

# Versions

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Change** |
| 03-03-2025 | 0.1 | Created first draft. Added chapters ‘theoretical background’ & ‘Research questions’ |
| 10-03-2025 | 0.2 | Added chapter ‘Assignment’ |
| 13-03-2025 | 0.3 | Added chapter ‘Theoretical framework’ |
| 26-03-2025 | 0.4 | Added CPU tests ‘Methods and Technology E1’ |
| 27-03-2025 | 0.5 | Added chapter ‘Hypothesis, CPU’, updated research questions, added OS, scripting software and container engine to chapter ‘Justification of choices’. |
| 04-04-2025 | 0.6 | Added chapter ‘Methods E2’ |
| 10-04-2025 | 0.7 | Added chapter results ‘Results CPU’ |
| 24-04-2025 | 0.8 | Rewrote chapter ‘theoretical framework’. Combined chapter ‘theoretical background’ into ‘theoretical framework’ |
| 28-04-2025 | 0.9 | Rewrote ‘Hypothesis chapter and added the Memory and I/O sub-chapters. Wrote the chapter ‘Methods’. Started rewriting the ‘Results’ section. |
| 29-04-2025 | 0.10 | Chapter structure form Hypothesis, Method, Results, Discussion to chapters per experiment. |

# Distributions

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Shared with** |
| 01-05-2025 | 0.10 | Tweede examinator, process begeleider & technisch begeleider. |
|  |  |  |

# Preface

# Executive summary

Contents

[Versions 2](#_Toc197519432)

[Distributions 2](#_Toc197519433)

[Preface 3](#_Toc197519434)

[Executive summary 4](#_Toc197519435)

[Assignment 6](#_Toc197519436)

[Context 6](#_Toc197519437)

[Goals 6](#_Toc197519438)

[Research questions 8](#_Toc197519439)

[Theoretical framework 9](#_Toc197519440)

[Real-time embedded systems 9](#_Toc197519441)

[Containers in real-time embedded systems 9](#_Toc197519442)

[The Linux Kernel and Container Processes 10](#_Toc197519443)

[Process Isolation: Linux Namespaces 10](#_Toc197519444)

[Resource Management: Control Groups (cgroups) 11](#_Toc197519445)

[Filesystems and storage 11](#_Toc197519446)

[Summary 11](#_Toc197519447)

[General experimental setup 12](#_Toc197519448)

[CPU experiments 13](#_Toc197519449)

[Experiment C1: Overhead single container 13](#_Toc197519450)

[Hypothesis 13](#_Toc197519451)

[Method 13](#_Toc197519452)

[Results 14](#_Toc197519453)

[Discussion 15](#_Toc197519454)

[Experiment C2: Container overhead multiple containers 17](#_Toc197519455)

[Hypothesis 17](#_Toc197519456)

[Method 17](#_Toc197519457)

[Results 17](#_Toc197519458)

[Discussion 17](#_Toc197519459)

[Memory experiments 18](#_Toc197519460)

[Experiment M1: Overhead single container 18](#_Toc197519461)

[Hypothesis 18](#_Toc197519462)

[Method 18](#_Toc197519463)

[Results 19](#_Toc197519464)

[Discussion 23](#_Toc197519465)

[Experiment M2: Influence swap memory on containers 25](#_Toc197519466)

[Hypothesis 25](#_Toc197519467)

[Method 25](#_Toc197519468)

[Results 25](#_Toc197519469)

[Discussion 26](#_Toc197519470)

[Experiment M3: Influence OOM killer on Container 27](#_Toc197519471)

[Hypothesis 27](#_Toc197519472)

[Method 27](#_Toc197519473)

[Results 27](#_Toc197519474)

[Discussion 27](#_Toc197519475)

[I/O Experiments 28](#_Toc197519476)

[Experiment I1: Writing I/O performance single container 28](#_Toc197519477)

[Hypothesis 28](#_Toc197519478)

[Method 28](#_Toc197519479)

[Results 29](#_Toc197519480)

[Discussion 29](#_Toc197519481)

[Experiment I2: Reading I/O performance single container 30](#_Toc197519482)

[Hypothesis 30](#_Toc197519483)

[Method 30](#_Toc197519484)

[Results 30](#_Toc197519485)

[Discussion 30](#_Toc197519486)

[Experiment I3: Reading multiple files 31](#_Toc197519487)

[Hypothesis 31](#_Toc197519488)

[Conclusion 32](#_Toc197519489)

[Recommendations 33](#_Toc197519490)

[Justification of choices 34](#_Toc197519491)

[Experiment hardware 34](#_Toc197519492)

[Operating system 35](#_Toc197519493)

[Scripting software 35](#_Toc197519494)

[Container engine 36](#_Toc197519495)

[Description of realized professional products 37](#_Toc197519496)

[Evaluation of quality criteria 38](#_Toc197519497)

[Process evaluation 39](#_Toc197519498)

[References 40](#_Toc197519499)

[Appendix 45](#_Toc197519500)

# Assignment

## Organization

During the graduation period, the student did an internship at Capgemini. The company is an international consultancy firm that provides services in the areas of digital transformation, engineering and R&D. During the internship period the student worked as part of the engineering branch within the company. This branch focusses on the delivery of innovative solutions based on the needs of clients in the transition to a digital world. The company serves major clients like ASML and Philips (Capgemini Engineering, 2024).

Worldwide Capgemini employs 340,000 people, with 65,000 are working in the engineering branch. The student worked within the Embedded Software Engineering discipline. In the Netherlands this team consists of approximately 150 employees. Even though the student was part of this team, the student focused on the assigned research, as discussed in this document.

## Context

Even though container software like Docker was initially created for server environments (Johnston, 2024), they are significantly more being used in real-time embedded systems. The incorporation of containers in these systems presents numerous functional advantages. For instance, firmware is no longer confined to a single device and software becomes easily reusable (Bodet, 2023). However, the effect of containers on real-time performance remains relatively unknown (see chapter theoretical background, containers).

Containers consist of various abstraction layers. These different layers are responsible for the isolation of processes and resources, limitation and monitoring of resources and memory isolation for the container. The abstraction layers could potentially cause a lot of overhead. Therefore, it is important to conduct research to gain a better understanding of the possible unknown disadvantages and limitations of using containers on real-time embedded systems.

## Goals

The aim of this research project was to map the boundaries of containers on real-time embedded systems. To achieve the goal both theoretical and experimental research had to be done.

This research is mostly conducted from a curiosity perspective on behalf of the product owner. The results will not have direct impact on the projects that Capgemini does for its clients. The research results will mostly be used for reference within the organization for colleagues to gain knowledge about the subject in a relatively short time span.

To successfully complete the project the products described in the table below need to be realized. The described quality criteria are based on the wishes of the product owner.

