Executive Summary

Our industry is facing the challenge of ever increasing system complexity with large systems integrated and procured from multiple vendors and combinations of DCS, Safety, APC, PLC, Historians etc. The legacy systems are increasing with continuous need to migrate or expand. On one side, the desire to achieve best in class is continuously increasing whereas on other side, the industry has increasing pressure of aging workforce and high turnover. Today’s challenges in managing automation assets ranges from increasing integration and interoperability, inadequate documentation, loss of knowledge and critical skills, poor configuration integrity, lack of adequate change tracking and managing spare capacity. These challenges make it extremely important to implement and maintain the proper management of change. We would discuss this topic in-depth and provide recommendations on various available industrial solutions on how to manage this situation.
Table of Contents

The Impact of Change .......................................................................................................... 3

Management of Change .......................................................................................................... 3

Advantages of Effective MOC Across Plant Automation Assets .................................................. 4

Honeywell’s Management of Change Solution ..................................................................................... 4

How iMOC Works ................................................................................................................ ....................................................................... 5

A Scenario Where iMOC Matters ................................................................................................. ............................................................. 7

The iMOC Solution Enables Key Business Improvements .............................................................. 7

  Increased Safety and Compliance ............................................................................................... .......................................................... 7

  Reliability ..................................................................................................................................... 7

  Economic Benefits ..................................................................................................................... 7
The Impact of Change

Automation systems directly impact the safety, profitability, and environmental performance of industrial plants. They provide the primary platform for continuous improvement, whereby such improvements are achieved through changes made to the configuration of the systems. Failing to rigorously manage the configuration of automation systems introduces risks and vulnerabilities that can lead to unintended consequences that can range from minor disturbances to catastrophic accidents.

While the processing industry has long recognized the essential value of a robust asset management program, most such programs have focused primarily on managing hard assets such as pumps, compressors, and instruments. Meanwhile, lack of proper management of change of the amorphous automation configuration has been identified as a significant contributing factor in a number of industrial accidents over the last two decades.

Undocumented and unapproved changes to the plant automation configuration are contributing factors to a number of process industry incidents and accidents. At many plants, a technician or control engineer can walk up to a control system and change any of the following:

- Tuning constants
- Alarm configurations
- Control configurations

These changes could potentially be made without requiring a management of change process. The types of systems involved such as DCS, PLC, SIS, Historian, MES, and advanced applications contain a unique and complex collection of tags, programs, databases, and user interfaces. When a configuration change is made to a given system, interdependent systems are affected. If the configuration change is undocumented and unapproved, then the associated effects on these interdependent systems go unnoticed.

Management of Change

Since automation systems directly control the process, improper changes have a potential for a tremendous negative impact upon plant safety, profitability, and compliance. As such, it is essential to rigorously manage all changes made to the control system infrastructure.

According to industry regulations (OSHA, ISO, NERC-CIP) the process of management of change (MOC) is required when making changes “not-in-kind,” meaning any change that is not a direct replacement of the original. Since many automation system parameters are alphanumeric in nature, any change would qualify as “not-in-kind,” and as such should be subject to change management. In a typical plant today, this is not the case. Unless a change affects a drawing or other entities currently under change control, no MOC process is initiated. If a MOC process is not initiated, unapproved and undocumented changes to automation configuration can be made, which could have undesired consequences.

While most process plants follow an MOC process for changes not-in-kind, they inadvertently exclude the automation system from this safety critical process. Existing MOC systems tend to be either paper-based, or an electronic version of the paper-based system, and are utilized in conjunction with a work order. This methodology results in the change being filed away and often forgotten after the change has been implemented. As a result, a large percentage of industrial plants live with significant vulnerabilities associated with automation change management. At large, this issue and the associated risks are unknown to management team of the facility.

In summary, most companies have recognized the need to manage change in process plants and have established regulations governing the MOC process. However, the proper management of automation changes is generally not fully addressed in MOC regulations.
The standards most closely associated with MOC in the process industries include:

A. OSHA 1910.119—The most significant MOC-related standard for the process industries, including refineries and petrochemical plants, this regulation stipulates, “The employer shall establish and implement written procedures to manage changes (except for “replacements in kind”) to process chemicals, technology, equipment and procedures; and, changes to facilities that affect a covered process.”

According to OSHA 29 CFR 1910.19, the specific items to be addressed for each change include:
- Technical basis for the change
- Time period for the change
- Safety and health impacts
- Authorization requirements

B. NERC-CIP—Specifically written for power generation facilities, this regulation states, “Policies with adherence monitoring and change control must be documented and in place, and change control policies and processes must be adhered to. This includes definitions and documentation on access control levels for critical assets such as Internet-facing systems and critical backend solutions.”

C. 21CFR Part 11—A stringent requirement for the pharmaceutical and life sciences industries, this standard calls for effective management of document control, change control, training control, audits, corrective/preventative action, and other quality and business processes.

D. International Standard IEC61511 recommends using a good MOC with a proper “Impact Analysis” before any change.

The above referenced standards are referring to critical infrastructure and, in practice, automation systems should be considered critical infrastructure.

Advantages of Effective MOC Across Plant Automation Assets

The overall objective of manufacturing is about reducing costs, becoming more efficient, complying with industry regulations, and running a safe plant. This requires a dedication to improvement and a focus on continuous change. However, unmanaged change is inefficient and risky, whereby changes go undetected and can result in industrial incidents and accidents.

A well-designed MOC process is an essential loss prevention tool for any process plant by:
- Improving safety by mitigating risks associated with undocumented and unapproved automation system changes
- Increasing efficiency through streamlining the management of change process
- Meeting regulatory compliance
- Increasing profitability by preventing costly plant upsets, incidents and excursions

Honeywell’s Management of Change Solution

The Intelligent Management of Change (iMOC™) solution is a management of change process workflow application. iMOC™ was specifically designed for automation systems and built upon the DOC4000® framework. It leverages Web 2.0 technologies to facilitate information push and collaboration.

iMOC™ is an integrated add-in module that runs on top of DOC4000 software. DOC4000 is a comprehensive application for automation configuration management. It aggregates and contextualizes configuration databases, programs and user interfaces, and simplifies the visualization and management of information in automation systems. DOC4000 provides comprehensive lifecycle documentation and change management. The software is used to document and track changes in distributed control systems, safety systems, programmable logic controllers, field instrumentation databases, and advanced solutions across an entire industrial automation platform.
iMOC™ is an intelligent management of change solution specifically designed for automation systems. As an DOC4000-enabled application, it takes full advantage of Honeywell’s DOC4000 software and provides the following capabilities:

- Minimizes search for information and analysis time by automatically creating an up-to-date documentation package at the start of an MOC case
- Accurately tracks configuration changes for over 50 different automation systems and their Microsoft® Windows-based servers
- Expedites the MOC workflow by automatically routing approval requests to appropriate approvers and following up
- Detects and reports unauthorized changes made to automation systems
- Provides automatic reconciliation of changes with approved MOC cases

How iMOC Works

iMOC™ leverages context-based information in the DOC4000 database to provide an intuitive MOC solution for industrial assets. The end-user defines the workflow process to meet the needs of a particular site.

iMOC™ automatically compiles the initial information and documentation needed to start the MOC process, ensures all changes made to a plant's automation systems are detected, and reconciles configuration changes with associated MOC cases to ensure that only approved and managed changes occur.

Unlike manual MOC systems, iMOC’s customized workflow process definition and checklist enable users to:

- Detect and reconcile automation changes;
- Route MOC packages for approval;
- Ensure approvals are facilitated properly;
- Push information to the next person required to take action.

The solution provides a graphical environment for definition of MOC workflows, including descriptions of each state within workflows as well as checklists and required transitions for states.

As a DOC4000-enabled application, iMOC™ takes full advantage of DOC4000 software, and also works with DOC4000 Recon™, which tracks changes made to the Windows-based computing infrastructure associated with those automation systems.

iMOC™ automatically reports reconciled changes, thus exposing vulnerabilities associated with improper automation change management.
Each workflow is constructed by dragging state definitions to the desktop and linking them with transitions. Each state definition describes a specific step or stage of the MOC process, such as “Initiation” or “Implementation.”

States may contain checklists that describe each action to be taken within that particular state, and include items such as text entry boxes, check boxes, file insertion points, proposed and reconciled changes, signatures, and informative text.

Transitions describe how a workflow moves from one state to another. If a state has a checklist associated with it, the checklist must generally be completed before transition to the next state is permitted.

Only users to whom permission has been given to execute that transition can execute any given transition. Configured users may be designated as primary or secondary, enabling continuation of the workflow in the event that a primary user is unavailable.
A Scenario Where iMOC Matters

In this example, a major North American petrochemical facility extended the periods between turnarounds, forcing the plant to perform online interlock testing.

The testing procedure called for bypassing an SIS output and ramping the transmitter value to test the interlock.

As expected, the interlock in the SIS tripped, but failed to trip the shut down valve.

Because of insufficient documentation, the testers were not aware of the changes that had been implemented to activate operator start-up assistance logic in the DCS.

The undocumented and unapproved DCS logic sensed the interlock trip, placed all controllers in manual, and set all valve outputs to the fail-safe or shutdown position.

As a consequence of this incident, the plant lost production valued at $150,000 and paid $25,000 in regulatory fines stemming from the environmental excursion.

The DOC4000 system could have prevented this incident by providing the testers with Documentation of the changes to the DCS logic using iMOC.

The iMOC Solution Enables Key Business Improvements

Automation assets are a part of a plant’s critical infrastructure, and therefore it is advantageous that an effective MOC solution is in place.

It ensures that the plant is operating at its highest level of:

- Safety and compliance
- Reliability
- Profitability

Increased Safety and Compliance

Implementing an effective MOC process can prevent a number of incidents, excursions, accidents and cyber security attacks.

With iMOC™, plants can proactively manage unapproved and undocumented changes and identify vulnerabilities.

Reliability

Thorough documentation of all changes made to the system is managed by iMOC™. Tracking these changes enables fast root-cause analysis to ensure business continuity, while helping to save days of investigation and reduce potentially significant financial impact on production.

Economic Benefits

When an incident occurs from neglecting to proactively manage change, the consequences can be potentially very costly.

Regulatory fines from an environmental excursion are estimated at $25,000 on average.

When industrial plants consider the cost of a single incident, then the quantifiable value of the iMOC solution comes apparent.

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost*/Per</th>
<th>Loss*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrels/hour (5.8k)</td>
<td>$112</td>
<td>$649,600.00</td>
</tr>
<tr>
<td>Barrels/day (140k)</td>
<td>$112</td>
<td>$15,680,000.00</td>
</tr>
<tr>
<td>Vendor Visit</td>
<td>$2,000</td>
<td>10,000.00</td>
</tr>
</tbody>
</table>

The iMOC™ solution brings significant value to companies including those needing to meet compliance requirements for MOC and to avert incidents that can be costly to production and reputation.

Entities seeking to avoid problems, mitigate the risk of environmental incidents, and accelerate resumption of operations as part of disaster recovery will equally benefit from the DOC4000 iMOC™ solution.
For More Information
Learn more about how Honeywell’s Management of Change solution can help you manage automation assets, visit our website www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com