BLOG POST

Virtualisation security design principles

How to design secure systems with virtual components

Stuart H

Our recently released Cyber security design principles can help when designing all manner of systems, from online digital services through to segregated cyber-physical systems. But what do you do if you have a more 'particular' set of requirements?

Sometimes, high level principles just don't provide the right level of detail. You may, for example, be designing a system which relies on a virtualised firewall, or virtual networking. How *exactly* do the principles apply to these technologies?

This is where the Virtualisation security design principles come into play. This new guidance extends the Cyber security design principles to focus on the high-level concepts of virtualisation.

Using the principles

Let's walk through an example to see how these virtualisation principles can be used when coming up with a (very) high-level design for a system using virtualisation.

One of the original requirements for the virtualisation principles came from the industrial process control community, who asked the question, *"How can I use virtualisation safely in an industrial control environment?"*

So, we'll come up with a design for a fictitious manufacturing company, who have an industrial control system (ICS). They're looking to consolidate infrastructure using virtualisation, without impacting on integrity or availability.

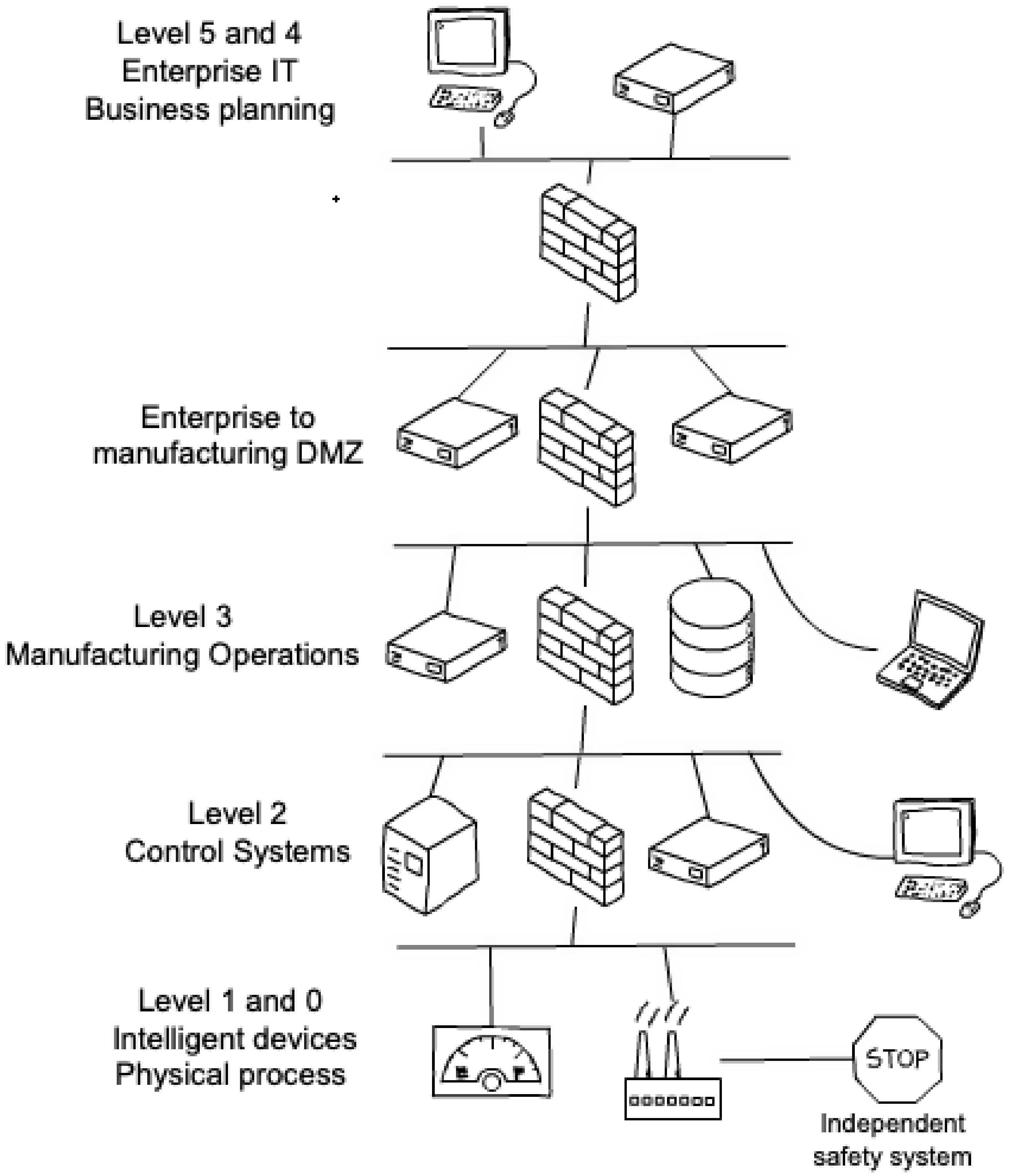
However, the top priority is that no aspect of system safety is compromised. This includes personnel in the workplace *and* any potential harm to the general public.

