

ARC WHITE PAPER

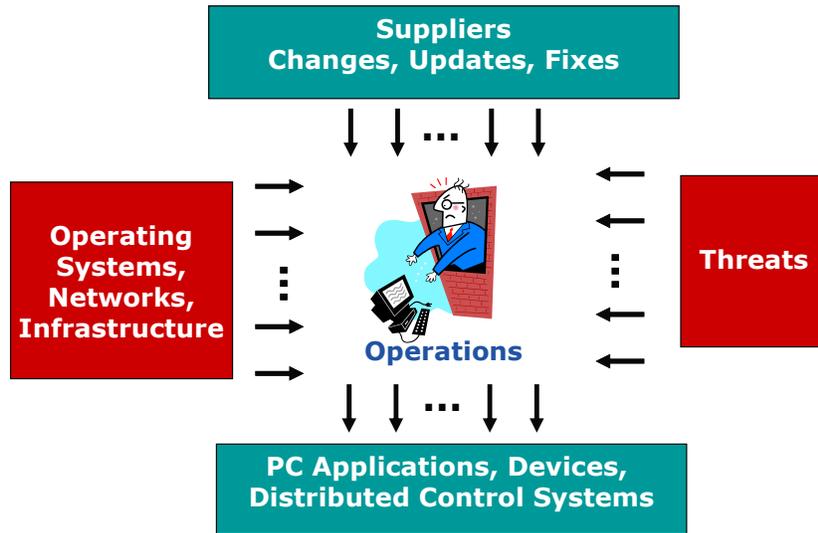
By ARC Advisory Group

JANUARY 2007

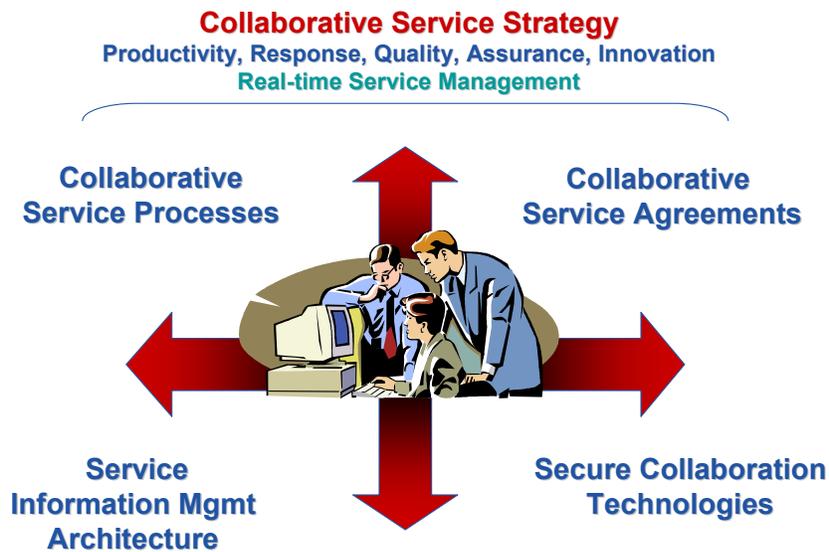
Collaborative Service Management Reduces Cost and Risk

Executive Overview	3
Trends in Process Industry Operations Challenge Service Models	4
Problems with Existing Service Models.....	5
Incremental Improvement Strategies May Offer Relief	7
Collaborative Service Strategies – A Framework for Innovation	8
Emerson’s Guardian Approach	11
Conclusions and Recommendations	14





Systems Maintenance and Security Updates Have Become High Risk



Create a Platform for Collaborative Service Innovation

Executive Overview

Security, compliance and others are changing systems update strategies while operations staffing remains limited. Continuing to add tasks and complexity to existing staff is high risk and we need a framework for service innovation. Collaborative Service Strategies involve suppliers more deeply than traditional service processes and enable the supplier to help their customers address growing requirements.

Increasing system complexity, a constant stream of updates, growing compliance requirements, and others are forcing change in the way process and other industries are keeping their information and control systems up-to-date. For example, security patch management requires that some updates be installed immediately in contrast to a traditional annual update process. The overall effect is that systems support engineers must constantly watch multiple Web sites for events that require action, analyze available information to determine whether they really affect installed systems, and then plan, test and deploy changes. Operations staffing has no capacity for this increasing load and associated skills and this is presenting a growing risk.

Incremental improvements to existing strategies may help, but the Industry needs more innovative approaches. Collaborative strategies can provide a framework for innovation in service to reduce costs and risks by enabling suppliers to become more involved and apply their deep system knowledge. This requires new contractual agreements, development of collaborative processes, service information management, and others.

Emerson's Guardian Support provides several examples of collaborative service. Guardian includes maintaining accurate information about customer systems remotely, and utilizing that information to provide new support services. For example, the Guardian service includes matching security and other information to actual customer installations. It also includes alerts that eliminate the need for customers to constantly monitor DeltaV and corresponding operating system support sites.

Ultimately, collaborative service strategies may require technology and common solutions that enable customers to securely manage remote access to their systems, including making changes. Common solutions reduce diversity in customer environments and eliminate the associated costs. Several levels of common solutions are likely to be needed and this can not be developed until collaborative processes and agreements have matured.

Trends in Process Industry Operations Challenge Service Models

Several industry, technology, and regional changes have invalidated traditional system service models and this presents a growing risk to Process Industry operations. This paper primarily addresses service of automation and information based systems but the issues are similar for other assets and other similar industries.

Security has changed the Update Process

Distributed control and information systems have moved from closed, proprietary components to open, commercially available systems, typically including Windows operating systems; this changed the maintenance processes, workload, and skills required. Operations engineers frequently receive critical updates, such as security patches, requiring constant attention and specialized knowledge. Systems within operations are often supported by controls engineers who do not have the time or training to handle the additional tasks. Additional training is seldom a solution because small teams must service diverse and complex systems.

Compliance and Due Diligence Pressures are increasing

Safety, environmental impact and regulatory compliance has always been a priority for process industry operations but recently confidentiality, financial reporting, and security concerns have created growing reporting requirements. To satisfy these needs, operations must keep additional records and also must provide assurances that processes are comprehensive and all solutions have been considered. This requires increased collaboration internally and externally.

Compliance and reporting in general is driving increased interest in collaborative arrangements where the experience and knowledge of others can be utilized to provide a higher confidence level.

Operations IT is getting More Diverse and Complex

Operations information technology and infrastructure has been getting gradually more diverse and more complex due to increases in security infrastructure and the need for increased integration and information sharing across the enterprise. This is problematic for operational sites where a

small engineering team has provided system support as only one of a diverse set of tasks. If operations cannot increase staff levels, they must rely on central organizations or outsource elements of support.

Operations Staffing Strategies are in Flux

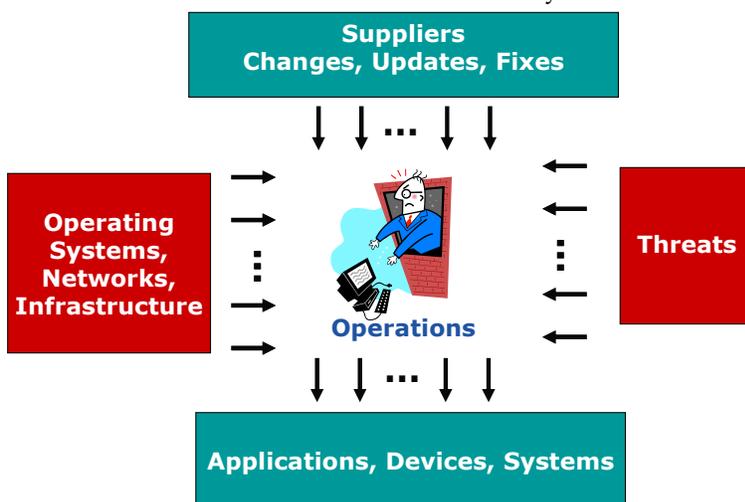
Process control engineering and corporate IT has traditionally been at least two independent organizations; domain and technology requirements were completely different. Recently, security issues, technology convergence, and cost pressures have driven the organizations much closer together, but best practices for managing this situation have not evolved. Many businesses are still working through various combinations of corporate, site and outside staffing. This state of flux means changing support roles with high training requirements and temporary loss of capabilities.

