitable where the required guest operating systems, support contracts and platform release are aligned, but the assessment identifies a higher commercial and strategic dependency risk compared to Hyper-V and Proxmox VE.

6.5 RED HAT VIRTUAL DATACENTER / OPENSHIFT VIRTUALIZATION AND SUSE HARVESTER

Red Hat Virtual Datacenter / OpenShift Virtualization and SUSE Harvester/SUSE Virtualization are relevant where modernization and convergence between virtual machines and containers are important. Although the two platforms differ in product scope, ecosystem maturity and commercial model, they can be seen as similar since both represent Kubernetes-managed virtualization rather than a classical standalone hypervisor model. Both platforms use KVM/KubeVirt-based virtualization and can run virtualization workloads on bare metal. However, their operational model is Kubernetes-based, which introduces additional lifecycle processes, abstraction layers and operational dependencies compared with classical standalone hypervisors such as Hyper-V or VMware ESXi. This may be valuable in environments where container platforms, automation and VM/container convergence are strategic objectives, but it is less directly aligned with a conservative legacy-preservation scenario. Both platforms can be operated in disconnected or air-gapped environments, but the practical maintainability of such environments depends on disciplined handling of registries, container images, operators, update artifacts and platform lifecycle procedures. Their 32-bit legacy suitability is assessed as technically plausible through the KVM base but should not be interpreted as vendor-certified support for specific legacy operating systems. Based on the selected criteria, OpenShift Virtualization and SUSE Harvester/SUSE Virtualization are therefore best understood as modernization-oriented virtualization platforms rather than primary candidates for conservative long-term legacy preservation. They may be relevant where Kubernetes-based operations are already accepted or strategically desired, but they introduce additional operational complexity compared with the strongest candidates in this evaluation.

6.6 SEAPATH

SEAPATH is strategically relevant from an OT and energy-sector perspective. Its focus on real-time operation, high availability and IEC 61850 digital substation environments makes it more directly aligned with critical energy infrastructure than the general-purpose enterprise platforms. At the same time, SEAPATH is assessed as less mature as a general enterprise virtualization platform. Based on the reviewed public documentation, SEAPATH is stronger around OT alignment, real-time intent and digital substation use cases than around broad enterprise lifecycle management, backup and restore, disaster recovery, commercial support and legacy OS preservation. Based on the available public documentation, SEAPATH is therefore better positioned as an OT-focused candidate than as the primary general-purpose virtualization platform.

6.7 KEY FINDINGS

6.7.1 32-bit legacy support is a decisive requirement

The need to support 32-bit legacy systems is one of the central drivers for virtualization in this study. In this context, 32-bit support does not mean that the virtualization platform itself is expected to run on 32-bit physical hardware. Rather, it refers to the ability to preserve older 32-bit operating systems or software environments by running them as guest workloads on modern 64-bit host hardware. Most of the evaluated platforms are technically capable of running 32-bit guest operating systems in some form, but for different reasons and with different levels of documentation and support. The main distinction is therefore not only whether 32-bit operation is technically possible, but whether it is clearly documented, supportable and suitable for long-term use in a regulated environment. For KVM-based platforms, such as Proxmox VE, OpenShift Virtualization, SUSE Harvester/SUSE Virtualization and SEAPATH, 32-bit guest operation is technically plausible because the underlying virtualization technology is KVM/QEMU. KVM/QEMU is broadly capable of running older x86 guest operating systems, including 32-bit systems, on modern 64-bit hardware. However, this does not automatically mean that each product vendor certifies or supports every legacy operating system. The practical supportability still depends on the specific guest OS, the platform version, the virtual hardware profile and the required drivers or tools. Proxmox VE is assessed as the strongest KVM-based candidate for legacy preservation because it exposes KVM/QEMU in a relatively direct and traditional virtualization model. It is less tied to a Kubernetes-based operating model, has strong offline lifecycle tooling and provides high flexibility when configuring virtual machines. However, this should not be interpreted as formal vendor-certified long-term support for specific 32-bit legacy operating systems. Its suitability for 32-bit legacy preservation must therefore be validated against the exact guest operating system, application stack, virtual hardware profile and future update path. In particular, platform updates should be tested before deployment to ensure that the selected legacy workload remains functional. Hyper-V is also assessed as a strong candidate because Microsoft documents Generation 1 virtual machines, which provide legacy BIOS-based virtual hardware and compatibility with older operating systems. This gives Hyper-V a clearer vendor-documented legacy path than the Kubernetes-based platforms. However, as with all platforms, the exact operating system and application stack must still be tested in the target configuration. VMware vSphere/ESXi remains technically capable for some legacy workloads, but its long-term suitability is more dependent on Broadcom's Compatibility Guide, guest operating system support classifications and the lifecycle of the vSphere platform itself. Older guest operating systems may be classified as Supported, Legacy, Deprecated, Terminated or Unsupported. This means that VMware may remain usable for some older systems, but its supportability depends strongly on the exact guest OS, vSphere release and support classification. In addition, the lifecycle of the VMware platform itself must be considered. OpenShift Virtualization and SUSE Harvester/SUSE Virtualization can technically run 32-bit guests through their KVM/KubeVirt foundation, but they are not primarily positioned as legacy-preservation platforms. Their strength is VM/container convergence and Kubernetes-based operations. Therefore, their 32-bit suitability should be treated as technically plausible, but requiring validation rather than as a vendor-certified legacy capability. SEAPATH is also KVM-based, which makes 32-bit guest operation technically plausible. However, its public documentation focuses mainly on real-time operation, IEC 61850 digital substations and OT-oriented workloads rather than preservation of legacy 32-bit operating systems. For this reason, SEAPATH should not be considered a primary legacy-preservation platform without further validation.