Table 1 Products and quality

|  |  |  |
| --- | --- | --- |
| **Product** | **Description** | **Quality** |
| Automated experiment | Code must be written to automatically carry out several tests to map the boundaries. | ***Repeatability***: The experiment needs to be repeatable within the timespan of a weekend by a colleague.  ***Reproducibility***: The experiment needs to be written in a way it can be repeated on different hardware. |
| Research document | A document must be written in which the choices and research results are described. | ***Readability***: The document must be written in clear and understandable English. The document needs to provide insight in the experiments, the results and the conclusions in the form of a ‘blog post’ format.  ***Substantiated***: the conclusions in the document must be clearly substantiated using graphs and diagrams. The sources for the conclusions need to be included. |

In addition to the products that needed to be provided for the company, the student worked on this thesis document to demonstrate the necessary skills for graduation.

# Research questions

To obtain meaningful research results, the following research questions were used.

***Main question:***

*What are the practical limits when using containers on real-time embedded systems, focused on the potential restrictions in the areas CPU-bound, memory-bound and I/O-bound, and how can these restrictions be explained?*

***Sub questions:***

The following sub questions will be used to answer the main research question.

* *Which Linux kernel features are used to run containers, and what theoretical risks, based on the three restricting factors can these features cause on real-time embedded systems?*

This question focusses on how containers operate and which building blocks they are made of. The theoretical background will be discussed in the chapter ‘Theoretical framework’. The theoretical knowledge will be used to form the hypotheses described in the ‘Hypothesis’ chapter.

* *How can an experiment be designed to map the practical limits of the CPU-bound, memory-bound and I/O-bound factors?*

To test the limitations of containers, experiments need to be designed. The methods used to map the limitations are described in the “Method” sub-chapters.

* *How can the practical limits from the experiment be explained?*

The experiment results need to be explained, which will be done in the ‘Discussion’ sub-chapters.

# Theoretical framework

In this chapter the theoretical foundation for the research will be outlined for running containers on real-time embedded systems.

## Real-time embedded systems

An embedded system is a combination of hardware and software designed to perform a specific task (GeeksforGeeks, 2022). When the task is time-critical, it is referred to as a ***real-time embedded system*** (RTOS LOGICS, 2020) , meaning the system must meet strict timing constraints for its operations (GeeksforGeeks, 2022).

Real-time embedded systems are typically classified as hard or soft real-time. In a hard real-time system, every deadline must be met, and a missed deadline can lead to complete system failure or unsafe situations (for example, in medical devices or aviation control systems). In contrast, a soft real-time system can tolerate occasional deadline misses, that only degrade the quality of service rather than cause a total failure (for example, multimedia streaming or online gaming)

## Containers in real-time embedded systems

Eventhough container technology originated in server environments, they are increasingly being used in embedded systems to leverage the benefits of portability, isolation, and scalability even on resource-constrained devices. Real-time embedded systems tend to have limited CPU power, memory and storage, resulting in the question what the practical limits are when using containers in these environments. Deploying containerized applications on a small embedded device could introduce overhead or resource contention that would not exist when running the same tasks natively. It’s important to research how the use of containers might affect system resources and timing.

​For this research three categories of potential performance bottlenecks are considered.

* ***CPU-bound***: A process is CPU bound when the execution speed is limited by the CPU’s processing power. The CPU limit can be reached by performing a lot of simple calculations in quick succession (Mortensen, 2009).
* ***Memory-bound***: A process is limited by the speed at which the memory (RAM) can be read from or written to (Mortensen, 2009).

# TODO: Add what type of program is suitable to reach the limit with source.

* ***I/O-bound***: A process is limited by the speed of an I/O subsystem. An example could be reading or writing to external data storage device. When the external medium is not able to keep up with the speed it is referred to as being I/O bound (Mortensen, 2009).

These categories are useful for analyzing container performance because container overhead might influence CPU usage, affect memory usage, or impact I/O. The experimental chapters focus on how containers perform under each of these constraints on a real-time embedded platform.

## The Linux Kernel and Container Processes

A diagram of a computer process

AI-generated content may be incorrect.Before being able to look at containers a basic understanding of Linux processes is necessary. The **Linux Kernel** is the core of the operating system that acts as the bridge between hardware and software applications on a system. It manages critical system resources, including the CPU, memory, and peripheral devices, and handles low-level tasks such as executing processes, managing memory, accessing files and coordinating I/O operations (GeeksforGeeks, 2025).

One of the responsibilities of the kernel is executing and managing processes.

In Linux, a process is an instance of a running program, including the program’s executed code and its allocated resources. A container is essentially a special Linux process. It runs on the same host kernel but is isolated so that it cannot see or affect the rest of the system outside its designated environment (Mullinix et al., z.d.)​.

### Process Isolation: Linux Namespaces

One of the essential features enabling container process isolation is done by the Linux namespace mechanism (Kuninoto, 2024). When the process is created the namespaces are set to provide isolation.

The Linux kernel implements multiple types of namespaces, each isolating a particular resource domain (Mullinix et al., z.d.).

* PID namespace: Isolates process ID’s. Each container gets its own process ID space. As a result, processes in the container can only be seen and reference process within that container’s PID namespace (Tiwari, 2024).
* Mount namespace (mnt): Isolates the filesystem view. Every container possesses its unique view of the filesystem, independent from the host and other containers (Tiwari, 2024).
* IPC namespace (inter process communication): Facilitates communication between processes (such as shared memory, semaphores, message queues). This namespace prevents interfering with other IPC’s (Boutnaru, 2023).
* UTS namespace: Allows the container to have its own host name (Arges, 2020).
* User namespace: Provides user ID (UID) and group ID (GID) separation, allowing containers to have different privilege levels compared to the host system.
* Network namespace (net): Provides network isolation. This namespace makes sure different containers have different IP addresses while sharing the same hardware (Arges, 2020).

### Resource Management: Control Groups (cgroups)

While namespaces isolate the view of resources, Linux control groups (cgroups) regulate the usage of resources by processes (Van Kalken, 2021). The main resource controls provided by cgroups include: CPU scheduling, memory usage, block I/O throughput, and network bandwidth. Using cgroups the percentage of CPU time, a fixed amount of RAM or a capped I/O rate can be limited.

Each container’s processes reside in their own cgroup hierarchy, ensuring that if a container process tries to overuse the CPU, memory or I/O the kernel will throttle it according to the limits defined in the cgroup. This prevents one container from starving the host or other containers of CPU cycles or memory.

### Filesystems and storage

Containers not only isolate processes and resource usage, but also the file system. ontainer frameworks use the union file systems to manage container images and storage. A union file system allows multiple distinct file system layers to be stacked or overlaid, presenting them as a single coherent file system to the container.

Using a union file system with copy-on-write semantics dramatically saves disk space and memory, since multiple containers can share one copy of an OS image or application binaries without duplication​.

For real-time embedded systems, the use of a union file system could mean that I/O performance might be affected by the extra layering. Reading a file might involve checking multiple layers and using the copy-on-write principle might lead to a slight overhead.

## Summary

In summary, container technology on Linux relies on kernel-provided features: namespaces to isolate process views, cgroups to control resource usage, and union file systems for efficient storage management. A real-time embedded system using containers will leverage these same mechanisms. Understanding how they work is crucial for anticipating how containerization might introduce performance overhead or resource contention in CPU-bound, memory-bound, or I/O-bound scenarios on real-time embedded systems.

# General experimental setup

By default, all experiments were performed on a Raspberry Pi Zero 2W running Raspberry Pi OS Lite (64-bit). The device features a 1 GHz quad-core ARM Cortex-A53 CPU and 512 MB of RAM, providing a constrained environment to test the practical limits.

The testing programs were created using Python. For each factor (CPU, memory and I/O) three scripts were created simulating varying resource intensities. In addition to the Python programs, bash scripts were created to automate doing the tests multiple times and to be able to log the results. Each test was performed ten times to account for variability.

For this research only Docker was used as the container software (see chapter ‘Justification of Choices’. The same base container was used for all the experiments. The container was built including Python version …(slim) with the necessary libraries installed. The files to run the experiments were mounted when the containers were created.

Details on how the experiments can be executed and reproduced can be found in the ‘experiment\_details.md’ file in the accompanying experimental repository.

# CPU experiments

The CPU-focused experiments were designed to measure the overhead introduced by containerization. To evaluate the impact of containers the following experiments were done.

1. Measuring the CPU overhead introduced by a single container.
2. Exploring the CPU limit when running multiple containers simultaneously.

To make sure no system processes could interfere with the measurements, cores were isolated for the program and container processes.

## Experiment C1: Overhead single container

The aim of the first experiment was to determine the overhead caused by a single container compared to running natively.

### Hypothesis

The overhead caused by a single container is expected to be very minimal on a Linux based system. Unlike VM’s containers share the host kernel and do no emulate hardware (Ferraz, 2022). Minor slowdowns can be caused by the various isolation layers, but they are minor and most likely negligible in practice (Morabito, 2016).

However, when running the container engine and the container on the same core, this might lead to longer execution times, since they share the same core and need to perform context switching.

*When running a program in a container minor CPU overhead is expected compared to running the program natively. When running the container and the engine on the same core, minor overhead can be expected.*

### Method

The experiment was conducted in three different test scenarios.

1. *Native execution (control):* In the control scenario, all three varying intensity Python programs were executed directly on the Raspberry Pi Zero 2 W, without containerization. To ensure consistent performance and limit the interference of different programs the control experiment was done on a single isolated CPU core.
2. *Separate container engine and container*: The Python programs were executed within a container on an isolated core, while the Docker engine was running on a separately isolated core.
3. *Same core container engine and container*: Both the Python program and the container engine were executed on the same core.

Each test was performed ten times per scenario to ensure reliability.

**Collected data**  
For each test, the execution time required to complete each type of program (simple, medium and long) and the total runtime of the container was recorded. These were automatically logged into CSV files. Additionally, CPU core usage and system load were monitored using htop to verify proper isolation and ensure no external processes interfered with the measurements.

### Results

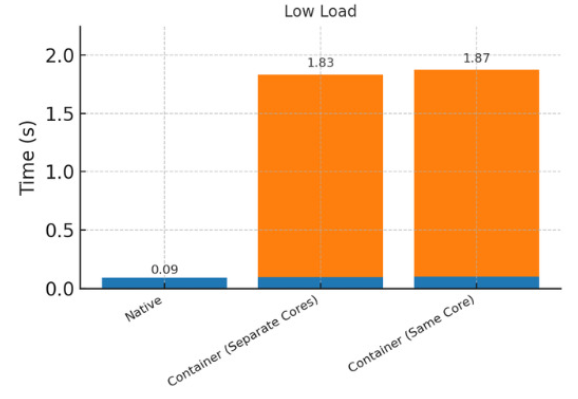
Experiment C1 measured the execution times for CPU-bound programs of varying complexities in both native and containerized environments. The execution times of three different CPU intensive Python programs were recorded while testing the three scenarios described in the methodology subchapter. Each measurement was done 10 times. Table … shows the average results of the measurements. It includes the program runtimes (Python program runtime) and the total execution time (Container runtime).

Table 2 Average program runtime and total execution time for each scenario under low, medium and high CPU workloads.

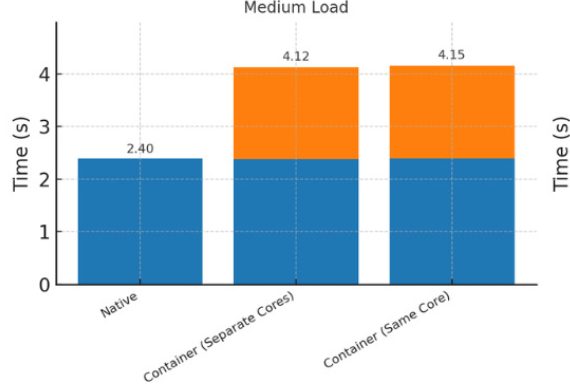
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Program** | **Control group** | **Container separate cores (program)** | **Container separate cores (total)** | **Container same core (program)** | **Container same core (total)** |
| *Simple* | 0.09 | 0.10 | 1.83 | 0.10 | 1.87 |
| *Medium* | 2.40 | 2.39 | 4.12 | 2.39 | 4.15 |
| *Long* | 44.46 | 46.84 | 56.94 | 46.79 | 56.27 |

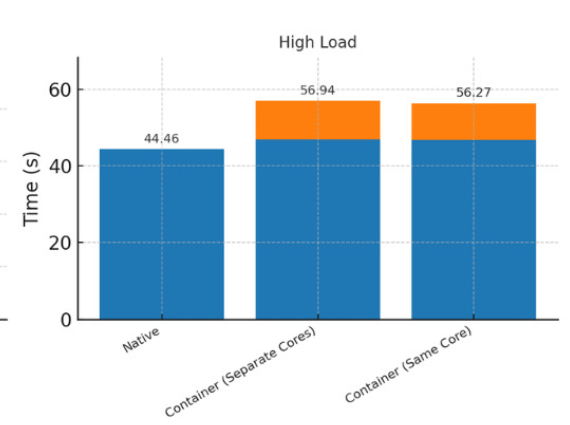
Based on the table results figures …, … and … were created to visualize the results. The blue bars represent the program runtime, and the orange bars the additional time the containers process required.

**Low CPU load**

Under the low CPU workload, the native executed program finished in 0.09 seconds on average. Within the container the program execution times were nearly identical (0.10 s). The total execution time, including the container process, was much higher. For the container and the engine running on separate cores the test took 1.83 seconds. The container and engine running on the same core took 1.87 seconds to finish (almost 20x longer than the runtime of the program itself).