Problems with Existing Service Models

Traditional service models present a growing risk to end users because they have become out of alignment with current need, and overburdened operational staff within a diverse and changing environment.

Service Agreements Are Out of Alignment with Need

Traditional support agreements do not address security patch management, leaving suppliers with no contractual service level agreement to satisfy related needs. Security vulnerabilities are more frequently found in the



Current Service Models Are Too Labor Intensive

operating system and network infrastructure and these are not directly the responsibility of application and system suppliers.

However, application and system suppliers are an integral part of the patch process: end users can not install operating system patches until suppliers validate their product with operating system patches and possibly develop needed changes to their products.

The lack of definition of responsibility has resulted in inconsistent responses from suppliers to security updates, ranging from days to months to never.

Even critical patch and update may not need to be deployed for some systems, but it takes considerable research to come to an informed conclusion.

Applications and systems suppliers are also essential to end user threat analysis and risk mitigation processes. While waiting for patch development and associated application validation, end users must consider the risk of threats and then decide what interim action to take, if any. To do this, end users need specific information from all system component suppliers. This level of interaction is also not defined in most agreements.

Current User Processes are Labor Intensive and Risky

Traditional service approaches depend too much on end users monitoring multiple sources for events and changes that may affect their systems operation, security or safety. For security alone, end users must:

- Maintain an accurate inventory of all systems and versions
- Monitor all suppliers for changes, version updates, issues, ...
- Monitor cyber security threats and their attack methods
- Analyze and assess actual risk within the users environment
- Lab test, deploy, field test, resolve issues, recovery ...

Of course, systems service includes many other tasks beyond security related issues such as diagnosing and correcting software and hardware failures, resolving performance issues, reporting, planning, managing routine changes, backup and recovery, and others. The size, complexity, knowledge requirements and interrupt nature of these responsibilities increase the chances of missing something and thereby increase risk.

End Users Must Integrate Services from Many Suppliers

It is important to remember that end users have many suppliers with diverse service agreements. This often results in a very complex update situation, especially when multiple products are integrated in one system or computer. Multi-site coordination and related issues also add another variable and degree of complexity for end users. The growing cost and complexity of this diversity suggests that there is a need for common industry level practices, technologies and solutions.

Incremental Improvement Strategies May Offer Relief

The most conservative and least disruptive improvement strategy is to address the weaknesses in current service arrangements one at a time. This provides more assurance that the most important weaknesses get addressed across a broad cross section of suppliers. However, it may also preclude rapid progress and limit ultimate solutions. A few important candidates for short term action follow.

Enhance Agreements with Security Service Levels

In process industries and similar environments, uptime is essential and establishing predictable threat, vulnerability and patch response process in service agreements enables end users to plan system downtime better, possibly batching changes into one shutdown. For example this might involve getting supplier commitments for:

Getting agreement from some suppliers may be more difficult than expected. In a sense we are asking suppliers to agree to corrections to unknown problems and this presents additional risk to the supplier.

- Recognizing operating system and other patches as their issue
- Initial response (days) to new threats and patches
- Final validation (weeks) of operating system patches
- Final corrections to their software
- Guidance and comprehensive information throughout the process

Many suppliers already have policies that can be used as a starting point when developing corporate standards.

Automate Service Processes for Consistency

Many of those labor intensive tasks discussed above (inventory, monitoring, testing, etc.) can be automated using a variety of software tools. Once accomplished, this can eliminate repetitive tasks, improve information accuracy and timeliness, and facilitate better planning.

Most such tools have been developed for corporate IT environments and special care must be taken when applying them to operations environments. Because tool developers have focused on corporate IT, their tools typically need to be extended for automation level systems and devices.

Consider the Indirect Impact of Regulations

Even when regulations are not aimed directly at operations, corporate culture and business practices that address regulated areas eventually spill over into other areas. The impact may be limited to increases in reporting but may also extend to requiring assurances that everything reasonable is being done to mitigate problems and meet responsibilities. Increased reporting may be handled by automation tools but assurances require more comprehensive service processes and industry level collaboration.

Collaborative Service Strategies – A Framework for Innovation

Collaborative strategies are intended to reduce user risk and improve service by involving suppliers more deeply in many aspects of service. Collaborative service strategies can more easily address the issues associated with current practices than incremental improvements within traditional approaches. They can also provide a framework for suppliers and end users to adapt to new requirements that will come from changes in regulations, technology and others.