Overall, the evaluation indicates that Proxmox VE and Hyper-V are the strongest candidates for 32-bit legacy preservation, but for different reasons. Proxmox VE provides the strongest technical flexibility through KVM/QEMU, while Hyper-V provides the clearest vendor-documented legacy VM model through Generation 1 virtual machines. VMware remains technically capable but is more dependent on guest OS support classification and platform lifecycle. OpenShift, SUSE Harvester and SEAPATH are technically plausible but require stronger validation for this specific use case.

6.7.2 Type-1 and bare-metal capability must be interpreted precisely

Hyper-V and VMware ESXi are classical native Type-1 hypervisors. Proxmox VE is a bare-metal KVM-based virtualization platform. These platforms are the easiest to map to a traditional virtualization model. OpenShift Virtualization and SUSE Harvester also use KVM-based virtualization on bare metal, but the operational model is Kubernetes/KubeVirt-based. They should therefore be treated as Kubernetes-managed virtualization platforms rather than classical standalone hypervisors. SEAPATH is also KVM-based and aligned with bare-metal OT use cases, but it is more specialized and less productized as a general enterprise virtualization platform.

6.7.3 Backup and recovery capabilities differ in maturity and implementation model

Backup and recovery is an important operational differentiator in this evaluation, even though it is not scored as a separate weighted criterion. In a nuclear power plant environment, these capabilities are relevant not only for technical failure recovery, but also for controlled maintenance, rollback, configuration governance and recovery from human error or security-related incidents. The evaluation indicates that VMware vSphere/ESXi, Windows Server Datacenter with Hyper-V and Proxmox VE have the clearest practical backup and recovery positions, but for different reasons. VMware benefits from a mature enterprise ecosystem with broad third-party backup integration and established operational tooling. Hyper-V benefits from the broader Windows Server ecosystem, including failover clustering, Hyper-V Replica and integration with enterprise backup solutions. Proxmox VE has a strong integrated backup position through Proxmox Backup Server, which makes backup, restore and separated backup storage a central part of the platform architecture. Red Hat Virtual Datacenter / OpenShift Virtualization and SUSE Harvester/SUSE Virtualization can also support backup and recovery, but the practical design is more dependent on the surrounding Kubernetes, storage, operator and platform architecture. This does not make them unsuitable, but it increases the importance of validating the complete backup and restore workflow rather than only the virtualization layer. SEAPATH is aligned with high-availability OT use cases, but the reviewed public documentation provides less evidence of broad enterprise backup, restore and disaster recovery workflows. For offline or air-gapped environments, backup suitability should be assessed as part of the complete deployment architecture rather than as an isolated product feature. The relevant question is not only whether a platform supports backup or snapshots, but whether backup data can be stored, verified, restored and protected without dependency on continuous external connectivity.

