Executive Summary
EEMUA Publication 191 “ALARM SYSTEMS - A Guide to Design, Management, and Procurement” was first released in 1999 and is well acknowledged as the defacto standard for Alarm Management. (A second edition was released in 2007). ISA and ANSI approved a new standard in June, ANSI/ISA-18.2-2009 “Management of Alarm Systems for the Process Industries”. The API Recommended practise 1167 was released in December 2010 which is the first alarm practise developed due to regulation.

These publications have similar KPIs for alarm system performance. So what does this mean for your industry?

As an employer, irrespective of the size of the business, you have the responsibility for the day-to-day health, safety and welfare of your employees, visitors to your workplace and the public. This duty of care is usually set out in the occupational health and safety (OHS) legislation of the relevant country. Companies as well as individuals from Supervisor level to CEO level have been legally prosecuted for breaches in OH&S regulations in some countries. Duty of care usually mandates that employers of process and other automated industries must provide a suitable alarm system that gives adequate warning of impending abnormal situations to operators so that they have time to take action to prevent the potential consequences from occurring. Duty of care also includes the provision of a control system that does not put the operators under undue levels of stress, which could also compromise the safety of other employees.

This paper provides information on what alarm management is and why it is important. It also provides an overview of these global standards, and what you can do to achieve compliance.
# Table of Contents

**Executive Summary** .................................................................................................................. 1

**Document Terminology** .......................................................................................................... 5

**What is Alarm Management?** .................................................................................................. 6
  - Definition ..................................................................................................................................... 6
  - Layer of Protection ...................................................................................................................... 6

**What Else is Alarm Management?** .......................................................................................... 6
  - Continuous Lifecycle .................................................................................................................. 6
  - Plant Maintenance/Reliability .................................................................................................... 6
  - Good Process Control ................................................................................................................ 6
  - Outcome of a Risk Assessment .................................................................................................. 7
  - Related to Equipment Failure ..................................................................................................... 7
  - Enhanced/Advanced Control...................................................................................................... 7
  - Abnormal Situation Management (ASM) .................................................................................... 7
  - It Has Been Widely Ignored for a Long Time ........................................................................... 7
  - Often Used In Fault Tree Analysis (FTA) ................................................................................... 7

**Demystifying Standards & Guidelines** ....................................................................................... 8
  - Introduction ............................................................................................................................... 8
  - Which standard do you comply with? ....................................................................................... 8

**Key Features of EEMUA 191 and ISA 18.2** ................................................................................. 8
  - EEMUA Key Features ............................................................................................................... 9
  - ISA 18.2 Key Features .............................................................................................................. 10

**EEMUA Alarm Performance KPIs** .............................................................................................. 10
  - ISA 18.2 Alarm Performance KPIs ............................................................................................ 10

**ISA 18.2 Lifecycle Model** .......................................................................................................... 11
  - Scope of the Lifecycle Model ...................................................................................................... 13
  - Stages of the Lifecycle Model .................................................................................................... 13
  - Philosophy ................................................................................................................................. 13
  - Identification .............................................................................................................................. 14
  - Rationalization .......................................................................................................................... 14
  - Design ....................................................................................................................................... 14
  - Implementation & Training ........................................................................................................ 14
  - Operation ................................................................................................................................... 14
  - Maintenance ............................................................................................................................... 14
  - Monitoring & Assessment ......................................................................................................... 14
  - Management of Change ............................................................................................................. 14
  - Audit .......................................................................................................................................... 14
  - Entering the Lifecycle Model ..................................................................................................... 15
  - Lifecycle Model Loops ............................................................................................................... 15
Table of Figures

Figure 1: Layers of Protection in a Processing Plant .............................................................. 5
Figure 2: Fault Tree Analysis .................................................................................................. 6
Figure 6: Sample EEMUA Results – Total Plant for One Month ............................................. 10
Figure 6: ISA 18.2 Alarm Management Lifecycle .................................................................. 11
Table 1: EEMUA 191 – Benchmark for Assessing Average Alarm Rates ............................. 9
Table 2: EEMUA 191 – Guidance on Alarm Rate Following an Upset .................................. 9
Table 3: Sample ISA 18.2 Alarm Performance KPIs ............................................................. 10
# Document Terminology

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEMUA</td>
<td>Engineering Equipment Material Users Association</td>
</tr>
<tr>
<td>LOP</td>
<td>Layers of Protection</td>
</tr>
<tr>
<td>LOPA</td>
<td>Layers of Protection Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>ISA 18.2</td>
<td>ANSI/ISA-18.2-2009</td>
</tr>
<tr>
<td>DCS</td>
<td>Distribute Control System</td>
</tr>
<tr>
<td>ASM</td>
<td>Abnormal Situation Management</td>
</tr>
<tr>
<td>OH&amp;S</td>
<td>Occupational Health and Safety</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society of Automation</td>
</tr>
<tr>
<td>API 1167</td>
<td>American Petroleum Institute Recommended Practice 1167</td>
</tr>
<tr>
<td>NOHSC</td>
<td>National Occupational Health and Safety Commission</td>
</tr>
</tbody>
</table>
What is Alarm Management?

**Definition**
“A process by which alarms are engineered, monitored, and managed to ensure safe, reliable operations”.

**Layer of Protection**
The concept of Layers of Protection is to provide Independent Layers of Protection around hazardous processes to reduce the risk of undesired consequences such as fire, toxic releases etc (Refer to Figure 1). Alarms are considered to be a Layer of Protection (LOP) and are often used in Safety Integrity Level (SIL) analysis. The intent of these alarms is to warn operators of an impending abnormal situation, which can often have safety related consequences. In determining the average Probability of Failure on Demand for a SIL loop that contains an alarm as a LOP, the probability of the operator failing to adequately respond to the alarm must be considered. Some of the plants that have been reviewed by the author have had unrealistic probability of failure figures such as 0.1 (i.e. a 1 in 10 year probability), where the alarm rates have been over the “maximum manageable” as deemed in the ISA 18.2 standard. This has the potential to make the SIL design for a loop to be inaccurate.

![Figure 1: Layers of Protection in a Processing Plant](image)

What Else is Alarm Management?

**Continuous Lifecycle**
The operating process is continuously changing to meet quality and production requirements. Alarms are an active component of the process and require changes to meet these same needs. Alarm management is a lifecycle process based on a continuous improvement process. If the alarms and associated process and equipment are not regularly maintained then it is most likely the system performance will degrade over time with alarms having a negative impact.

**Process Maintenance/Reliability**
Good process maintenance practices are absolutely critical in terms of process production rates, safety, and alarm system performance. Poor practices can result in chattering alarms, ineffective instruments, false alarms, unplanned outages, environmental excursions, increased operator load and safety related incidents.
Good Process Control
Good process control assists in minimizing the probability of abnormal situations from occurring due to oscillation of the process causing upset conditions, interlock failure, incorrect logic configuration or uncontrolled PID loops. Typically poor process control results in operator actions, chattering alarms, noisy consoles and operator inaction.

Outcome of a Risk Assessment
Every task that is required within a processing plant should be subject to a risk assessment, including determining the requirement to use an alarm to minimize the risk potential. This should be considered simply good engineering practice.

Related to Equipment Failure
All manufactured equipment eventually fails with time! Unfortunately some companies rely too heavily on the higher LOPs (safety systems, pressure relief valves etc) to protect the integrity of their plants. All safety equipment has a probability to fail on demand and should only be employed as a last means of defence.

Enhanced/Advanced Control
There have been significant developments in smart alarming techniques such as state-based alarming, model-based alarming and predictive alarming. These techniques are used to improve the performance of the alarm system as well as minimizing the chance of abnormal situations from occurring.

Abnormal Situation Management (ASM)
This is all about allowing the operator enough time and resources to prevent an unusual event from occurring. The ASM® Consortium has undertaken significant research into graphics, control systems and alarm systems for abnormal situation management.

It Has Been Widely Ignored for a Long Time
On many sites the operators ignore the alarms as the systems are unusable in their current state. There are still chemical plants, coal preparation plants, refineries, power stations, etc where this is the case!

Often Used In Fault Tree Analysis (FTA)
Fault Tree Analysis is a common method of undertaking quantitative risk assessments and is often used to determine the SIL level of a Safety Integrity Level loop.

FTA inputs are either frequency of an event occurring or the average probability of failure on demand. If the PFD for the operator failing to respond to the high level alarm is changed to 0.5, the loop PFD is increased from 0.00011 to 0.00051. Also if the high level trip system is only tested once a year (instead of twice) then the PFD is effectively doubled.

Some industrial plants have fault tree analysis results that put unrealistic targets on operators being able to detect and respond to an alarm before the safety system takes action.

![Figure 2: Fault Tree Analysis](image)
Demystifying Standards & Guidelines

Introduction

EEMUA 191 was first released in 1999 and has since been referred to as the defacto standard for alarm management. EEMUA is written in a text book format and provides some excellent examples in the appendixes. ISA 18.2 has been written more like a standard and has many similarities to the safety instrumented systems standards IEC 61508/11. The API 1167 was released in December 2010 and references the EEMUA 191 and ISA 18.2.

Which standard do you comply with?

EEMUA 191 and ISA 18.2 complement each other. In summary EEMUA describes in detail the tools and techniques for various aspects of alarm management (e.g. rationalization, risk assessments, graphics design), whilst ISA 18.2 clearly defines the required performance KPIs and the overall lifecycle approach to alarm management. The performance KPIs for both documents are similar, although they are more clearly defined in Table 14 of ISA 18.2. The API 1167 is required for pipelines due to the DOT and PHMSA regulation.

Key Features of EEMUA 191, ISA 18.2, API 1167

The main features of EEMUA 191, ISA 18.2 and API 1167 are highlighted in this section.

EEMUA Key Features

- Good detail on alarm design, including different risk assessment approaches.
- Written in a easily readable text-book format – excellent worked examples.
- New section on Alerts.
- Philosophy, principles of alarm system design, implementation issues.
- Measuring performance and managing an improvement programme.
- Specifications for alarm systems.
- Design of field sensors.
- Design of alarm displays.
- Performance metrics and useful questionnaires.
- Alarm suppression hazard study.
- Sample risk assessments and determining priority – enhanced.
- New section on alarm management in Batch Plants.
- New section on alarm system improvement process.
- Complementary to ISA 18.2.

ISA 18.2 Key Features

- Large focus on an alarm system lifecycle.
- Very clear alarm system performance KPIs.
- Written like other similar standards – eg IEC AS 61511.
- Section on compliance.
- Alarm Philosophy – what must be included in table format..
- Alarm System requirements specification.
- Identification and rationalization.
- Basic alarm design, HMI design, and enhanced and advanced methods.
- Implementation, operation, and maintenance.
- Monitoring and assessment, management of change, and auditing.
- Less examples are given.
- Complementary to EEMUA 191.
API 1167 Key Features
- Follows the EEMUA 191
- Has added the lifecycle from the ISA 18.2
- Defines different alarm types and usage
- Defines alarm cases
- Defines roles and responsibilities
- Has a section on alerts
- Has a section on audits
- Describes the purpose of management of change
- Detailed description of Alarm Philosophy Document contents

EEMUA Alarm Performance KPIs
The standards suggest three main KPIs on a per operator basis for 10 minute time periods:
- Average Alarm Rate
- Maximum Alarm rate
- % of time Alarm rates are outside of acceptability target

Average alarm rate is defined as a level of acceptability in Table 1 below. Maximum alarm rates following a plant upset are shown in Table 2. It mentions that the percentage of time alarm rates which are outside of the acceptability target of one per two minutes (or 30 per hour) should be a small number. Once a small number is achieved then it should be based on 1 per 5 minutes to ensure continuous improvement.

<table>
<thead>
<tr>
<th>Long term average alarm rate in steady operation</th>
<th>Acceptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than one per minute</td>
<td>Very likely to be unacceptable</td>
</tr>
<tr>
<td>One per 2 minutes</td>
<td>Likely to be over-demanding</td>
</tr>
<tr>
<td></td>
<td>(industry average in HSE survey)</td>
</tr>
<tr>
<td>One per 5 minutes</td>
<td>Manageable</td>
</tr>
<tr>
<td>Less than one per 10 minutes</td>
<td>Very likely to be acceptable</td>
</tr>
</tbody>
</table>

Table 1: Benchmark for Assessing Average Alarm Rates

<table>
<thead>
<tr>
<th>Number of alarms displayed in 10 minutes following a major plant upset</th>
<th>Acceptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 100</td>
<td>Definitely excessive and very likely to lead to the operator abandoning use of the system</td>
</tr>
<tr>
<td>20 – 100</td>
<td>Hard to cope with</td>
</tr>
<tr>
<td>Under 10</td>
<td>Should be manageable – but may be difficult if several of the alarms require a complex operator response.</td>
</tr>
</tbody>
</table>

Table 2: Guidance on Alarm Rate Following an Upset

EEMUA states that a site, which has a control system with greater than 1000 configured alarms, should be targeting fewer than 10 standing alarms and fewer than 30 shelved alarms (excluding maintenance shelved alarms). EEMUA also provides a graphical representation for different levels of performance of an alarm system. A sample scatter graph report for a plant is shown in Figure 6.
Table 3 shows the important performance metrics listed in Figure 14 of the standard. These alarm performance metrics and target values are very clearly defined and should be the target KPIs for your plant. While these targets may initially appear onerous, they should be possible over time. If your plant’s alarm system performance does not meet the following KPIs, it is important that you can demonstrate continuous improvement with the goal and processes in place to reach these targets.

A flood is defined as starting when 10 or more alarms (per operator) are received within a 10 minute period, and ends when less than 5 alarms are received in a subsequent 10 minute period. A chattering alarm is one that is on then off and on again in a short period of time (e.g. 1 min). Fleeting and/or momentary alarms turn on and off very quickly, but do not necessarily repeat. Stale alarms are those that go into alarm and do not return to the normal state for at least 24 hrs.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Target Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annunciated Alarms per Time:</td>
<td>Target Value: Very likely to be Acceptable</td>
</tr>
<tr>
<td></td>
<td>Target Value: Maximum Manageable</td>
</tr>
<tr>
<td>Annunciated Alarms Per 10 Minutes per Operating Position</td>
<td>~ 1 (average)</td>
</tr>
<tr>
<td>Percentage of hours containing more than 30 alarms</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>Percentage of 10-minute periods containing more than 5 alarms</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>Maximum number of alarms in a 10 minute period</td>
<td>10 or less</td>
</tr>
<tr>
<td>Percentage of time the alarm system is in a flood condition</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>Percentage contribution of the top 10 most frequent alarms to the overall alarm load</td>
<td>1% to 5% maximum, with action plans to address</td>
</tr>
<tr>
<td>Quantity for chattering and fleeting alarms</td>
<td>Zero, action plans to correct any that occur</td>
</tr>
<tr>
<td>Stale Alarms</td>
<td>Less than 5 present on any day, with action plans to address</td>
</tr>
<tr>
<td>Annunciated Priority Distribution</td>
<td>3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, &lt;1% “highest” Other special-purpose priorities excluded from the calculation</td>
</tr>
<tr>
<td>Unauthorised Alarm Suppression</td>
<td>Zero alarms suppressed outside of controlled or approved methodologies.</td>
</tr>
<tr>
<td>Improper Alarm Attribute Change</td>
<td>Zero alarm attribute changes outside of approved methodologies or MOC.</td>
</tr>
</tbody>
</table>

Table 3: Sample ISA 18.2 Alarm Performance KPIs
ISA 18.2 Lifecycle Model

The lifecycle model is an excellent method of representing the overall process of alarm system management. It is an ongoing process that is suitable for new or existing systems. It has been designed to represent sequential stages, some of which run simultaneously with other stages that are linked horizontally (e.g., MOC (Stage I) must be followed for Stages B, C, D, and E).

In some cases, a sequential stage may be "skipped". For example, during a rationalization exercise, the outcome may be an alarm setting change, which may not require detailed design to implement.

Figure 6: ISA 18.2 Alarm Management Lifecycle

Scope of the Lifecycle Model

The lifecycle model is limited to computer-based alarm systems and excludes sensors and final control elements. Safety Instrumented Systems (SIS) are also excluded except for any alarms generated from them.
Stages of the lifecycle model

Philosophy
An Alarm Philosophy documents the site approach to alarm management and is a mandatory requirement. It includes definitions, principles and details of the practices and procedures for each of the remaining life cycle stages. It provides a lasting reference to sustain an effective alarm system. A table containing the required and recommended contents of the Alarm Philosophy is provided in the draft standard. Alarm System Functional Specifications detail the control system specific implementation related to the Alarm Philosophy definitions.

Identification
Many methods are available to determine if an alarm is required. Some of these are Process Hazard Analysis (PHA), incident investigations, HAZOPS/CHAZOPS, and alarm design/rationalization workshops. The outcome of a HAZOP might be that an alarm is required to warn the operator of an abnormal situation (eg High Pressure). Typically a HAZOP exercise does not consider the following: is the particular tag the most suitable to alarm, what is the ideal setting, configuration details, the potential operator workload etc. These details are discussed in the Rationalization stage before an alarm is to be implemented. Identification and the following three stages are closely related. Due to different terminology used in process industries, it can be somewhat confusing as to which steps in the overall design process are undertaken in each stage.

Rationalization
Alarm rationalization is about reconciling each individual alarm against the principles and requirements of the alarm philosophy. It is important that the relevant data for each alarm is documented to support the other stages of the life cycle. This includes the alarm description, settings, causes of an alarm, consequence of no action, the required operator action, response time, consequence rating, etc. Consequences and the response time are documented and the alarm priority is determined from a matrix of the consequence severity and response time. This matrix is defined by the alarm philosophy. The methodology in the Rationalization stage also applies for new projects. The main difference with new projects is typically there is no historical trends or alarm data that can be referred to.

Design
The design phase includes the basic DCS/PLC configuration of the alarm, Human Machine Interface (HMI) for the alarm, and any advanced methods of alarm management. These requirements are determined in the rationalization stage.

Implementation & Training
This stage involves the various other activities required to put the alarm into service. It includes testing of the alarm system functions as well as relevant training for the operator and other personnel.

Operation
The alarm is now in service and reporting abnormal conditions to the operator.

Maintenance
Process measurement instruments, final control elements, and control systems all require periodic/predictive maintenance to ensure their continued reliable operation. This is critical to ensure the ongoing performance of the alarm system.

Monitoring & Assessment
This stage includes the periodic collection and analysis of data from alarms. Without monitoring it is virtually impossible to maintain an effective alarm system. Assessment should be undertaken frequently (daily or weekly) and is the primary method for determining problems such as nuisance alarms, stale alarms, and alarm floods.

Management of Change
Management of change is a critical stage that helps ensure the ongoing integrity of the alarm system. It needs to be a structured process of approval and authorization for any additions, modifications, and deletions of alarms from the system.
Audit
A periodic audit of the alarm system and the processes detailed in the alarm philosophy may determine the need to modify processes, the philosophy, or the design etc. This is also the ideal stage to enter the alarm system lifecycle process. The audit may also highlight that an organization’s discipline to follow the processes (especially MOC) may need improvement.

Entering the Lifecycle Model
It is possible to enter the lifecycle model from the Philosophy, Monitoring and Assessment, or Auditing stage.

For Greenfields projects it is best to start with a Philosophy before any rationalization/design is undertaken.

For existing sites the ideal entry point is usually the Monitoring and Assessment stage, which will provide a benchmark for the site alarm system (per operator). This provides a snapshot of the health of the alarm system and can be used to justify improvement work. Undertaking a detailed audit will highlight any deficiencies that your alarm system will have in any of the other stages (A-I).

Lifecycle Model Loops
There are three “loops” in the lifecycle model that are represented by the dotted lines in Figure 6. If an alarm issue is detected in the Monitoring and Assessment stage then it would be resolved via the Monitoring and Maintenance Loop (e.g. chattering alarm) or the Monitoring and Management of Change Loop (e.g. more complex issue). The monitoring and maintenance loop typically is applied for simple maintenance related issues whereby the Monitoring and Management of Change Loop is required for any design changes. The Auditing and Philosophy Loop basically entails the whole lifecycle process. Periodic audits of your alarm system are a requirement of the standard.

ISA 18.2 Compliance.
The ISA 18.2 has a section on compliance (section 4.1) and a grandfather clause (section 4.2). It refers to those existing plants that must be able to demonstrate that their alarm system “equipment is designed, maintained, inspected, tested, and operated in a safe manner”.

Dynamic Alarming – Is it Right for You?
With the advancement of alarm management more companies are moving forward with programs to reduce alarm rates and are utilizing alarm rationalization to improve the design of alarms. The next phase is to analyse flood conditions and implement dynamic alarming to improve the alarm rates during upset conditions. Implementing dynamic alarming will require ongoing effort to verify the strategy and changes to the strategy when there are process changes.

It is recommended to reduce alarm chattering and complete a full rationalization before applying dynamic alarming to flood conditions because these improvements will reduce the alarm rates and potentially solve the flood condition during upsets and not require additional flood suppression logic. However during the rationalization process there is benefits in using one of the following suppression techniques to minimize alarming:

- First out alarm
- Command disagree
- Escalating alarm
- Calculated alarm based on
  - Process conditions
  - State conditions

Flood condition during upset conditions should not be taken lightly because the operator does not normally operate under these conditions and with the added increase in alarm rates and equipment failures; there is an opportunity for critical alarms to be missed. Reducing the alarms will allow the operator to focus on the issues and use the alarms to identify the cause and mitigate the failure.
Remember the alarms are a tool the operator uses to solve process problems, reducing the alarm rate to a point that increases the time to determine the issue by an operator will have a negative impact on production, safety and environmental. The operator is capable of determining that 2 or 3 alarms are related and the additional information points in the direction of the solution.

What Steps Can You Take?

Now is the time to act. The following steps will help you get on the road to a successful alarm management program:

- Purchase EEMUA 191, ISA 18.2 and API 1167.
- Undertake some form of an audit of your alarm system. An audit will highlight the deficiencies of your alarm system and what areas need to be improved. As an absolute minimum, undertake a benchmarking and assessment project to determine if your alarm rates are acceptable.
- It is critical to get senior management sponsorship for an alarm system improvement project. Information that should help management sponsor your project are operator survey results, and a benchmarking and assessment report which compares your plant alarm system KPIs with EEMUA 191, ISA 18.2 or API 1167 requirements.
- Prepare a Strategic Plan to reach compliance. This plan may contain the following:
  1. Alarm Philosophy Document development
  2. Functional Specifications
  3. Purchase of alarm database and associated software tools
  4. Top 20 and/or Classic rationalization depending on budget and the state of the alarm system
  5. Project plan for the next 12 – 24 months (including milestones)
  6. Required training – engineers, technician, and operators
- Implement the Strategic Plan!

Conclusion

The author has visited many processing plants globally over a number of years and the situation remains that many plants are still not taking alarm management seriously enough. Alarms form part of your plant’s layer of protection and as such should be maintained to a level stated in EEMUA 191, ISA 18.2 or API 1167.

EEMUA was first released in 1999 and ISA 18.2 was released in 2008 and API 1167 was released in 2010 – if your plant’s alarm system is ineffective or even totally ignored by the operators – then I suggest you act now!

In the future it is expected that there will be more prosecutions for OH&S breaches!

References

1. EEMUA Publication 191 “ALARM SYSTEMS - A guide to Design, Management, and Procurement”
4. IEC 61511-2004 “Functional safety - Safety instrumented systems for the process industry sector”
5. API Recommended Practice 1167 First Edition, December 2010
For More Information
Learn more about how Honeywell’s Alarm Management solution can improve safety and reliability at your plant, 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