The essence of collaborative service strategies lies in the development of collaborative processes that are supported by new service agreements, shared information management and technologies that enable secure remote access to the target systems.

There are likely to be at least two phases in evolution toward ideal collaborative solutions. During the first phase, service is optimized by collaboration between a single end user and each of an end user's suppliers.

Collaborative Service Processes

One way to improve the effectiveness of service is to create collaborative service processes that involve suppliers more deeply. Suppliers and their customers must define and examine comprehensive service processes and identify places where the supplier can perform more effectively than the end user to reduce end user cost, improve asset performance, increase confidence that programs are comprehensive and others.

Supplier Strength	Design Collaborative Processes To Use Supplier Strengths
Deep Internal Product Knowledge	Suppliers have internal knowledge of their products, access to source code, extensive test experience and knowledge of what and how external functions are used. This knowledge is necessary to evaluate the impact of environment changes such as security patches to operating systems. It is difficult to document all this knowledge and pass it to end users for consumption in a short period. Consequently, problem diagnosis, risk assessment and impact predictions processes can benefit significantly from deep involvement from suppliers.
Multi-customer Visibility	End users know their particular implementations and configurations best but suppliers gain perspective and experiences from many customers. Collaborative processes that enable end users to benefit from the suppliers general knowledge will avoid mistakes made by others.
Invest in Capabilities	Heavy involvement in customer service processes enable them to identify common needs and develop capabilities that automate many functions performed manually. End users typically find it difficult to justify high levels of service automation while suppliers can distribute the cost over many customers. Some of these capabilities also reduce supplier support costs and become competitive differentiators in addition to additional source of revenues.

Considerations for Extending Collaborative Processes

Collaborative Service Agreements

Some service improvements will come at little or no cost to end users, possibly where both supplier and end user benefits. But rapid progress is more likely to come when suppliers can simply perform functions at a lower cost than end users and are compensated for it. Of course, this requires changes to service agreements with well defined performance and other expectations.

Service Information Management Architecture

Collaborative service processes will require end users and suppliers to share more information and collaborate remotely, and it is not clear how this should be implemented. At this point it is done with a mixture of technologies ranging from email to portals combined with instant messaging, remote control products and others. As information needs grow and suppliers become more deeply engaged in their customer service processes, overall service information architecture will need to mature and standardize as much as possible.

Suppliers need more detailed information about customer systems. This may be simply a systems inventory with sufficient detail to enable supplier

Collaborative service processes require that end users and suppliers routinely share more information and collaborate remotely. This now requires several technologies and must be assembled according to the needs of specific service agreements. Architecture for collecting, managing and accessing shared information must be developed.

to make more specific service recommendations, or may include operational information that enables a supplier to monitor performance for optimization or more proactive maintenance activities. It may also include configuration information so that suppliers can determine which system functions are actually in use when filtering information and updates.

One basic architectural question is whether to store information in the supplier systems, customer systems, or both. Considerations for multiple suppliers, security, confidentiality, intellectual property and others can make the decision difficult. A related question is how and when to exchanged or synchronized information. Clearly, information system flexibility is required to accommodate the evolution of collaborative processes for analysis, reporting, and planning.

Secure Remote Collaboration Technologies

Collaborative service typically involves people, information and systems located in several locations. The systems to be serviced are in the operating sites; some corporate support staff may be in a different location; and supplier support staff may be elsewhere. Consequently, to provide fast response and high availability of expert help, some form of remote access to serviced systems is necessary.

A very large range of remote access techniques may be used, depending on the service to be provided, service level agreement and most importantly

security policies of the end user. In some cases, simple information exchanges may suffice and in others, remote service personnel may need the capability to actually re-configure certain systems aspects remotely. The latter requires that the end user have granular control over remote service capabilities and few solutions are available.

Emerson's Guardian Approach

Emerson Process Systems recently developed Guardian Support for DeltaV systems with the goal of providing personalized service that will enable customers to be more proactive. Many of the Guardian features provide good examples of collaborative service and validate a collaborative approach.