6.7.4 Offline operation is broadly possible, but offline lifecycle management differs

All evaluated platforms can operate in offline or disconnected environments in some form. The main difference is how installation, patching, updating, licensing and recovery are handled over time without internet access. Proxmox VE has the clearest practical model for offline maintenance through offline repository and mirror tooling. Hyper-V also has a strong and well-understood offline model through Windows Server update and activation mechanisms. VMware can operate offline, but update artifacts, support access and entitlement workflows are more dependent on vendor portals and contract status. OpenShift and SUSE Harvester support disconnected or air-gapped operation, but require more complex internal handling of registries, container images, operators and update artifacts. SEAPATH is conceptually aligned with offline OT environments, but public documentation around long-term offline lifecycle operations is less mature.

6.7.5 Licensing and commercial risk materially affect suitability

Licensing is a significant factor in this evaluation because the intended environments are long-lived, offline or semi-isolated, and require predictable maintenance conditions over time. A licensing model that depends on recurring subscriptions, vendor entitlement systems or changing product packaging may introduce operational and commercial uncertainty, particularly when systems are expected to remain stable for many years. The preference for perpetual or non-subscription-based licensing is therefore understandable in the context of nuclear power plant environments. However, the evaluation also shows that the wider enterprise software market is moving increasingly toward subscription-based models. This is visible in VMware's transition under Broadcom, where perpetual licenses have been replaced by subscription offerings, and in Red Hat's subscription-based OpenShift model. In practice, this means that subscription dependency may not always be avoidable if the organization selects a major enterprise vendor platform. Proxmox VE, SUSE Harvester and SEAPATH have the strongest licensing position in this comparison because they are open-source-based and do not require mandatory runtime subscriptions. This reduces license-related lock-in and improves long-term independence. However, this does not remove the need for support arrangements, lifecycle planning, internal competence and controlled update processes. Hyper-V and VMware are both proprietary and vendor-dependent platforms. Hyper-V's dependency is tied to Microsoft licensing, Windows Server lifecycle policy and activation models, but it is assessed as comparatively predictable and well documented. VMware's dependency is tied to Broadcom's subscription-based licensing, product packaging and entitlement-based lifecycle model, which creates greater commercial uncertainty in the context of long-lived offline environments. OpenShift also carries commercial dependency through Red Hat's subscription and entitlement model. This may be manageable where OpenShift is strategically justified, but it is less aligned with requirements where long-term offline stability, licensing independence and cost predictability are central concerns.

Overall, licensing should not be treated only as a cost factor. In this context, it is also a lifecycle and operational risk factor. Platforms with lower license dependency provide greater strategic independence, while subscription-based enterprise platforms may provide stronger vendor support but require acceptance of long-term commercial dependency.

6.7.6 Documentation strength affects regulatory defensibility

In a regulated environment, technical capability alone is not sufficient. The ability to justify a platform choice depends heavily on documented vendor support and clear operational evidence. Hyper-V, VMware and OpenShift generally provide the strongest vendor documentation. Proxmox VE provides strong technical documentation, especially around offline operation and backup, but less formal enterprise lifecycle framing. Harvester and SEAPATH require more careful interpretation because parts of the assessment rely on architecture, underlying components or project-level documentation rather than long-established enterprise product evidence.

6.7.7 Cybersecurity depends on platform capabilities and site-specific operation

Cybersecurity is not assessed as a separate standalone ranking criterion in this study, because platform security depends on several combined factors. These include access control, audit logging, hardening guidance, encryption, patch management, lifecycle control, backup integrity and the ability to maintain the platform securely in an offline or air-gapped environment. Based on public documentation, the established enterprise platforms, particularly Windows Server Datacenter with Hyper-V, VMware vSphere/ESXi and Red Hat Virtual Datacenter / OpenShift Virtualization, generally provide the strongest public documentation for security-related administration, hardening and lifecycle management. Proxmox VE provides relevant technical security capabilities, but with less formal enterprise security and compliance framing. SUSE Harvester/SUSE Virtualization and SEAPATH include relevant security mechanisms through their underlying Linux, Kubernetes, KVM or OT-oriented architectures, but their public documentation is less extensive for regulated enterprise use. The evaluation therefore does not identify one platform as generally "best" for cybersecurity. Instead, cybersecurity suitability should be assessed in relation to the target plant's architecture, network segmentation, offline update process, access control model, logging requirements, backup strategy, internal competence and regulatory expectations. Offline operation may reduce some external exposure, but it also increases the importance of controlled internal patching, vulnerability management and configuration governance.