Establish the context

The first thing we need to do is establish the context of the system. This process is all about understanding what business operations the system will support, the risks it will face and the impact of its compromise.

In this case, we're dealing with a system used for industrial control. It currently has a traditional architecture, based on the Purdue model, with physically separate infrastructure between each level.

Traditional architecture



The aspiration is to consolidate as much of the ICS as possible. However, based on risk analysis and threat modelling, it has been decided that consolidation of the enterprise IT with the ICS would be too risky.

Consolidation of operations together with the control systems *is* suitable because *the risk profiles of all systems sharing the virtualisation platform will be a* *similar level.*

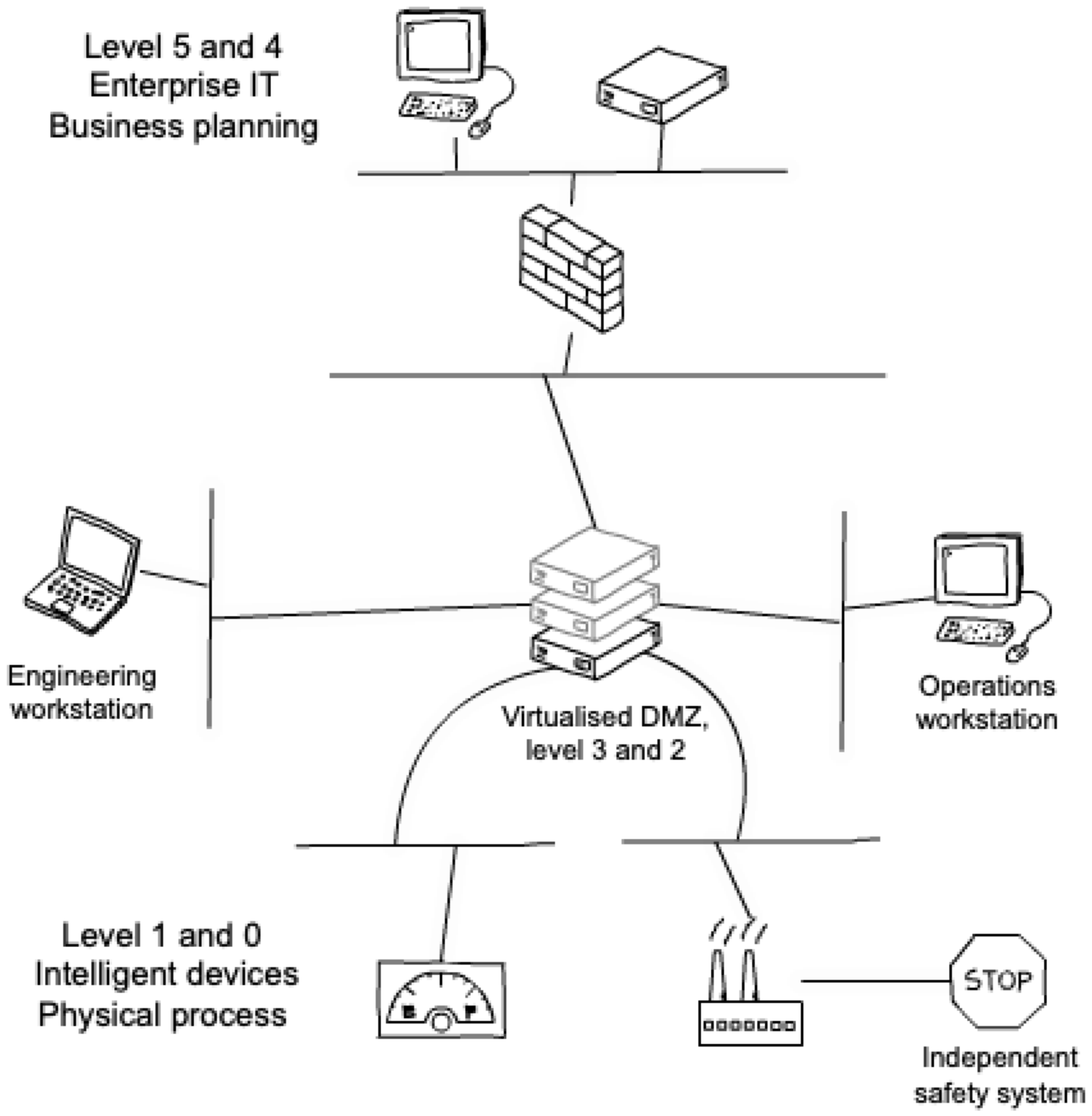
There are availability concerns about putting all components of the system on to one virtualisation platform, so the design needs to ensure it doesn't become a single point of failure.

Consolidated design with virtualisation

There is also a legacy system used to control machinery that is no longer supported and has known vulnerabilities. Unfortunately, this is tightly integrated into the system and prohibitively costly to replace.

The technical architects understand that virtualisation doesn't mitigate vulnerabilities in legacy systems. To manage this risk, they plan on using micro-segmentation. This is a technique whereby the workload of a system is divided into segments, based on security needs. Necessary controls are then applied on a per-segment basis.

The system architects take the business context and requirements and start to develop an architecture which consolidates the layers of the ICS, using virtualisation. They come up with the following high-level concept diagram.



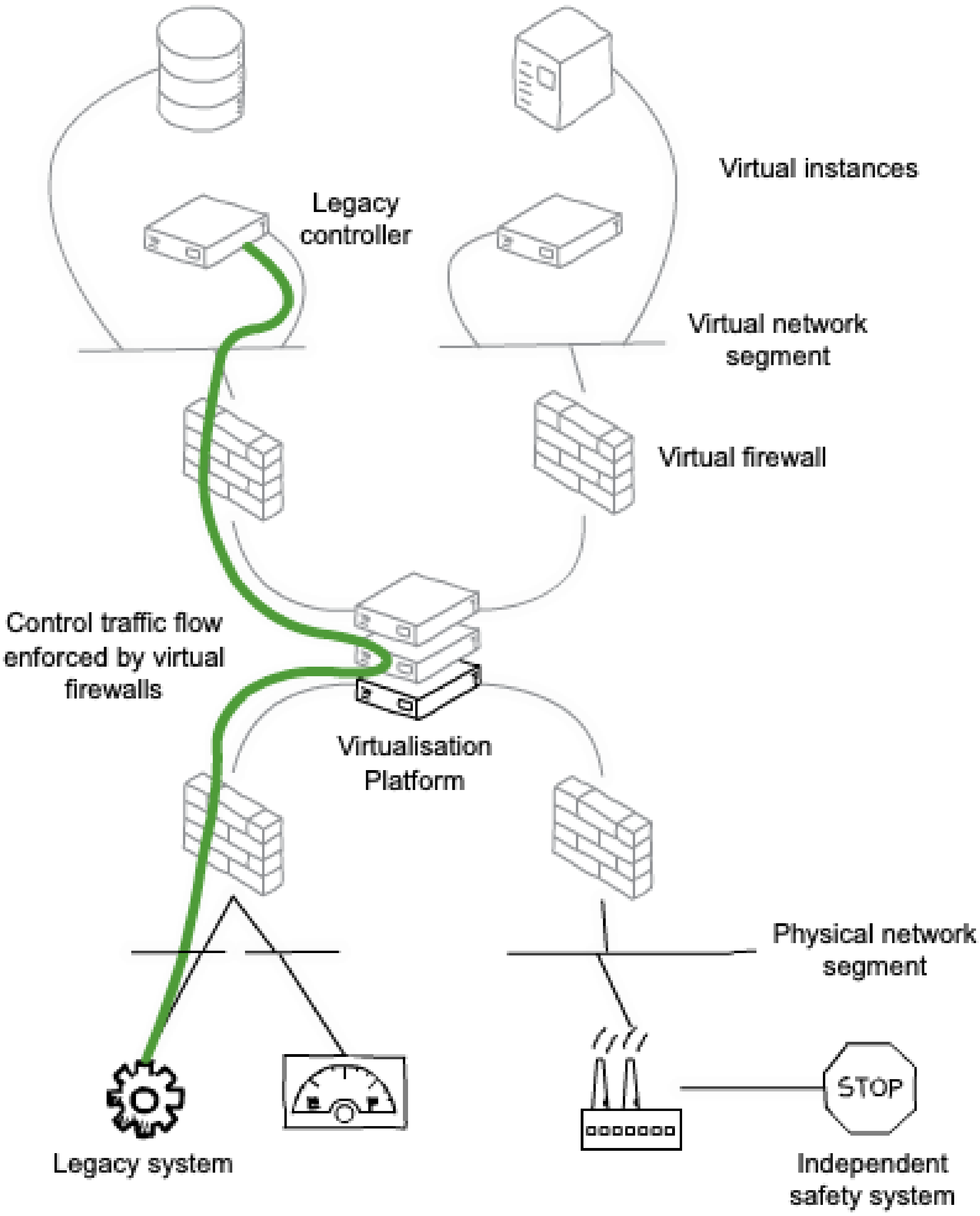
Make compromise difficult

Each layer of the virtualised system should be designed with security in mind. This will help to make compromise more difficult.

Securing legacy components using micro-segmentation

In our example, a legacy component needs to be used, but access to it must be tightly controlled. To achieve this, the design makes use of virtual networking and micro-segmentation. This also helps to ensure that virtual instances don't impact on one another, by helping to limit the lateral movement an attacker could make if they compromise the legacy component.

