BUILDING A BETTER LAB SYSTEM: A NEW APPROACH TO ACHIEVE ACCURACY, AVAILABILITY AND SECURITY.

Honeywell

TABLE OF CONTENTS

ABSTRACT

1

Lab systems play a vital role in most industrial control settings. Systems replicating the operating environment without connecting to the live process provide a safe method to test changes or updates without risking disruption or safety.

They do, however, have their limitations. Three are critical.

The first is the difficulty in keeping the lab system current. Over time changes to the system or process will see differences between the lab system and live environment emerge. Failure to adjust for modifications, updates, upgrades and expansions will reduce the reliability and utility of the lab system: Its tests will only accurately illustrate the impact of changes on the live system if it accurately reflects that system. A digital twin of the operating environment needs to be an identical twin to be of use.

This gives rise to a further weakness, for it means that each new test requires a new lab system to be built, ensuring it accurately reflects the current operation. For smaller projects and testing of hotfixes or back-ups, the work and cost involved mean this is rarely practical. Such changes go untested.

AN OPEN AND SHUT CASE

2

There is a final, less discussed factor that decreases its utility, too: Lack of access. There is little use in a lab system if those that need it can't get to it. With dispersed operations, assets and people, that again can make lab testing impractical even where it may be possible.

One way around this weakness is to network the lab system in some way, which is what many plants do to allow users remote access. That can solve the problem of access, but it opens a can of worms regarding security. Such non-standard networks present a key area of vulnerability for operators, especially when the labs might run on earlier operating system versions or require exceptions for patches.

It is critical to be clear: The danger is not the lab system itself. By definition, the lab system should have no connection to the live process; it simply replicates the operating environment, effectively a simulation of the control system. However, such ad-hoc connectivity can provide malicious actors with a route in. To take an early example, it was the vulnerability of the retailer's network providing access to the heating, ventilation, and air conditioning systems that ultimately gave hackers access to Target's payment systems in 2013 – still one of the biggest security breaches in history.

In an environment where almost four in ten industrial control systems were targeted by malicious activity last year, operators face a difficult choice: Either run a completely un-networked and air-gapped lab system, there further limiting its utility to the business; or run the risk of networking it and potentially leaving themselves vulnerable to attacks.

There is, however, an alternative.

INTRODUCING HONEYWELL DIGITAL PRIME

3

Honeywell's Digital Prime was built to address all the challenges and weaknesses in traditional lab systems – including security.

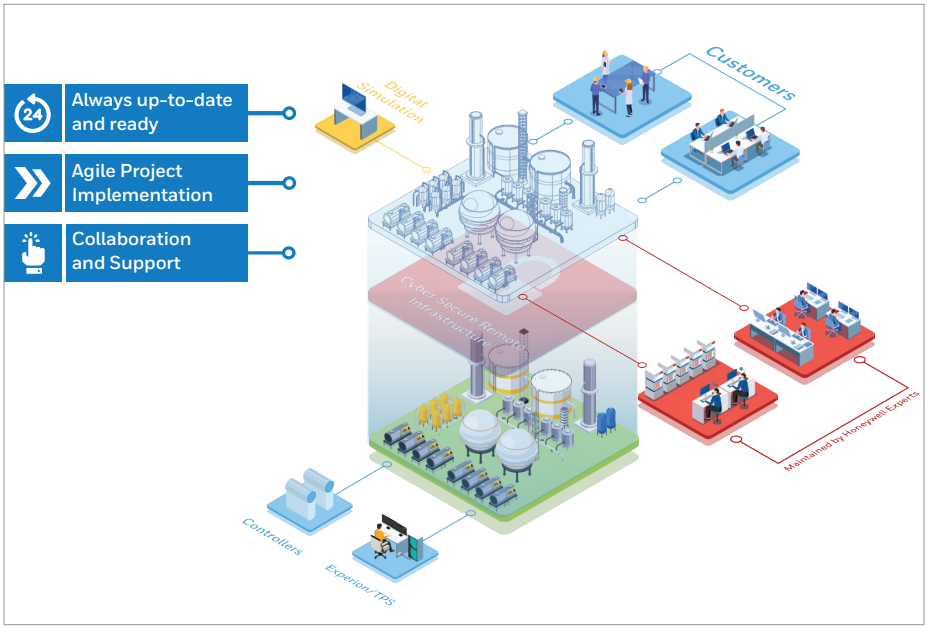
It provides a "lab system as a service" that is always available and consistently accurate. A subscription service, it is continually updated to reflect changes to the operating environment, providing a consistent digital twin. Because it's continuously maintained and hosted by Honeywell, it is always available for users to test even minor changes, patches, and upgrades.