Emerson Matches Service Events to Customer Systems

Emerson, like other suppliers, is monitoring security alerts from operating systems suppliers, analyzing the impact on DeltaV systems and providing relevant documentation and updates for DeltaV systems. However, under Guardian Support, Emerson takes the additional responsibility for match-

Guardian Support includes traditional support in the form of access to technical experts, service tickets management, trouble shooting help, defect corrections, a support knowledge base, and others. Other features indicate that Emerson has a collaborative model in mind.

ing and ranking alerts to specific customer DeltaV systems, and provides recommendations on the urgency for installing operating systems patches. To make this level of analysis, Emerson must develop and maintain an accurate inventory of customer systems, including an awareness of updates actually deployed.

Emerson Maintains a Shared Customer Database

Emerson forms the customer database by instrumenting all DeltaV systems (version 7.4 and above) with a utility that collects detailed system information – models, versions, operating system version, patch status, configuration, etc. – and packages it for transmittal to Emerson. Of course, the exchange of information is under customer control and the system operator may use the internet, email or a manual method. The information may be updated as frequently as the customer feels necessary.

Once Emerson receives the information package, it is processed and stored in a secure database along with other support information where it may be accessed by Emerson support staff as well as the Guardian customer. Having accurate, current information on hand in the Emerson support group, eliminates slow and error prone manual data collections by the customer when support is needed. It also enables Emerson to proactively analyze the impact of changes on customer systems - even when customer support people are not available - and alert customers only when necessary.

Guardian Customer Access the Support Database

Collaborative service strategies require effective communications, and Guardian takes a Web-based approach for sharing the customer database and other support information. A secure Web-site organizes all Guardian customer collaborations in one place. This includes all information needed for the system maintenance, service calls, license maintenance and configuring the Guardian service.

As described, the Guardian database enables faster and more comprehensive responses for traditional support, and Emerson is also finding that it

Web-based Access to ...

Service call status

Service and warranty status

DeltaV license status

Actual Emerson and operating system versions

Cyber Security Status

Filtered knowledge base articles

System change monitoring

Available service reports

Configuration of Alerts

Guardian Service Visibility

provides other value to customers. For example, customers often find it difficult to maintain an up-to-date inventory of automation systems in a readily useable form; Guardian does this for customer DeltaV systems, sharing current information through the secure Web site.

In addition to viewing details about their systems, customers can also review knowledge base articles and service information which has been filtered and annotated for Guardian customers. For example, this means that DeltaV customers do not have to monitor each operating system security patch, analyze them for relevance to DeltaV systems. The knowledge base also includes assessments for non-security related service activity as well.

Customer Alerts Drive Collaborative Processes

Guardian Support includes customer selectable alerts which enable collaborative processes and eliminate the need for Guardian customers to routinely check the site. Customers can select the alerts which suit their

maintenance processes and have them delivered by email or the increasingly popular RSS feeds.

Customers must consider their overall network architecture, security and other infrastructure when deciding what final action to take. However, relative to traditional support, Guardian information gathering, filtered alerts and Web-based customer site offer the capabilities to significantly reduce customer work load and reduce the risk of missing important service events.

When a customer receives an alert, they know that Emerson support has already decided that it is relevant to them and some form of action is advisable. The customer can go to the secure Web site, view knowledge base articles that are relevant to the topic of the alert and see Emerson recommended actions, explanations, work arounds and other information.

Customer Feedback Validates Collaborative Models

ARC validated some of the collaborative service concepts in Guardian customer interviews. Their situations were somewhat different but all were wrestling with issues created by small control system support teams and growing diversity across operations.

In general, distributed control systems are reliable and no one wants to change them when they serve the purpose. Consequently, there is no justification for a large support staff, creating a situation where a small staff must perform a large number of complex tasks infrequently. The lack of practice and experience presents a high risk. Emerson guardian mitigated this risk by providing an accumulated knowledge base that could be easily accessed when needed. This supplements traditional support methods provided by call centers and email.

The introduction of PC and Windows technology into distributed control systems brought along a growing need for deep knowledge that was beyond what service organizations could build and maintain, mostly because of lack of time. Adequate computer, operating system and security expertise typically resided elsewhere in the company but those groups lack knowledge and practices that are appropriate for control systems. Guardian offered immediate relief by moving the tracking and analysis function to the Emerson team. The Emerson team, which has the PC, Windows, security and systems experience, filters information for the customer and sends them only the information and recommendations that apply.

Another immediate benefit came from having access to a shared call and problem-tracking database. This eliminates significant customer record keeping and provides the capability to analyze problems across systems.

In general, Guardian customers found immediate value in the certain features and were looking forward to exploring other features. There was no concern with sharing system information with Emerson. We conclude that the Guardian customer experience is a validation of the potential of collaborative service processes in manufacturing operations.

Customer	Comment
Laurentiu Lungu, ROMPETROL PETROMIDIA	"The economic situation in Romania makes it difficult to keep control system experts and hire experienced replacements. Emerson Guardian service fills in many of our knowledge gaps and restores much of the confidence a larger staff gave us."
David DeBari Santoprene Speciality Products	"Our control systems engineers could spend 20-30% of their time sifting through system and security updates and this is not their primary job function. Emerson Guardian got it right by filtering all that info to just what we need to act on and pushing it to me in alerts in a manner that I can configure to my liking."
Dan Brown Canfor Taylor Pulp Div	"After installing our DeltaV system we found that it took hours to manage the Windows-based system updates and patches. Guardian service not only reduces the time need but also reduces the risk - when we started, Guardian even found that we had applied a patch that had not been tested. One of the nice things is how Guardian manages service call history and gives us easy access to it - this eliminates the stack of manila folders and notes that I would have to keep."

Customer Comments Validate Initial Benefits

Conclusions and Recommendations

Service of information-based systems has become more difficult, requiring time and people that are not available on operational sites. This is driving the industry to examine innovative service models that distribute the workload and share information and knowledge between end users and suppliers.

Some suppliers recognize the need and opportunity and will lead; others will wait until the collaborative service model has evolved, resulting in a variety of solutions which can become problematic for end users. This pre-

sents an opportunity for a second phase collaborative model that encourages industry wide approaches and standardization to the extent possible.

- Collaborative service management provides a valid model for developing next generation service offerings. End users and suppliers should explore collaborative options for lowering overall risk and costs while increasing service.
- Emerson is on the right track and should utilize Guardian Support customer engagements to define and deliver additional innovate services.
- End users should standardize their collaborative service requirements, consistent with their security practices, and work them into purchase agreements.
- End users should also work within industry groups to form common practices to enable suppliers to develop consistent offerings to the extent possible.

Analyst: Robert Mick

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Community/terms/terms.htm

APS Advanced Planning & Scheduling	HMI Human Machine Interface
B2B Business-to-Business	ISV Independent Software Vendor
BPM Business Process Management	IT Information Technology
CAS Collaborative Automation System	MRP Materials Resource Planning
CMM Collaborative Manufacturing Management	OpX Operational Excellence
CPAS Collaborative Process Automation System	OEE Operational Equipment Effectiveness
CPM Collaborative Production Management	PAS Process Automation System
CRM Customer Relationship Management	PLC Programmable Logic Controller
DCS Distributed Control System	PLM Product Lifecycle Management
EAI Enterprise Application Integration	RFID Radio Frequency Identification
EAM Enterprise Asset Management	ROA Return on Assets
ERP Enterprise Resource Planning	RPM Real-time Performance Management
	SCM Supply Chain Management
	WMS Warehouse Management System

Founded in 1986, ARC Advisory Group has grown to become the Thought Leader in Manufacturing and Supply Chain solutions. For even your most complex business issues, our analysts have the expert industry knowledge and firsthand experience to help you find the best answer. We focus on simple, yet critical goals: improving your return on assets, operational performance, total cost of ownership, project time-to-benefit, and shareholder value.

All information in this report is proprietary to and copyrighted by ARC. No part of it may be reproduced without prior permission from ARC. This research has been sponsored in part by Emerson Process Systems. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100, Email: info@arcweb.com
Visit our web pages at www.arcweb.com



3 ALLIED DRIVE DEDHAM MA 02026 USA 781-471-1000

BOSTON, MA | WASHINGTON, D.C. | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA
CAMBRIDGE, U.K. | DÜSSELDORF, GERMANY | MUNICH, GERMANY | HAMBURG, GERMANY | TOKYO, JAPAN | BANGALORE, INDIA | SHANGHAI, CHINA