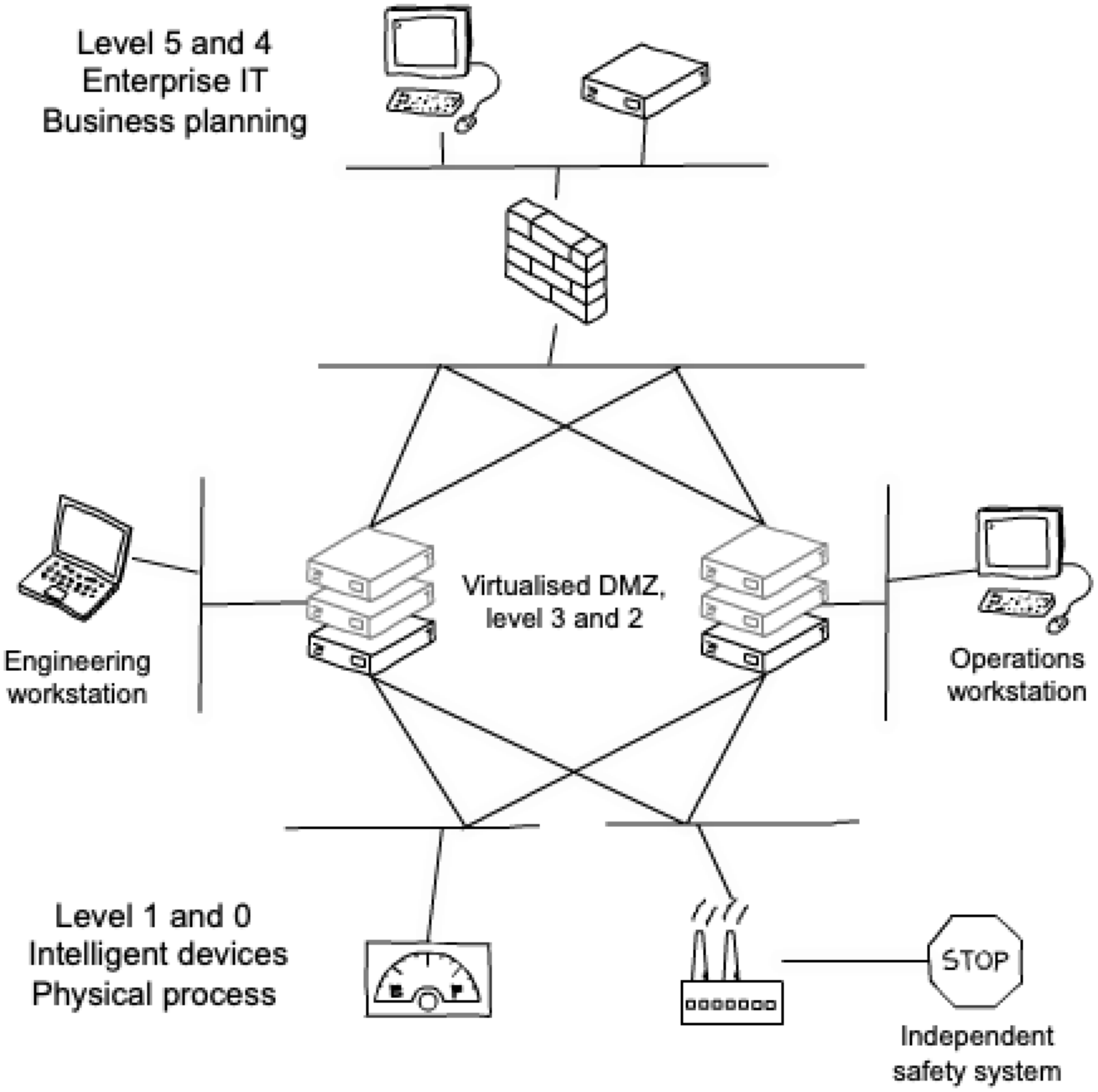
In our example we've used the virtual firewalls to enforce a network traffic flow from the legacy controller virtual instance to a physical network segment, used only for the legacy equipment.



Make disruption difficult

It's important for the manufacturing industry to maximise up-time. Virtualisation has a number of features which can help with this. However, care must be taken with these features as they can have a negative effect if used incorrectly.