It has a wide range of use cases:

- Functional reviews and impact analysis
- Remote FAT tests
- Training
- Documenting digital changes.

Its features include anomaly detection, automated change management, configuration compliance checks. For engineering and design, it helps eliminate the need for on-site reworks, ensure execution quality, simplify system documentation updates and provide a historical overview of the control changes. For project execution and testing, it centralizes planning and resource allocation and provides project visibility, improving collaboration, helping cut travel costs and time, reducing risks and ensuring compliance with detailed design specifications.

Apart from all this, it addresses the two fundamental weaknesses of traditional on-site lab systems: Their tendency to deviate from the current system setup and their impracticability for smaller systems. But it also resolves the central conflict such systems present regarding access and security.



A CENTRALIZED SOLUTION

4

The benefits of a hosted, software as a service (SaaS) solution for a lab system are two-fold. The first – accessibility – is inherent. A hosted solution provides access to authorised users across the enterprise where and when it's needed. Users have access to a consistent (and consistently updated) digital twin for their own use and to collaborate with others, regardless of their location.

The second is achieved through industry-leading levels of cyber security to give users complete confidence and control.

As with a traditional lab system, the digital twin provided by Honeywell's Digital Prime is entirely separate and independent of the actual control system. There is no communication between the two. But in addition to this, the solution also provides the highest standards of security.

First, VMware, which provides the service's infrastructure, is continually updated by Honeywell as the host. There's no need for users to maintain the system. Effectively centralizing the lab system solution, there's no need to update the virtual machines or apply patches. Users don't even need anti-malware protection; it is built into the VMware infrastructure itself rather than dependent on the virtual machine. The centralized approach doesn't just simplify the management of the solution for users; it also ensures this level of security is consistently maintained.

Moreover, each virtual machine is entirely logically separated. There are no network paths between different subscribers nor between the virtual machine and the customer's operating system. Access can be managed using multi-factor authentication – giving users complete oversight and control of who can connect and view the solution. Within Honeywell itself, access is controlled according to the strictest policies to exclude anyone outside IT staff necessary for the hosting environment's smooth operation.

To ensure these standards are maintained, Honeywell's SaaS platform is annually audited against ISO/IEC 27001 – the rigorous international standard on managing information security. This details the requirements for establishing, implementing, maintaining and continually improving an information security management system. Honeywell has held a current certification for each of the three years.

In addition, Honeywell carriers out dozens of initiatives and practices to ensure the highest levels of security. These include daily scans of the infrastructure to identify emerging security vulnerabilities; rigorous security analysis of any external suppliers; penetration testing in accordance with ISO requirements; and Commvault backups across the entire infrastructure.

SQUARING THE CIRCLE

5

Combining the best of a traditional lab system with the latest SaaS solutions for connectivity, Honeywell Digital Prime offers a solution that achieves the best of both worlds: Readily available access and tight security.

It also provides a cost-effective solution to address the traditional limitations of lab systems, allowing users to test more frequently and have greater confidence in the results. It provides a digital twin that is always current, always available, and always secure. Once the industry adopts such an approach, it will never go back.

For more information

Visit process.honeywell.com
or contact your Honeywell Account Manager.

Honeywell Process Solutions

2101 City West Blvd, Houston, Texas 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road
Zhangjiang Hi-Tech Industrial Park
Pudong New Area, Shanghai 201203

process.honeywell.com

WPR-22-13-EN | 09/22

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell