DEPLOYING AND USING CONTAINERIZED/MODULAR DATA CENTER FACILITIES

EDITORS:
Christopher Kelley, Cisco Systems
Jud Cooley, Oracle

CONTRIBUTORS:
Ron Bednar, Emerson
Buster Long, Cisco Systems
Suzen Shaw, Microsoft
Executive Summary

The rapidly maturing containerized and/modular data center facility (CMDF) platforms offered within the industry today can enable organizations to realize significant and demonstrated technical and business value when properly applied. This value comes from the repeatable, pre-engineered, prefabricated, and quality-assured set of building blocks that together bring online the necessary amount of IT capacity.

This new containerized/modular approach to the construction and deployment of a data center can be expected to be rapidly deployed, have lower operating and capital costs, and be equipped with higher density and energy-savings targets. CMDF architecture has become an increasingly viable and robust alternative when considering a data center build, with multiple implementation approaches from various suppliers in the industry.
Table of Contents

I. Introduction ......................................................................................................................................................... 3
II. Defining Traditional Data Center Facilities........................................................................................................ 4
III. Defining Containerized/Modular Data Center Facilities................................................................................... 7
IV. Business Flexibility Considerations ................................................................................................................. 13
V. Financial and Planning Considerations ........................................................................................................... 17
VI. Additional Considerations ................................................................................................................................ 21
VII. Conclusion ......................................................................................................................................................... 36
VIII. References ........................................................................................................................................................ 36
IX. About The Green Grid ....................................................................................................................................... 37
X. Appendix A. Understanding Reliability and Resiliency.................................................................................... 38

I. Introduction

Over the past several years, the data center facilities industry has started toward a significant transformation. In this transformation, traditional perceptions of data center facilities as multi-year, site-constructed, low-density buildings are shifting toward viewing them as conceived and constructed from a modular, flexible, and certainly more rapidly deployable set of solutions. Within this latter view are solutions that include not only containerized platforms, but also modular, pre-engineered, and prefabricated building blocks. When deployed and integrated with the required mechanical, electrical, and related services, these building blocks come together and enable the end user to realize a complete data center facility.

In contrast to traditional site-construction methods, the new containerized/modular approach to the construction and deployment of a data center can result in a faster deployment, lower operating and capital costs, and the potential to be equipped with higher density and energy-savings targets. Furthermore, this new approach enables organizations to adjust their data center facilities’ capacity up and down in smaller, prescribed steps rather than in large jumps. Many organizations also will look at the containerized/modular approach to help them cycle new IT and facility technologies into production, while cycling out older and less cost-effective solutions. That said, there are particular considerations that need to be accounted for as part of the planning, design, deployment, operations, and decommissioning phases of the facility lifecycle.

The Green Grid (TGG)—an international, non-profit consortium working to enhance data center resource efficiency—produced this white paper to introduce the audience to some of the more critical of these considerations. It offers a framework of understanding that, when coupled with the right qualified expertise,
may enable potential end users of containerized/modular data center facility (CMDF) platforms to be more prepared and successful in their proposed projects. The following chapter explores the traditional facility construction approach, with a deep discussion of the containerized/modular facility approach in Chapter III. Chapters IV, V, and VI explore particular considerations, limitations, and advantages of the containerized/modular facility architecture and contrasts those factors with the traditional construction approach.

II. Defining Traditional Data Center Facilities

In order to understand the potential value and opportunity that containerized/modular facility platforms offer, it is essential to understand how this new approach differs from the traditional site-constructed model. This section introduces a view of that traditional approach.

Traditional data center facilities are commonly referred to as “site-constructed, fixed structures” and may also be called “brick-and-mortar” buildings. These traditional facilities are typically custom-designed for the specific site, and all or most of the construction occurs with the use of local trade labor at that site. Additionally, they tend to incorporate multiple design methodologies, including both low- and high-efficiency architectures as well as innovative and non-innovative approaches to power, cooling, and other systems within the facility.

COMPONENTS OF A TRADITIONAL FIXED DATA CENTER FACILITY

Regardless of the approach used in the design and construction of these traditional fixed facilities, it can be expected that certain elements of the building would always exist. Described as core facility areas (CFAs), they include:

- Information technology (IT) payload or data hall areas
- Infrastructure or support areas
- Ancillary areas

In many ways, a data center facility is much like a series of blocks. Together, these blocks provide the capacity and services necessary to support the installed IT equipment, the needs of the facility itself, the needs of its occupants, and the needs of regulatory and other parties. (See Figure 1.)
Figure 1. Many interrelated parts make up a facility’s whole

Nearly all data center facilities will have a combination of these CFAs. The intricacy and nature of any given area will vary based on specific requirements (such as density\(^1\) or security requirements). Table 1 below defines each of the major CFAs.

Table 1. Types of CFAs

<table>
<thead>
<tr>
<th>Core Facility Area</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload/data hall areas</td>
<td>The portion(s) of the facility that provides the underlying spatial area to house data processing and communications equipment</td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Whitespace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Racks and cabinets (traditional and self-cooling)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Power distribution within, between, and to the racks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Room and rack-level cooling, humidification, and dehumidification systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Fire detection and other life-safety services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Lighting and other general services</td>
</tr>
<tr>
<td>Infrastructure areas</td>
<td>The portion(s) of the facility that provides the required underlying power and cooling capacity to support the payload/data hall</td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Cooling systems (including chillers, air exchangers and economizers, condensers, misting systems, and related apparatus)</td>
</tr>
</tbody>
</table>

\(^1\) “Density” as used here refers to the measure of the amount of power and cooling made available per spatial unit, usually expressed as kilowatt (kW) per rack, or watt (W) per square foot (or meter).

©2011 The Green Grid. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted, or stored in any retrieval system of any nature without the written permission of the copyright owner.
<table>
<thead>
<tr>
<th>Ancillary areas</th>
<th>area(s) and the facility at large</th>
<th>Heat rejection systems (including cooling towers, dry coolers, and related apparatus)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Power generation systems (including generators, cogeneration plants, fuel, starting equipment, and related apparatus)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Power conditioning systems (including uninterruptible power supply [UPS], switchboards/gear, power ingress, transient voltage surge suppressor [TVSS], and related apparatus)</td>
</tr>
</tbody>
</table>

The portions of a facility that can be regarded as the spaces that represent the “overhead” required by practice, business need, or code to be able to occupy and operate the facility

May include:

• Workspaces, staging areas, and network operations centers (NOCs)
• Storage areas and stockrooms
• Common areas
• Bathrooms, break rooms, and kitchens
• Reception areas
• Lifting equipment and people-moving apparatus
• Parking facilities
• Security and safety equipment and zones (including mantraps and protection layers), blast zones, and other similar capabilities and areas

Figure 2 below visually represents the relationships among the CFAs in the context of the cube introduced in Figure 1.
III. Defining Containerized/Modular Data Center Facilities

In contrast to a site-constructed data center facility, a containerized/modular data center facility (CMDF) separates some or all of the core facility areas described earlier into discrete, prefabricated components that are assembled at the target location. In many respects, this approach is more like the assembly of literal building blocks—where the right mixture and type of blocks, when assembled together, produce an operational facility that meets the requirements of the customer or operator—than the traditional fixed data center facility described thus far.
A CMDF is defined as:

“A set of one or more prefabricated modules that are transported to and assembled at a specific site and together provide the required payload capacity, while optionally providing the underlying power and cooling infrastructure supporting the solution.”

For the purpose of addressing common construction language, a CMDF is a set of one or more prefabricated and pre-engineered metal buildings (PMBs), along with any optional and required building infrastructure equipment (which may or may not be PMBs).

**TRANSLATING TRADITIONAL DATA CENTERS INTO CMDFS**

There is a clear distinction between traditional site-constructed facilities and CMDFs. A traditional build can have pre-designed components and repeatable elements (where the design or element is similarly built for more than one data center site). A CMDF module, however, is fully pre-engineered\(^2\) and prefabricated.

To illustrate the difference, an example of the first, more traditional approach would be buying a set of shed designs from a local hardware store, procuring the components, and then constructing the shed in a backyard. The alternative, CMDF example would be similar to buying a pre-built shed, dropping it into the backyard, and using it that afternoon. This is not to say that the pre-built shed (or CMDF) cannot be made to meet specific needs; it can potentially be designed and built per particular specifications. However, the distinction here is in the repeatability, the quality control, and the pre-engineering found with the CMDF, which can deliver deep technical and business value when properly applied.

After all, when constructing a traditional facility, the defects encountered and the efforts necessary to resolve them have limited application to the next facility and the next site. The next project will likely use a different workforce, different M&E expertise, different site customizations, and potentially different materials and construction methodologies. In a prefabricated world, the first unit’s defects can be addressed and resultant lessons applied toward the second unit as part of the manufacturing quality control process. Thus, in the CMDF domain, learning can be immediately and effectively applied to the next specific module. This speed is

\(^2\) “Engineering” in this context explicitly refers to the profession of the application of technical, scientific, and mathematical knowledge to design and implement the materials, structures, devices, and methods in order to realize the desired result or objective.
especially valuable given the rapid manufacturing pace possible when taking advantage of assembly-line efficiencies.

When looking at a containerized/modular data center facility, many if not all of the traditional CFAs described earlier still exist. A CMDF’s core areas can be described in that same manner, with the understanding that the end facility’s complexity will vary along with the particular CMDF solution’s level of maturity. The CMDF modules discussed below are direct equivalents to traditional CFAs, although most are likely to be prefabricated.

Additionally, there are inherent advantages to CMDF modules (of any type) that can be leveraged as part of the pre-engineering design activity. These advantages include:

- The integrity of the envelope can be predicted and engineered for efficiency and also to account for secondary requirements (such as high wind or projectile tolerances).
- The airflow and cooling systems within a module can be optimized from spatial, performance, and efficiency perspectives.
- Tighter management of set point and equipment inlet temperatures is possible, potentially reducing energy demand.

**Similar modular applications**

The modular approach, while seemingly novel within the data center industry, has been employed for other applications before. For instance, some operators use specialized facilities for specific purposes, such as for housing telecommunications equipment and mobile command stations. These solutions may be modular in that the payload is deployed within prefabricated shelters, trucks, shipping containers that are compliant with International Organization for Standardization (ISO) specifications, or similar modular form factors.

This modularized paradigm has also been popular in logistics-sensitive industries, such as government and military bodies, that typically need to be able to set up facilities in remote locations without the benefit of access to traditional construction approaches. Additionally, the modular approach has been popular in some manufacturing industries, where speed of deployment, componentization, and repeatability with minimal defects are key advantages. That said, the modular building legacy can also introduce difficulties with some jurisdictions that may have particular requirements that cannot be overcome when deploying a CMDF solution. (Please see the Additional Considerations section for more information on jurisdictional requirements.)

Historically, the modular approach has been largely limited to particular point applications. Yet CMDF architecture has become an increasingly viable and robust alternative when considering a data center build,
with multiple implementation approaches available from various suppliers in the industry. It is important to note that CMDF architecture presents unique challenges as well as opportunities, and the advantages and disadvantages of any deployment scenario merit careful consideration.

**CMDF MODULES**

A CMDF solution is comprised of one or more modules that together enable proper support of the payload. (See Table 2 below.)

**Table 2. CMDF module types**

<table>
<thead>
<tr>
<th>Module Type</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload/data hall modules</td>
<td><em>The portion of the CMDF solution that (at a minimum) houses the IT equipment to be operated at the facility and provides the direct cooling, power, and support equipment required for the space per the design and requirements of the payload, pursuant to code</em></td>
<td>Must include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Rack or rack space allocations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ IT equipment and ambient cooling or air distribution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Power distribution from the service entrance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ One or more of the services provided by an infrastructure module (such as heat rejection, power conditioning, or other services/capabilities)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ One or more of the services provided by an ancillary module (such as a vestibule/airlock or other services/capabilities)</td>
</tr>
<tr>
<td>Infrastructure modules</td>
<td><em>The portion of the CMDF solution that (at a minimum) houses facility support equipment such as heat rejection, mechanical cooling, power conditioning, and power generation as selected for the particular application and needs of one or more payload modules, geography, and code</em></td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Packaged air-cooled chillers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Water-cooled chillers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Cooling towers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Air coolers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Free-air economizers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Generators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Power protection/UPS plants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Cogeneration plants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Other facility infrastructure components</td>
</tr>
<tr>
<td>Ancillary modules and areas</td>
<td><em>The portion of the CMDF solution that (at a minimum) provides non-payload and non-infrastructure features and is not part of a fixed</em></td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Workspaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Vestibules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Access spaces</td>
</tr>
</tbody>
</table>

©2011 The Green Grid. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted, or stored in any retrieval system of any nature without the written permission of the copyright owner.
Payload modules

Payload modules can be designed across a wide spectrum of capabilities. On one end, a module may be designed to support IT equipment in racks, but it has no ability to directly reject the generated heat, does not provide any conditioning of power, and does not generate or store backup power. On the other end are payload modules that have built-in heat rejection and/or UPS capacity. Some may even have some degree of power generation capabilities.