**Medium CPU load**

At medium load the native execution took about 2.40s on average. The containerized program runtime remained virtually the same for both container scenarios (2.39s). For both containers the total runtime was higher (at 4.12s) for the container and engine running on different cores, and 4.15s for the container and engine running on the same core. This is roughly 1.7s of extra time compared to the native run (~70% increase over the program runtime).

**High CPU load**

For the high CPU load task, the native execution of the program finished in 44.46s on average. The containerized program runtimes took slightly longer, at roughly 46.8s for both scenarios. When looking at the container runtime, the separate core scenario averaged at 56.94s and the shared core scenario at 56.27s. Containerization introduced roughly 11-12 seconds of additional delay.

#### Summary

Across all workloads, the containerized scenario showed a noticeable overhead in total execution time, while the program runtime remained quite similar to the natively executed program. For both the low and medium CPU loads the added overhead was approximately 1.7s. The overhead is significant compared to the program runtime. For the high load scenario, the absolute overhead was larger (~12s), but the relative overhead was a lot smaller compared to the other intensity tests (~25%). compared to the less intensive scenarios.

### Discussion

This experiment evaluated the performance overhead of running a single container compared to native execution. Below the results are discussed in comparison to the hypothesis.

**Minimal overhead program runtime**

The overhead caused by containers on the program runtime is minimal when looking at the three different CPU intensity scripts. The simple, medium and heavy CPU load within the containers resulted in very similar runtimes compared to the natively executed program. This is in accordance with the understanding that containers do not share the host OS and do not emulate hardware. Resulting the should add minimal overhead in their tasks.

The high workload program showed an average runtime of 44.66 seconds natively and 46.8 seconds for both container configurations. This only means an increase of about 5%, which is little enough to confirm the hypothesis. For the short and medium scripts the increase was even less. The slight difference could have multiple causes. Additional research and experiments need to be done to determine the exact causes of the minor increase.

**Significant overhead total runtime**

While the program runtimes were consistent, the runtime difference when looking at the total container runtime is substantial.

The relative overhead is largest for small tasks and gets relatively less the longer the task is. Looking at the easiest CPU intensive program the added runtime was … %, whilst for the highest intensity calculation the increase in time was only ~25%.

The execution of the container itself includes container creation and managing the container. Looking at the results, this demonstrates that these tasks cause significant overhead.

**Difference engine and container shared core and separate core**

On of the expectations mentioned in the hypothesis was that the container sharing the same core with the engine would have a longer runtime compared to the scenario where the container and engine were isolated on separate cores. However, the results did not reveal a consistent performance difference between the two scenarios.

The Docker daemon is most likely only active during the startup and shutdown. When the program inside the container is being executed the daemon becomes idle, therefore not competing with the program for CPU cycles.

## Experiment C2: Container overhead multiple containers

This experiment was conducted to assess the CPU overhead introduced by containerization when increasing the amount of running containers. The goal was to determine if and when the performance starts to decrease compared to running the same amount of containers natively.

### Hypothesis

When running multiple containers the primary performance limit is most likely that the CPU cores need to be shared between the processes rather than containerization itself (ZPiDer, 2018). As the number of processes increases, each process gets a smaller share of the CPU cycles, therefore resulting in longer completion times.

*When running multiple containerized programs simultaneously, the runtime should be quite similar to running the same number programs natively.*

### Method

# Aanvullen op basis van aanpassingen die gemaakt moeten worden om te vergelijken met native.

**Collected data**The main data collected during this experiment were the container- and script runtimes. The data was stored in a CSV file.

* *Container timings:* The container runtimes were logged using the creation and stop timings of the subprocess created when starting the container.
* *Script timings:*The runtime of the Python program being executed within the container was logged.

Additionally, CPU, memory and swap memory usage were monitored during the experiment using htop.

### Results

### Discussion

# Memory experiments

The memory experiments were designed to examine how memory intensive tasks in containerized environments perform. The Following tests were done:

1. Measuring the overhead caused by a single container.
2. Determining the influence of swap memory on a single container.
3. Determining the influence of the OOM killer on containers.

Unlike the CPU experiments there is no option to isolate a memory core. In addition to the experiments minimal OS processes were running consistently in the background across all experiments.

## Experiment M1: Overhead single container

The goal of the first memory experiment was to determine the overhead caused by a single container on the memory usage.

### Hypothesis

Containerized applications introduce additional memory usage compared to running a program natively (Ferraz, 2022). Each container has its own isolated user space that duplicates resources that could be shared in a single native environment (Duffy, 2014).

*When running an application natively compared to containerized, an observable runtime difference is expected due to the overhead caused by the isolated environment.*

### Method

The three different memory intensive Python scripts were used to perform the tests for the control experiment and the actual experiment.

* *Native execution (control)*: The Python programs were performed natively to determine the baseline performance.
* *Container execution*: The Python scripts were executed using the base container image described above.

Each test was performed 10 times to ensure viability was considered.

**Collected data**

The metrics collected during this experiment were the total execution time of the container and the total execution time of the Python program. Additionally, the memory usage was logged every 0.1 second.

### Results

The data mentioned above was collected using the three varying memory intensive Python programs. The tests were done according to the methodology described previously.

#### Time results

The average results based on the time measurements are shown in table … . The tests were performed 10 times to account for variability. Looking at the raw results (appendix … ) this the medium intensity program shows two outliers in both the container and program runtime. These were removed for the calculated average results shown in the table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Program** | **Control (s)** | **Container program time (s)** | **Container total time (s)** |
| *Simple* | 0.25 | 0.35 | 5.97 |
| *Medium* | 0.54 | 2.43 | 12.43 |
| *Long* | 24.85 | 29.48 | 43.86 |

Based on the results described in the table the bar charts … were created. Each graph shows the control and program runtime (in blue) and the added container surplus time (in orange).

To calculate the average runtime two outliers were removed from the medium experiment to ensure consistency.

A graph with a bar and a number of blue and orange bars

AI-generated content may be incorrect.**Low Memory load**

Looking at the lowest intensity memory script, the control took 0.25s on average. The program runtime increased when executed within a container by 0.35s (40% increase). When comparing the total execution time (5.97s) to the control (0.25s) the container took almost 24x longer to execute (~2300% increase).

A graph with blue and orange bars

AI-generated content may be incorrect.**Medium Memory Load**

At medium load the control test took 0.54s. The program being executed within the container averaged at 2.43 seconds showing an increase of ~350%. Looking at the total container runtime the average runtime increased to 12.43s, resulting in a ~1200% increase compared to the control scenario.

A graph of a number of people

AI-generated content may be incorrect.**Heavy Memory Load**

For the heaviest memory operation, the control experiment took 24.85 s. Looking at the program runtime within the container, execution took 29.48s (increase of ~19%). The total runtime of both the container and the executed program was 43.86s (increase of ~77%).