7 Conclusion and recommendations

To conclude, this pre-study evaluated a selection of virtualization platforms against requirements considered relevant for nuclear power plant environments, with particular focus on Type-1/bare-metal capability, 32-bit legacy support, offline operability, licensing, commercial risk and documentation strength. The results show that no single platform is universally optimal for all nuclear power plant contexts. Instead, the suitability of a platform depends heavily on the specific technical, cybersecurity, operational and regulatory conditions of the individual facility. Factors such as existing infrastructure, legacy system dependencies, organizational competence, lifecycle expectations, cybersecurity requirements, vendor relationships and regulatory strategy are all decisive for platform selection.

Based on the analysis, Proxmox VE and Windows Server Datacenter with Hyper-V emerge as the strongest overall candidates for further evaluation, although for different reasons. Proxmox VE demonstrates strong flexibility, offline operability and licensing independence, while Hyper-V provides a more traditional enterprise model with strong vendor documentation and established lifecycle processes. VMware vSphere/ESXi remains technically mature but introduces greater commercial and lifecycle dependency risks. OpenShift Virtualization, SUSE Harvester/SUSE Virtualization and SEAPATH may also be relevant in specific contexts, particularly where Kubernetes-based operations, modernization initiatives or OT-focused use cases are strategic priorities.

The purpose of this study is therefore not to recommend a single virtualization platform, but rather to identify which platforms appear most relevant for continued investigation in nuclear power plant environments. Any final platform decision should be based on detailed validation, testing and assessment within the specific operational and regulatory context of the target facility.

7.1 RECOMMENDATIONS

Based on the findings of this study, the next step should be a more detailed technical and operational evaluation of the most relevant candidate platforms within a representative nuclear power plant environment. In particular, Proxmox VE and Windows Server Datacenter with Hyper-V are recommended for continued investigation due to their strong overall alignment with the evaluated requirements.

Future work should focus on practical validation of critical use cases, including long-term operation of legacy 32-bit systems, offline patch and update management, backup and disaster recovery procedures, cybersecurity, and integration with existing operational technology (OT) environments. Regulatory and lifecycle considerations should also be evaluated in greater depth, including documentation requirements, supportability, change management and long-term maintainability.

Where specific legacy systems cannot be preserved through standard virtualization, emulation may be assessed as a separate special-case option rather than as a general alternative to virtualization. Such assessment should include performance, timing behavior, hardware dependencies, supportability, cybersecurity implications and validation requirements.

In addition, a more detailed, deployment-specific evaluation is recommended before deciding on the virtual platform. This should include hands-on testing or proof-of-concept validation in the target environment, verification of compatibility with existing systems and infrastructure, a comprehensive cybersecurity assessment, as well as a detailed cost and total cost of ownership analysis covering both implementation and long-term operations.

VIRTUALIZATION PLATFORMS COMPARISON

Reliable and maintainable digital systems are essential for the long-term operation of nuclear power plants. Increasing reliance on virtualization introduces opportunities and challenges, particularly regarding stability, offline operation, and preservation of legacy systems in highly regulated environments.

This study evaluates the suitability of different virtualization platforms for Nordic nuclear power plant applications. It provides a structured comparison of available technologies, focusing on key requirements such as legacy support, offline operability, licensing models, and long-term maintainability.

The results of the study shortlists three platforms, but also highlights that no single platform fulfils all requirements and that each nuclear power plant therefore must continue the evaluation based on the individual needs of the specific plant.

A new step in energy research

The research company Energiforsk initiates, coordinates, and conducts energy research and analyses, as well as communicates knowledge in favor of a robust and sustainable energy system. We are a politically neutral limited company that reinvests our profit in more research. Our owners are industry organisations Swedenergy and the Swedish Gas Association, the Swedish TSO Svenska kraftnät, and the gas and energy company Nordion Energi.

Energiforsk