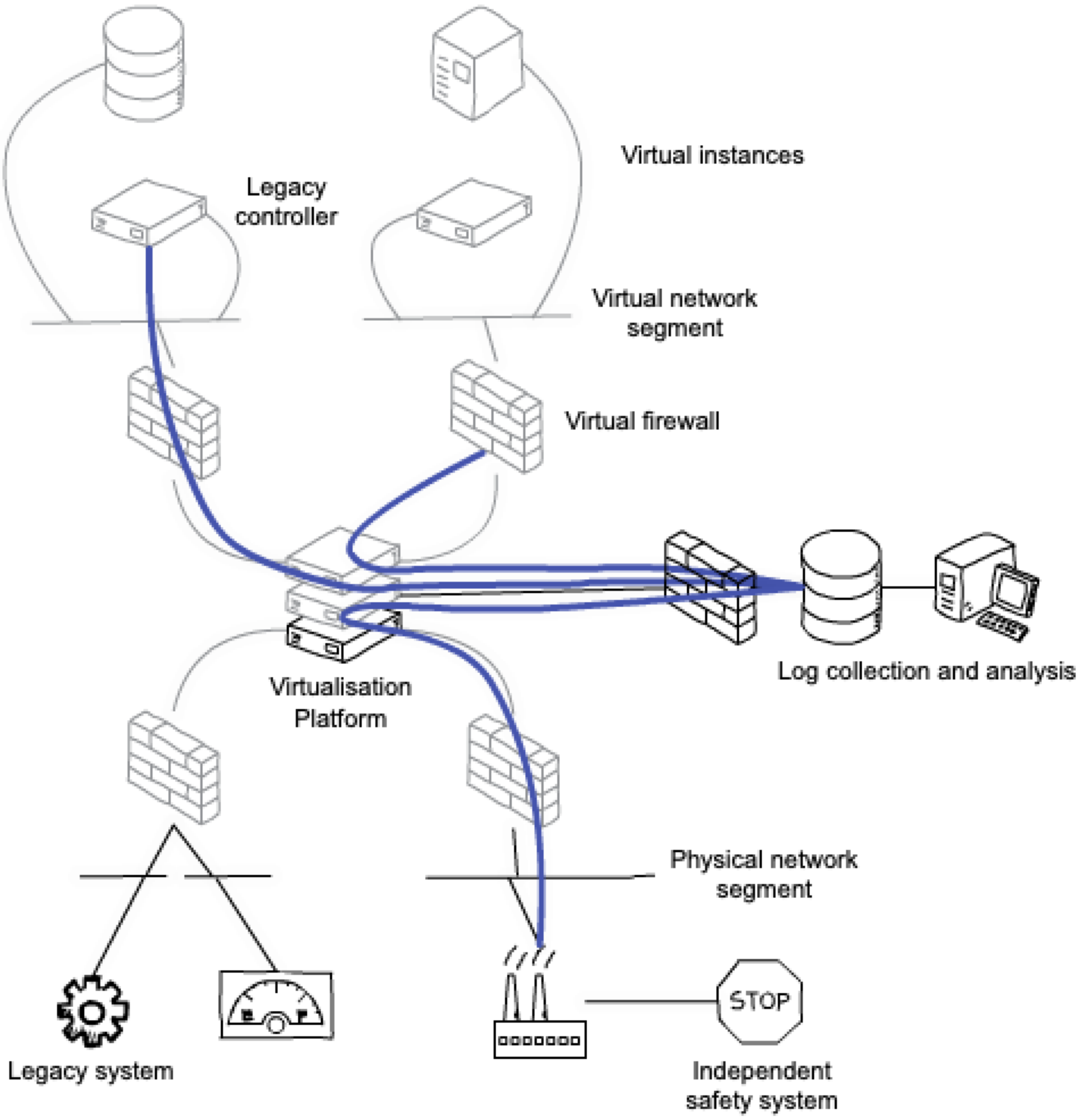
Our system design will incorporate features such as high-availability clustering and automated failover. These features have the added benefit of allowing the operations team to continually update virtual instances and virtualisation platforms while making disruption difficult.



Making compromise detection easier

Monitoring across all the layers of your architecture can be improved using virtualisation.

For example, using virtual networking to enable flexible network-level monitoring, sending system logs to collectors via dedicated virtual networks, enabling logs to be sent from each compartmentalised segment to a central log collection and analysis platform.



Performance monitoring of your system's virtual instances is easier too, as the virtualisation platform oversees their resource allocation. All of this helps to make compromise detection easier.

Minimise the impact of compromise

No matter how well you design a system you cannot be certain it will never be compromised. So, it’s a good idea to anticipate and be prepared for system compromise and failures.

You should put in place a response plan which makes it easy to recover and ultimately reduce the impact of compromise. Virtualisation can help with this too. Thanks to features already deployed for high availability, such as clustering and failover, snapshots and backups, you can rapidly restore a system using orchestration.

The design process

I hope going through this simple design process has shown how useful the Cyber security design principles are for building security into your systems.

The base principles bring consistency to the design, and review, of your systems. The Virtualisation security design principles extend this concept to address the specific set of problems and strengths faced by virtualised systems.

If you have any feedback on either set of principles, we’d be glad to hear from you.

Stuart H
Senior Security Architect

WRITTEN BY
Stuart H

PUBLISHED
7 August 2019

WRITTEN FOR ⓘ

Small & medium sized organisations

Public sector

Cyber security professionals

Large organisations