#### Memory results

In addition to runtimes the memory over time was measured. Every 0.1s memory used by the process was logged. The raw results can be found in the appendix. Figures …, … and … show the average memory used (10 iterations), measured at each 0.1s interval for the varying intensity programs. In addition, the graph shows the fluctuations per datapoint based on the standard deviation.

The total runtime for the low and medium experiments was

**Low Memory load**

Upon examining the graph shown in Figure …, a clear linear relationship with minimal deviation is observed for the control experiment. The maximum speed achieved during the control experiment was slightly below 120 MB.

In contrast, the actual test had a longer total duration (5.97s), resulting in a greater number of data measurements. Similar to the control experiment, the data shows a linear increase up to 0.2 seconds. Beyond this point, only a slight increase is observed. The maximum speed achieved by the program within the container was slightly above **A graph of a line and a line

AI-generated content may be incorrect.**110 MB.

**Medium Memory load**

As illustrated in figure …, the memory usage in the control experiment initially increases rapidly, reaching a peak at just over 200 MB after ~0.4s. After this point the memory usage remains constant. Over the course of time axis the memory fluctuation remains minimal.

In comparison, the test executed within the container displays a more irregular pattern. Memory usage increases quickly within the first 0.5s but afterwards a fluctuating plateau can be observed. After ~2.0 seconds the memory usage starts to decline, plateauing again around 2.8s. In addition to the differing memory usage the fluctuations are demonstrated to be significantly indicated by the broad standard deviation band.

**A screenshot of a graph

AI-generated content may be incorrect.**

**Heavy Memory Load**

Figure ... reveals that in the control experiment shows a similar increase in memory usage over the first few measurements. Afterwards it stabilizes around ~250MB. The plateau remains relatively stable, decreasing slightly, until approximately 21s. At this point a steep decline occurs.

In contrast the test conducted inside the container shows greater variability throughout the runtime. Similar to the control experiment, the actual test mirrors the first rapid increase in memory. In contrast the test stabilizes more slowly and has larger fluctuations throughout the middle of the test. Compared to the control experiment the memory decrease starts later than the control experiment at 26s.

When comparing the fluctuations between the control and the actual experiment the control remains relatively stable until ~21s. The same goes for the actual test, but instead the fluctuations become more frequent at ~17s instead.

A graph of a graph showing a number of different colored lines

AI-generated content may be incorrect.

#### Summary

The results demonstrate a clear trend in both execution time and memory behavior as the memory intensity of the scripts increases.

For all intensity levels, running the programs within a container resulted in increased total runtime compared to native execution. The overhead introduced by the container was most pronounced in the low and medium memory load tests, with runtime increases of approximately 2300% and 1200%. At the highest memory load, the container added a more modest 77% increase in total runtime.

Memory usage patterns also varied between control and containerized executions. In the control tests, memory usage followed predictable trends: a rapid increase followed by a stable plateau and, in the high-intensity case, a sharp drop near completion. In contrast, the containerized runs exhibited more fluctuation and variability across all memory loads, with broader standard deviation bands and less stable plateaus.

### Discussion

In this subchapter the results are discussed and compared to the predictions made in the hypothesis. The hypothesis stated that running an application in a container would introduce overhead compared to native execution due to the isolation mechanisms of the container. Looking at the results, the hypothesis is largely supported by the findings. Across all three intensity scenarios containerized execution resulted in an increase in total runtime and greater memory fluctuations.

**Outliers**

Each program was performed 10 times for each intensity test. The medium intensity test showed two big outliers in the data. These were removed to ensure consistency for both the timing logs and the usage logs (see results). The outliers could have many causes. Even with removed outliers the results of the medium intensity experiment still show great variability and are likely caused by the container. Especially because the natively executed programs showed much more stable results. Additional research is required to determine a more exact cause.

**Program runtime**

When comparing the program runtime of the natively executed program to the containerized execution a noticeable increase can be observed. The medium intensity script had the highest increase in program runtime, at 350%, while the increase was 40% for the low and 18% for the highest intensity test.

Based on the observations the hypothesis runs true when looking at just the program runtimes, because of the increased runtime.

**Total runtime**

Looking at the total runtime (container runtime) a striking increase (almost 2300%) was observed for the lowest intensity Python script. The medium intensity script showed an almost 1200% increase. These results suggest that especially for shorter programs container processes add significant overhead. For the higher workload test the relative overhead was less at roughly 77%. This is still a significant increase but less compared to shorter memory intensive programs. These results support the hypothesis.

**Memory usage**

When looking at the memory usage over time all experiments showed a large increase in memory upon startup of the program. Once a memory plateau was reached the memory usage stayed relatively consistent across all experiments, until the program was finished.

Only the most intensive test showed a rapid decrease in memory usage nearing the end of the program runtime.

# Waarom wel bij de intense een drop en niet bij de simple en mid?

Comparing the containerized application to the natively executed program showed a much larger variability and instability for the test results, especially for the medium and high intensity scenarios. This increased fluctuation is in line with the hypothesis saying that overhead is likely caused by containers having their own isolated user space (Duffy, 2014).

**Unpredictability**

This research focusses on real-time embedded systems. In the context of this research the unpredictability of the memory fluctuations can undermine the timing guarantees required in real-time embedded systems. When planning to use containers in real-time embedded systems the causes of the fluctuations need to be researched further.

The hypothesis states that containers do cause overhead in the memory domain. Eventhough it is likely that the overhead is caused by the containers additional research needs to be performed to determine which parts of the containers causes the fluctuations.

The following research is suggested:

* Research the predefined memory settings in the cgroups and their influence on the memory being used by the program.
* It is recommended to measure the memory, not just being used by the program, but also by the container itself to ensure the results.

## Experiment M2: Influence swap memory on containers

The aim of this experiment was to determine the influence of swap memory on the container and is a follow-up experiment to M1.

### Hypothesis

Swap memory is a portion of the storage memory (SD card on Raspberry Pi) that is used to extend the available memory by acting as temporary virtual memory. When the RAM runs out of physical memory, inactive areas in the RAM are moved to the swap space to create space for active processes. Swap is significantly slower because it relies on the speed of the storage device, which is generally a lot slower.

*With swap-memory disabled, containers will crash sooner, but maintain higher performance until they crash.*

### Method

To determine how swap memory impacts the performance it was important to reach the hardware limits of the Raspberry Pi Zero 2W. For this experiment only the most intensive Python program was used.

* *Swap memory enabled (control)*: The swap memory was enabled at the default value of 512MB.
* *Swap memory disabled*: The swap memory was disabled during the runtime of the experiment (experiment\_instructions.md).

After crashing log data was gathered using rsyslog.

**Collected data**

For this experiment both the program runtime and container runtime were logged. The memory being used was logged every 0.1 seconds. Additionally using htop the swap memory was monitored.

### Results

#### Time results

The program time and container time for the control experiment and the actual test are shown in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Program** | **Container program time Control (s)** | **Container total time Control (s)** | **Container program time Test (s)** | **Container total time Test (s)** |
| *Simple* | 0.41 | 4.53 | 0.29 | 10.01 |
| *Medium* | 5.40 | 16.94 | Crash | Crash |
| *Long* | 30.21 | 44.12 | ? | ? |

**Medium memory load**

When executing the medium intensity program the Pi instantly cashed after starting the program with swap memory disabled. The Pi was very hot directly after crashing and the light started blinking consistently in ~0.5 second intervals.

When running the long experiment the following error message shows: ‘Unable to allocate 436 MiB fir ab array with shape (11000, 5200) and datatype float 64.

#### Usage results

In addition to the time measurements the memory usage was measured every 0.1 seconds. Figures … were created to illustrate the average memory usage. The raw results can be found in the appendix.

### Discussion

**Memory medium crash**

After the crash the logs were observed using various log commands (experiment\_instructions.md). The log results didn’t show indication of crashes caused by OOM, kernel panic, overheating, segmentation faults or thermal throttling.

This could indicate a hard crash. When true, the kernel likely froze or panicked. As a result, the system couldn’t write to the disk to log the results when the system crashed.

These kinds of crashes can likely be captured using a watchdog. To determine the exact cause of the crash additional logging is required.

## Experiment M3: Influence OOM killer on Container

The goal of this experiment is to determine the influence of the OOM killer on containers.

### Hypothesis

When a Linux system runs out of memory the default behavior is for the OOM (out-of-memory) killer to terminate one or more processes to free memory. The amount of memory a container can use can be limited using cgroups. When the limit is exceeded the OOM killer kills the process.

*When limiting the amount of memory the container can use the OOM killer will kill the container process instead of resulting in a system crash.*

### Method

# Dit experiment moet eigenlijk ook worden aangepast. Wil eigenlijk juist weten of de limieten te zetten zijn voor de container en dat OOM het process dan juist killt.

**Collected data**

The data collected during this experiment were the container runtime and the program runtime. In addition, the memory being used by the Python program was measured for both the control and the actual experiment.

### Results

### Discussion

# I/O Experiments

The I/O experiments were used to map the influence of containers on I/O operations. To determine the reading and writing performance in containerization the following experiments were designed:

1. Determining the writing performance of a single container compared to native execution.
2. Determining the reading performance of a single container compared to native execution.
3. Reading multiple files.

The experiments were performed using a … USB. The device was a USB 2.0 device with a theoretical reading and writing speed of … .

## Experiment I1: Writing I/O performance single container

Experiment I1 focused on the performance of writing data to an external USB storage device from within a container. The performance difference between writing data natively compared to writing within a container was measured.

### Hypothesis

Docker on Linux used the Union File System (OverlayFS) for container storage (Heinz, 2021). Write operations go through a copy-on-write layer. The first time the container writes a file that originates from the read-only layer, the file system needs to copy the file to the writable layer first (*OverlayFS Storage Driver*, 2025). This might cause notable overhead.

*Writing a file natively to an external I/O medium will take notably less time than writing the same file from within a container.*

### Method

To determine the writing performance three different intensity Python programs were used. Each program writes a different amount of generated data to a file (created on the USB).

Using the programs the following tests were performed:

* *Writing native (control):* The data generated by the varying Python programs was written to the USB using the native tools.
* *Writing within container*: The Python programs were executed from within the container writing the generated output the USB from within the container.

**Collected data**

The data collected during this experiment consists of the reading and writing speed to and from the USB device. The read and write speeds were monitored every 0.1 seconds. In addition, the program runtime and container time were logged.

### Results

For this experiment data was written to the USB using the three different intensity Python scripts.

#### Time results

The average program runtimes and container runtime measured are shown in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Program** | **Control (s)** | **Container program time (s)** | **Container total time (s)** |
| *Simple* |  |  |  |
| *Medium* |  |  |  |
| *Long* |  |  |  |

### Discussion

## Experiment I2: Reading I/O performance single container

The goal of this test was to measure the performance difference of reading a file from an external I/O device natively compared to running it from within a container.

### Hypothesis

The performance of reading data from within a container is much closer to reading the data natively. If the file is not modified by the container the file is read form the lower read-only layer, that can be shared and doesn’t need to be copied for every container instance (LearnCantrill, 2023).

*Reading from within a container will not cause much overhead compared to reading a file natively, because read only layers are not copied to the container exclusive space.*

### Method

This experiment focused on reading one file. The file that was used for both the control and the actual experiment was a 1GB binary file. The file was stored on the USB.

* *Reading native (control):* The file on the USB stick was read using natively by the Raspberry Pi to determine the reading speed.
* *Reading within container:* The file on the USB device was read from within the container.

**Collected data**

Similar to the experiment above the reading and writing speeds of the I/O device were measured and the container runtime and program runtime were logged.

### Results

### Discussion

## Experiment I3: Reading multiple files

The goal of this experiment was to determine the performance difference between reading one file and multiple files from within a container and natively.

### Hypothesis

Handling small files tends to be slower than one larger file of the same size. Each file read incurs opening the file, reading its metadata, updating access times and finally reading the file itself.

# Nog even kijken hoe ik dit wil doen: nu vergelijk ik meerdere files tov 1 file binnen de container context maar niks native.

# Conclusion

# Recommendations

The discussion leaves many possibilities for follow-up research. This chapter discusses the suggested tests to determine what caused the unexpected experimental results. In addition, a general plan for a follow up research project was created in this chapter.

# Justification of choices

## Experiment hardware

To successfully complete the experiments, selecting the appropriate hardware is necessary. The choice of hardware depends on the scope and requirements of the project. By comparing the different options available within the defined scope, the right hardware can be selected.

#### Scope

Due to time constraints, choosing the hardware for the experiment will be limited to the Raspberry Pi range (see chapter on demarcation). The Raspberry Pi series consist of four primary models: Flagship series, Zero series, Compute Model series and Pico microcontrollers (Contino Nate, 2024).

#### Requirements

***Must haves:***

* ***Support Linux OS version*:** As clarified in the demarcation chapter, this project will exclusively focus on Linux OS containers. Therefore, the selected container must support Linux OS versions.
* ***Availability*:** The controller needs to be available within 4 weeks after ordering to be able to meet upcoming deadlines.
* ***Budget***: The project has a maximum budget of €500. While it is unlikely that the hardware will exceed this limit within the Raspberry Pi range, the controller cannot exceed the limit. Als long as the controller is priced below €500 the price will not impact the final decision.

***Deciding factor:***

* ***Limited resources***: The experiment aims to test the limits of containers on the selected controller. If the hardware is too powerful, it could prolong the process and complicate reaching the limits of container performance. Selecting a controller with limited resources is important.

#### Comparison

Based on the scope and requirements, the four main Raspberry Pi models are compared. Due to time constraints only the newest model in each series will be considered. The table below provides an overview of the key specifications, including pricing and availability as of March 2025. Pricing is an estimate based on various suppliers.

Table 3 Comparison table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Flagship (5) | Zero (2 W) | Compute module (4) | Pico (2) |
| Linux OS support | Yes | Yes | Yes | No |
| Availability | < 1 week | < 1 week | < 1 week | < 1 week |
| Budget | €100, - | €20, - | €45, - | €9, - |
| RAM | 2GB, 4GB, 8GB | 512 MB | 1GB, 2GB, 4GB, 8GB | 520KB |
| CPU | Quad core 2.4 Ghz | Quad core 1.0 Ghz | Quad core 1.5 Ghz | Dual core 150 Mhz |

#### Choosing hardware

Based on the comparison, three models meet the essential requirements of supporting Linux OS, budget and availability. Only the Raspberry Pi Pico 2 is not able to meet the criteria as it does not support a Linux operating system.

This leaves three suitable options: the Raspberry Pi 5, the Raspberry Pi Zero W and the Raspberry Pi Compute 4.

After evaluating these models, the **Raspberry Pi Zero 2 W** emerges as the most fitting choice. While it has the least powerful hardware, the key factor is the project’s focus on limited resources.

## Operating system

To be able to use the Raspberry Pi Zero 2 W it is required to install an operating system. Raspberry Pi provides different alternatives. Since the Raspberry Pi Zero 2 W is equipped with a 64-bit processor downloading a 64-bit OS is recommended. Raspberry Pi offers 3 different 64-bit versions(Raspberry Pi, z.d.-a):

* Raspberry Pi OS with desktop
* Raspberry Pi OS with desktop and recommended software
* Raspberry Pi OS Lite

When comparing these OS versions, the biggest difference is that the Lite OS doesn’t include the desktop environment. It is the most basic OS version only including a text only console (klricks, 2022).

## Scripting software

To create the scripts running in the container a scripting language had to be chosen. One of the main requirements of this project was that it would be easily understandable and repeatable by colleagues. Even though a language like C++ generally offers better performance, Python remains the more accessible language. Therefore, the use of Python was preferred over other languages.

## Container engine

To create, manage and run containers a container engine had to be decided on. Even though there are many different services providing container engines, Docker is the most widely used. As a result, there is a lot of documentation available.

One of the main requirements of this project is accessibility and reproducibility. For this reason, Docker was chosen for this project due to Dockers popularity and the availability of documentation.

## I/O device

To test the influence of containers on I/O reading and writing speed, an I/O device had to be selected for the experiments.

One of the requirements was that the I/O device used for the experiments had to be separate from the I/O device used for the OS. This was necessary to make sure the OS processes did not interfere with the I/O reading and writing performance.

The Raspberry Pi Zero 2 W has a USB port. For ease of use and costs a USB stick was chosen for these experiments. The Philips FM64FD18OB was most accessible and therefore used for this purpose.

# Description of realized professional products

# Evaluation of quality criteria

# Process evaluation

# References

AltexSoft. (2022, 14 december). The good and the bad of docker containers. *AltexSoft*. https://www.altexsoft.com/blog/docker-pros-and-cons/

Appeti, Y. W. (2023, 24 augustus). Docker: Union File System. *Medium*. https://medium.com/@yao.wateba/docker-union-file-system-e3cce523137b

Arges, C. (2020, 17 december). *Navigating Containers in the Linux Kernel*. Confluera. https://www.confluera.com/post/navigating-containers-in-the-linux-kernel

ARMO. (2024, 19 december). *Linux Kernel*. https://www.armosec.io/glossary/linux-kernel/

Balaban, D. (2024, 21 juni). *The Pros and Cons of Containerization in 2024*. https://www.networkcomputing.com/network-infrastructure/the-pros-and-cons-of-containerization-in-2024

Barron, B. (2023, 21 november). *The pros and cons of using containers in web development*. Verpex. https://verpex.com/blog/website-tips/the-pros-and-cons-of-using-containers-in-web-development

Bodet, J.-C. (2023, 24 augustus). *Good News for Embedded: Containers Now Available for 32-Bit Edge Devices*. NXP Semiconductors. https://www.nxp.com/company/about-nxp/smarter-world-blog/BL-GOOD-NEWS-FOR-EMBEDDED

Boutnaru, S., PhD. (2023, 11 januari). Linux — namespaces: IPC namespace. *Medium*. https://medium.com/@boutnaru/linux-namespaces-ipc-namespace-927f01cbcf3d

Capgemini. (2023, 16 november). *Sectoren*. https://www.capgemini.com/nl-nl/sectoren/

Capgemini Engineering. (z.d.). *Intro part 1 2025 - General Divisions*.

Capgemini Engineering. (2024, 17 september). *Pioneering new horizons with Capgemini Engineering*. Capgemini. https://www.capgemini.com/us-en/about-us/who-we-are/our-brands/capgemini-engineering/

Carrigan, T. (2023, 12 januari). Linux Command Basics: 7 commands for process management. *Red Hat Blog*. https://www.redhat.com/en/blog/linux-command-basics-7-commands-process-management

Contino Nate. (2024, 30 oktober). *Raspberry Pi product series explained*. Raspberry Pi. https://www.raspberrypi.com/news/raspberry-pi-product-series-explained/

Datadog. (z.d.). *The IPC namespace on the host should remain isolated from containers*. https://docs.datadoghq.com/security/default\_rules/cis-docker-1.2.0-5.16/

Duffy, C. (2014, 26 september). *What is the runtime performance cost of a Docker container?* https://stackoverflow.com/questions/21889053/what-is-the-runtime-performance-cost-of-a-docker-container

DuploCloud. (2023, 4 december). Docker Advantages and Disadvantages: What you need to know before you switch. *DuploCloud*. https://duplocloud.com/blog/docker-advantages-and-disadvantages/

Ehrman, N. (2024, 20 juli). *What is a Container Engine?* wiz.io. https://www.wiz.io/academy/container-engine

Ferraz, L. (2022, 13 december). *Performance Impact of Docker Containers on Linux*. Torizon. https://www.torizon.io/blog/containers-in-linux-and-performance-impact#:~:text=The%20key%20difference%20between%20those,relevant%20variables%20are%20correctly%20controlled

Fidus. (2024, 28 november). *Real-Time Operating Systems: Design and Implementation for Critical Applications*. Fidus Systems. https://fidus.com/blog/real-time-operating-systems-design-and-implementation-for-critical-applications/

Gaurav Gahlot. (2021, 2 augustus). *Kernel Internals | namespaces | cgroups | Containers | Docker* [Video]. YouTube. https://www.youtube.com/watch?v=-I2PnsyUou4

GeeksforGeeks. (2022a, november 9). *Embedded realtime system*. GeeksforGeeks. https://www.geeksforgeeks.org/embedded-real-time-system/

GeeksforGeeks. (2022b, december 7). *Processes in Linux/Unix*. GeeksforGeeks. https://www.geeksforgeeks.org/processes-in-linuxunix/

GeeksforGeeks. (2024, 20 september). *Difference Between Hard Real Time and Soft Real Time System*. https://www.geeksforgeeks.org/difference-between-hard-real-time-and-soft-real-time-system/

GeeksforGeeks. (2025, 24 januari). *Kernel in operating system*. GeeksforGeeks. https://www.geeksforgeeks.org/kernel-in-operating-system/

Gökmen, B., & Azar, J. (2024, 12 mei). *Why is it recommended to run one process per container?* Baeldung. https://www.baeldung.com/ops/one-process-per-container

Heinz, M. (2021, 1 maart). *Deep Dive into Docker Internals - Union Filesystem*. Martin Heinz | Personal Website & Blog. https://martinheinz.dev/blog/44

Johnston, S. (2024, 16 juli). 11 Years of Docker: Shaping the Next Decade of Development | Docker. *Docker*. https://www.docker.com/blog/docker-11-year-anniversary/

klricks. (2022, 3 september). *Difference between the Raspberry Pi OS images*. Raspberry Pi. https://forums.raspberrypi.com/viewtopic.php?t=339721

Knoldus Inc. (2019, 13 maart). UnionFS : A File System of a Container. *Medium*. https://medium.com/@knoldus/unionfs-a-file-system-of-a-container-2136cd11a779

Kuninoto. (2024, 24 mei). How does Docker really work under the hood? — A dive into Docker’s internals. *Medium*. https://medium.com/@kuninoto/how-does-docker-really-work-under-the-hood-a-dive-into-dockers-internals-2fef63f7c9bb

LearnCantrill. (2023, 25 januari). *Free Docker Fundamentals Course - Docker Storage - Writable Layer, Bind Mounts & Volumes* [Video]. YouTube. https://www.youtube.com/watch?v=OAeVsjwRVe8

McCune, R. (2023a, april 17). *Container security fundamentals part 3: Capabilities*. https://securitylabs.datadoghq.com/articles/container-security-fundamentals-part-3/

McCune, R. (2023b, september 11). *Container security fundamentals part 6: seccomp*. https://securitylabs.datadoghq.com/articles/container-security-fundamentals-part-6/

Morabito, R. (2016). A Performance Evaluation of COntainer Technologies on Internet of Things Devices. In *Arxiv*. Erricson Research. https://arxiv.org/pdf/1603.02955

Mortensen, P. (2009, 17 oktober). *What do the terms “CPU bound” and “I/O bound” mean?* Stack Overflow. https://stackoverflow.com/questions/868568/what-do-the-terms-cpu-bound-and-i-o-bound-mean

Mullinix, S., Konomi, E., Townsend, R. D., & Parizi, R. (z.d.). *On Security Measures for Containerized Applications Imaged with Docker* [Kennesaw State University]. https://arxiv.org/pdf/2008.04814#:~:text=By%20allocating%20a%20dedicated%20namespace,be%20assigned%20a%20limited%20number

*OverlayFS storage driver*. (2025, 28 februari). Docker Documentation. https://docs.docker.com/engine/storage/drivers/overlayfs-driver/#:~:text=,for%20the%20first%20time

PowerCert Animated Videos. (2022, 28 december). *Virtual Machines vs Containers* [Video]. YouTube. https://www.youtube.com/watch?v=eyNBf1sqdBQ

Raspberry Pi. (z.d.-a). *Operating system images*. https://www.raspberrypi.com/software/operating-systems/

Raspberry Pi. (z.d.-b). *Raspberry Pi Connect (Beta)*. https://www.raspberrypi.com/documentation/services/connect.html

Red Hat Inc. (z.d.). *Chapter 15. Managing Out of Memory states*. Red Hat Documentation. https://docs.redhat.com/en/documentation/red\_hat\_enterprise\_linux\_for\_real\_time/8/html/optimizing\_rhel\_8\_for\_real\_time\_for\_low\_latency\_operation/assembly\_managing-out-of-memory-states\_optimizing-rhel8-for-real-time-for-low-latency-operation#assembly\_managing-out-of-memory-states\_optimizing-RHEL8-for-real-time-for-low-latency-operation

RTOS LOGICS. (2020, 16 november). *What is the need of an RTOS in an Embedded System* [Video]. YouTube. https://www.youtube.com/watch?v=ZJ8rtkMoxFI

Srinivas. (2021, 16 maart). *Securing Docker Containers with Linux Kernel Features*. https://www.infosecinstitute.com/resources/general-security/how-docker-primitives-secure-container-environments/

Sroor, M., Das, T., Mohanani, R., & Mikkonen, T. (2024). A Systematic Mapping Study on Software Containers Risks and Vulnerabilities. *SSRN*. https://doi.org/10.2139/ssrn.4741002

Stichting HBO-i, Crasborn Communicatie Vormgevers, Epping, L., Giesen, M., Groot, P. D., Kleijn, J. van D., Linsen, B., Reus, M. D., Rijsenbrij, K., Roosen, F., Schreurs, F., Viersen, R. V., Wijden, P. van D., Willemsen, R., & Wollenweber, M. (2023). HBO-I domeinbeschrijving. In M. Valkenburg (Red.), *Stichting HBO-i*. Stichting HBO-i. https://www.hbo-i.nl/wp-content/uploads/2024/02/24040\_HBOi\_Domeinbeschrijving\_NL.pdf

Swaen, B. (2024, 15 juli). *Soorten onderzoeksvragen perfect formuleren (met voorbeelden)*. Scribbr. https://www.scribbr.nl/starten-met-je-scriptie/type-onderzoeksvragen/

TechSquidTV. (2018, 19 augustus). *What is Docker in 5 minutes* [Video]. YouTube. https://www.youtube.com/watch?v=\_dfLOzuIg2o

Tiwari, A. (2024, 17 december). What Containers Really Are: Understanding Namespaces, cgroups, and Linux Kernel Features. *Medium*. https://medium.com/%40princetiwari97940/what-containers-really-are-understanding-namespaces-cgroups-and-linux-kernel-features-de4dc71ed63c

Van Kalken, S. (2021, 21 juli). *What Are Namespaces and cgroups, and How Do They Work?* https://blog.nginx.org/blog/what-are-namespaces-cgroups-how-do-they-work

Wind River Systems. (z.d.). *What are embedded containers*. Wind River. https://www.windriver.com/solutions/learning/embedded-containers

Windriver. (z.d.). *What is the difference between embedded containers and virtual machines?* Wind River. https://www.windriver.com/solutions/learning/difference-between-embedded-containers-virtual-machines

ZPiDer. (2018, 14 mei). *Multiple docker container performance*. Stack Overflow. https://stackoverflow.com/questions/50325454/multiple-docker-container-performance#:~:text=1

# Appendix

Experiment M1:

A graph of a memory usage

AI-generated content may be incorrect.

Long experiment all data.