In all cases, a CMDF payload module can be expected to have the power and cooling infrastructure needed to directly support the payload, such as rack-based or non-rack-based heat exchangers, fans, power distribution units (PDUs), and bulk power supplies. The module may also have fire-control equipment, security equipment, and other components as required to establish an operating condition and to meet the obligations of the authority having jurisdiction (AHJ). Thus, the payload module is very similar to a traditional data center’s white space, where cooling and power distribution may be within the space (regardless of the mechanism), but the nature of the specific solutions inside the payload module may differ from what one would select for a fixed facility.

In some configurations, the payload module may be fully self-sustaining, perhaps only requiring an outside power connection to provide all of the services necessary to support the installed IT equipment. Of course, adding additional capabilities to the payload module may affect capacity or present other tradeoffs. Thus, the selection of the scale and scope of a payload module may vary widely from organization to organization and from need to need.

A CMDF solution is comprised, at a minimum, of the payload module, which may or may not require other supporting modules or key services (such as conditioned power and chilled water) to be supplied by the site or through other modules.

Infrastructure modules

Infrastructure modules generally do not include any IT equipment other than the underlying controls and related systems necessary to support the operation of the infrastructure equipment itself and to provide any required interfaces for these operations (usually through building management protocols, such as oBIX,
BACnet, or MODBUS). Much of the infrastructure module equipment used in a CMDF approach can itself be modularized, or packaged, with varying degrees of self-resiliency and can be both prefabricated and pre-engineered. Form factors will vary widely depending on the vendor and the type of equipment. Infrastructure modules may be broken up into multiple segments that together provide a unified set of services for the payload module.

Alternatively, these segments may be combined into a single solution. For instance, an organization may use one pre-engineered and prefabricated module for its housing power protection, power generation, and chiller. The appropriateness of such a unified module largely depends on the total capacity required, with larger capacities being more likely to be delivered in multiple segments and assembled at the final installation site.

**Ancillary modules and areas**

With a CMDF design, some ancillary areas may be rendered unnecessary; their features may either be provided via other means or integrated in some way as features of a given module. For the latter, integration may include protection levels, such as blast or electromagnetic protections. Nonetheless, some ancillary modules or site remediation may be required, depending on local code and jurisdictional guidance as well as on some practical operational and project-specific considerations.

As with the prior module definitions, ancillary modules are both prefabricated and pre-engineered, and they may be described as having the features of vestibules, airlocks, various housing types, mantraps, security buffer zones, protection apparatus, etc.

Many CMDF deployments will involve a mix of ancillary modules, site work, and remediation. This is an essential point with modules—most (but not all) have site-specific requirements (such as concrete pads or mounting platforms), weatherization, or other needs. Not all of these prerequisites can be practically met with ancillary modules or the addition of new features to a module. Thus, all deployments necessitate some degree of site work performed by local or vendor-provided labor. That said, the level of site work required to support a CMDF deployment is generally lower than that of a fixed facility. After all, CMDF modules are generally designed with fairly limited site-remediation requirements. A fixed facility typically requires more extensive foundations, evacuation, and related work to be performed. Moreover, CMDF architectures can inherently reduce the amount of the overall wider site-executed work, because much (if not all) of the core electrical, mechanical, and envelope-construction activity is performed at the factory.
IV. Business Flexibility Considerations

CMDFs can help enable flexibility in how organizations purchase, deploy, and manage their IT, infrastructure, and facility assets. This section highlights some of the potential opportunities and issues to be considered when evaluating CMDFs.

OWNERSHIP MODEL

There is no “one-size-fits-all” model for how an organization can make the best use of its resources in the provisioning of data center capacity. As with conventional data centers and hosting markets, it is expected that a number of different ownership models will appear that make use of CMDFs. Just like with any asset purchase, lease, or outsource opportunity, each organization should consider the impacts of operating expenses and monthly recurring charges versus capital expenditures and depreciation cycles. For example, a traditional raised-floor data center may be depreciated over 15 or 20 years, whereas a CMDF may be depreciated on the same schedule as the servers it houses. The following subsections discuss three CMDF ownership models for an organization to consider as a part of its overall financial plan.

Ownership of both the CMDF and the IT equipment

This is a conventional model where an organization owns both the CMDF and the IT equipment within it. While servers would likely be depreciated the same as in a traditional data center, the CMDF may be depreciated as a building, as IT equipment, or somewhere in between. The module may be installed at either a commercial or purpose-built facility that the organization either owns or leases.

Partial or complete leasing

It may make sense for an organization to lease a CMDF from the manufacturer, especially when the organization anticipates adding servers to the module over time rather than deploying a fully populated CMDF at the start. This option may lessen the initial financial impact. Some organizations may prefer to pay all IT expenses as a monthly recurring charge to limit capital exposure and maintain a more consistent cash flow. Alternatively, owning the module and leasing the IT equipment may be well suited to hosting or co-location organizations that are interested in developing facilities specifically for CMDFs and leasing servers or capacity directly to customers.

Cloud and SLA-based IT capacity

When IT resources are fully outsourced or virtualized to cloud and hosting providers on an SLA basis, there is an opportunity for those hosting providers to begin leveraging CMDFs to potentially obtain a competitive cost, feature, or other advantage. In this case, the CMDF is abstracted from the customer organization, just as a
physical server is abstracted from the end user in a virtualized environment. Another option for organizations is to continue to host their IT equipment in conventional data centers but use hosted CMDFs for cost-efficient, SLA-based business continuity and disaster recovery (BCDR) solutions.

**DEPLOYMENT**

For some organizations where IT resources are deployed at a large scale, the ability to simply deploy entire CMDFs pre-racked with configured servers can be an attractive option. This practice gives the organizations not only faster time to market, but also faster beneficial use of their data center infrastructure investments in power and cooling, which makes for a faster return on their invested capital.

Organizations with scale-out applications—such as cloud computing, Internet search, and high-performance computing clusters—have historically constructed data center facilities and then filled them with either discrete servers or discrete racks of servers over time. In this model, an organization must wait until the data center is ready and could spend weeks installing and configuring hundreds or thousands of servers. In a CMDF model, those same servers could be installed and configured at the factory, and the CMDF could then be deployed to the organization’s site and possibly be online in a matter of days. For large-scale data centers that often cost in excess of U.S.$100 million, this could mean obtaining beneficial use months early and getting quicker business value from the depreciating facility.

Additionally, an organization may experience significant generational changes over the life of a data center facility. For example, the first servers deployed in a new data center may rely on air cooling and chimney cabinets. Five years later, the highest-performing and most economical cooling solution may be a water-cooled cabinet. Provisioning for both of these possibilities in the initial data center design may be prohibitively expensive. Using a CMDF model, which bundles the cooling methodology with the servers, helps support generational changes and effectively allows the organization to procure equipment based on best performance and efficiency, with less regard to legacy environments. When generational changes occur or even when additional power or cooling capacity needs to be provisioned for a facility, an organization can address its needs through a CMDF, which has a much lower impact on existing systems than a conventional data center environment, where scheduled outages or complex construction sequencing may be required.

**PROCUREMENT**

One of the biggest factors to consider in the deployment of a CMDF is whether an organization is purchasing a fully populated module (with hundreds or thousands of servers) or simply purchasing an empty one and then installing servers discretely. In many cases, it may be advantageous to spread the cost of the module across many factory-integrated servers from the outset.
Another consideration is whether multiple manufacturers’ servers or IT equipment will be installed in the module over its lifetime. While most module manufacturers have the ability to support nearly any industry-standard rack-mountable server, each manufacturer tends to optimize and tailor its module for its own systems. In some cases, a module’s form factor may not allow the use of any other manufacturer’s equipment. It is important to know whether there are any vendor lock-in issues when selecting a particular module manufacturer or model.

RELIABILITY

It is important to review and understand how the power and cooling systems in a CMDF and its supporting systems are architected (both individually and in aggregate). A given module can be every bit as intricate as a conventional data center, and, in some ways, it can be more so. When an organization/architects a CMDF solution in conjunction with a proper and mature view of its IT architecture, it can better align uptime requirements with business demands.

For instance, an organization may choose to procure multiple payload modules with different resiliency and uptime features, with the intent of moving applications that require lower uptime targets to the modules that are designed for those lower targets. Conversely, the organization may move applications with higher uptime targets to highly available CMDF platforms or to a traditional high-availability facility. In many ways, a well-architected CMDF solution can make it easier to deploy platforms and applications at granular uptime target levels.

The ability to acquire and decommission capacity in modular chunks has another potential advantage in terms of uptime and failure risk. When properly designed, the CMDF architecture can reduce the footprint of possible failures to individual modules and to a more granular level if the design permits. That said, there are limitations, especially with modules whose cooling platforms are based on chilled-water supplies. Many modules that rely on chilled water for cooling with module-level or rack-level coils may have limitations in their ability to serve more than one chilled-water loop into an individual air handler/cooling unit. Thus, how an organization addresses the need for higher uptime requirements for a particular design in a CMDF scenario may differ from the redundancy and resiliency approach employed in traditional builds. One may expect to see different testing levels and more emphasis on mean time between failures (MTBF) in a CMDF module. (For a more in-depth discussion, please see Appendix A. Understanding Reliability and Resiliency.)
SUPPORT MODELS
A CMDF deployment can enable new support models when compared with traditional data center spaces. If an organization receives the module, racks, IT equipment, and power and cooling systems from the same manufacturer, this packaged solution may provide one point of ownership for warranty, maintenance, and service demands. This unification can simplify overall support for the solution. Whether a hard drive has failed or a temperature sensor is giving faulty readings, a single phone call can potentially dispatch the right technician to fix the problem. An organization may alternatively opt to implement a fail-in-place support model, where it runs a module until some percentage of the servers have failed, at which point it swaps out the entire module, servers and all.

However, CMDF operators should think about how a potential support model particularly relates to any day-to-day, hands-on server work required. Many payload modules have significant limitations in the working environment in terms of space and comfort constraints. This may present difficulties for a technician who needs to stand in front of a server for long periods of time installing software or troubleshooting. The ability to remotely manage, image, and troubleshoot servers is highly desirable in a containerized environment. In many ways, a CMDF module may inherently enforce a lights-out, mature services approach. Organizations that are unaccustomed to this type of mature IT operations practice may find the transition to a CMDF difficult, or they may simply rely on the CMDF’s deployment to impose new operational disciplines on their IT workers.

FACILITY IMPACTS
A CMDF may also be used to expand data center capacity in existing facilities in which all of the IT areas are full but stranded power and/or cooling capacity remains. For example, an organization that has a few hundred kilowatts of power available from a utility feed or UPS may benefit from deploying a module outside its facility and simply connecting the module to existing support systems. In those cases, it is important to understand how much power and cooling is available and what level of reliability and quality those systems provide. In the best-case scenario, an organization may have spare UPS and chilled-water capacity available from the existing facility, which could be used by the module. In another scenario, all UPS power may be consumed, but additional non-critical (non-UPS or generator-backed) power is available that may allow for a low-reliability module to be installed. Or a higher-availability module may be deployed with the addition of a UPS (and perhaps other systems).

In facilities that lack sufficient power, cooling, or available redundant systems capacity, it is important to note that additional electrical distribution, UPS, generator, chilled-water, and other systems capacity may need to be procured and constructed in order to support a CMDF at the level of reliability required by the organization.
REAL ESTATE CONSIDERATIONS
Many organizations currently house their data centers in relatively expensive office buildings where departments compete to expand both their personnel and computing resources. In these scenarios, organizations could lessen the space constraints on departments by moving the IT equipment out of the “people space” and into a CMDF located in the parking garage, on the roof, or in a utility yard. One of the bigger advantages offered by a CMDF is that it can be deployed in a wide variety of field conditions, which can free up land or space for demands that require more valuable resources.

MOVING CMDF MODULES
Transporting a CMDF module raises new opportunities, along with some questions and challenges to consider. In an effort to mitigate the failures that can occur “on the road,” it is important to understand to what level a particular module design has been engineered and tested for regular or occasional movement. In one instance, the server or storage refresh cycle could be used to redeploy data center capacity to a new or different geographical location. For example, when the servers or storage units within the CMDF reach the end of their depreciable lives, the entire unit could be shipped back to the manufacturer, where the equipment would be recycled in compliance with local regulations. The module could then be refurbished, repopulated with new IT equipment, and redeployed to the organization’s site at a lower overall potential cost than purchasing a new module.

V. Financial and Planning Considerations
The data center industry has long accepted the benefits of modularity in IT design as a mechanism to allow hard-pressed CIOs to deliver capacity that is closer to the demand curve, as opposed to maintaining large underutilized and expensive capacity. A CMDF approach to the expansion and contraction of data center capacity is a logical extension of the proven modularity concept and offers, arguably, an even richer financial benefit.

This section is not intended to be a critique of the traditional data center approach. Rather, it is useful to look at some of the financial concerns involved with building a conventional facility as background before discussing the benefits of the CMDF model.
Figure 3. Understanding the traditional IT capacity demand curve

Figure 3 illustrates a reasonably typical IT capacity demand curve for a data center and the estimated build projects required to keep pace with this demand. While conventional construction can leverage some degree of modularity, helping to more closely align a given facility’s with the organization’s demand curve, one typically would pre-provision large, expensive items such as land and buildings (and to a lesser extent, physical plants) to deliver economies of scale. The key issue here is that the data center only becomes truly efficient when the facility is at or near capacity. For long periods of time, the organization is maintaining a deprecating, underutilized asset in a belief that this will mitigate the risk of the facility being unable to accommodate increased demand or short-term load spikes.

Similarly, undercapacity can become an issue. There are periods of time during which demand exceeds capacity, and these may trigger a new build project. However, under the traditional model, that build project will take a significant amount of time, increasing the potential impact of the undercapacity. Thus, organizations either shift the demand to potentially more expensive outside hosting capacity or suppress the demand, which can affect business performance.
Another significant concern is what to do with data center facilities when demand declines. This may be a very real risk for IT managers as virtualization and other technologies moderate demand and changing economic cycles affect industries differently than historical records would suggest. Organizations can minimize the financial bets they make regarding demand by establishing a unit of data center capacity that can be deployed or decommissioned “just in time” as opposed to building a wholly new facility. Doing so also can reduce their dependence on predicting future IT demand, or simply shift and operationalize data center capacity to align with the same provisioning and operational lifecycle as the IT assets they support.

Figure 4. Understanding the CMDF demand curve

Figure 4 above illustrates the difference between the traditional lifecycle and one that is facilitated by the CMDF approach. It shows that the CMDF approach can better align data center capacity with demand. That said, a CMDF is most appropriate for organizations that can leverage the lower capacity chunks fairly quickly. For some, a 20-foot module with perhaps six to eight racks might still be “too much” capacity. Matching the CMDF or an alternative solution to organizational capacity needs is always the preferable approach. Even more preferable would be to design and scale the overall IT solution used by the organization to minimize the need for more capacity—after all, if one is more efficient in the use of IT assets, there may be less of a need to procure and deploy facility capacity to handle any avoidable demand.
## ADDITIONAL FINANCIAL BENEFITS

Deploying the CMDF architecture can provide additional benefits for many organizations, as highlighted in Table 3 below.

**Table 3. Further financial benefits of the CMDF approach**

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital costs</td>
<td>A CMDF approach may deliver similar compute capacity as a traditional facility but at significantly lower capital investment costs. A major portion of this benefit stems from the use of higher-density IT equipment that requires less space and consequently less construction. However, the reduction in cost can also be realized from the deployment of just-in-time capacity instead of overcapacity, as well as from savings in local construction and labor costs.</td>
</tr>
<tr>
<td>Energy costs</td>
<td>Most CMDF designs are optimized for energy efficiency. Their heat loads typically are closer to their cooling coils, generally require smaller volumes of air, and are designed to tolerate wider temperature and humidity bands. Also, some CMDF vendors are minimizing fan load and power conversions through design innovations such as by using bulk fan and power distribution systems. All of these efficiencies translate into lower energy costs for power and cooling and should be examined in detail. When comparing one similar solution platform with another, the use of The Green Grid’s partial power usage effectiveness (pPUE™) metric can result in a more accurate, informative assessment.</td>
</tr>
<tr>
<td>Capital efficiency</td>
<td>The just-in-time approach to provisioning that is afforded by a CMDF model means that organizations can begin to support new projects and businesses with less capital commitment than is required for a traditional data center. The fungible nature of CMDFs also lends itself to lease financing, which can be an effective way of preserving cash liquidity for the organization.</td>
</tr>
<tr>
<td>Operational costs</td>
<td>Between lower energy costs, optimized maintenance procedures, and reduced depreciation costs per unit, an organization should expect significantly lower overall operational cost per unit of IT.</td>
</tr>
<tr>
<td>Time to market</td>
<td>The financial costs and risks of committing to a multimillion-dollar data center build can be mitigated by a CMDF approach due to the granular nature of its deployment. Organizations often want to prove a new business model or test a region without affecting capacity for their traditional business.</td>
</tr>
</tbody>
</table>
Some CMDF vendors offer pre-integrated servers, storage, and network components. Deploying a fully integrated CMDF can reduce labor cost if the integration tasks are performed in a cost-optimized factory environment rather than relying on local labor. Another benefit may be in the reduction of errors and the need for problem resolution during installation because the work can be executed and tested in a repeatable, manufactured manner by personnel who are experts in working within CMDF spaces.

Installing a fully integrated CMDF can reduce the risk associated with performing integration activities in an operational data center. Additionally, the deployment of CMDF modules themselves can have significantly reduced risk through higher expected quality and pre-engineering, which can reduce the potential for site-level remediation and “punch list” repairs.

A CMDF can be considered a module of IT capacity that will be decommissioned/replaced in its entirety. This will allow for repair refresh with minimal resources and minimal risk to other parts of the IT operation. Similarly, a CMDF module can have significant residual value. The redeployment or resale of the asset may be easily accomplished, or the leasing rates may be lower in contrast to alternative approaches.

This is to say that a CMDF approach can enable the facility itself to participate in a lifecycle not dissimilar to that normally attributed to IT equipment, though with a longer useful life and capacity for repurposing. Individual modules may have different lifecycles and can be replaced or reallocated fairly easily in contrast to fixed facility equipment.

It is important to note that when looking to put a value on energy savings for a given project, power usage effectiveness (PUE™) is a coarse metric and a lower PUE does not always mean lower costs. A cost analysis must account for both the solution’s PUE and its total consumed power. PUE is useful for trending performance in a single instance but not as useful in comparing different solutions. Only partial PUE (pPUE™) should be used to compare an individual CMDF module with a similar alternative, and even then, the measurements used to calculate the pPUE scope must be materially the same.

VI. Additional Considerations

FIRE DETECTION AND SUPPRESSION

Since CMDF deployments provide physical isolation of groups of components, they have an inherent impact on fire containment. The modularization of data centers enables fire to be more readily contained and reduces the potential for fire spread and smoke damage. CMDF units have an even greater ability than traditional data centers to smother fire with all systems/vents shut and can prevent or retard the spread of fire from a CMDF.
outward or from the outside inward. This isolation may allow the module to be reused/refurbished in a relatively short time period following a fire at the site. This should not be construed to imply that all CMDF deployments are fire proof or fire safe, just that they have inherent containment built in, although some CMDF vendors do offer fire-rated containment. To be clear, careful planning is always a requirement when looking at any aspect of fire safety for any facility, whether deploying CMDFs or not. Many of the requirements around fire protection can be influenced greatly by local regulations and practices.

**AHJ TREATMENT AND CERTIFICATION**

One of the most important factors when deploying a CMDF module is to understand who has the jurisdictional authority to approve use of the unit. The AHJ might be a local building inspector, a safety committee agent, a fire marshal, or some combination of people fulfilling these roles. The AHJ needs to sign his or her name to a document declaring the deployment safe to operate; the document should account for electrical and fire safety as well as access and other requirements.

Special care must be given to how CMDFs will be treated by a given AHJ. Some jurisdictions might look at a CMDF as a building and apply building code criteria. Alternatively, some AHJs might consider it a device and look for a rating, label, or stamp from a nationally recognized testing laboratory (NRTL) such as UL. Requirements will vary by locality. However, *it can and should be presumed that local authorities will largely apply building codes to at least some of the CMDF module types.* As a general practice, The Green Grid recommends taking a pessimistic stance toward AHJ risk, planning for wide compliance requirements regarding the overall CMDF solution, and seeking the capability to meet those requirements in every individual module.

For instance, the decision as to whether or not a CMDF is “habitable space” will have an impact on whether the local AHJ applies Occupational Safety and Health Administration (OSHA) rules or other human safety regulations. It is important to consider access and working conditions inside CMDFs as well as between them and around their exteriors. Never assume that the local AHJ will see the situation a certain way without consulting it first. CMDFs are new and unfamiliar to many safety inspectors; it is their job to be cautious and conservative in the name of human safety. It is highly advisable to work closely with the AHJ during the planning cycle for a CMDF deployment. While AHJs typically look for certifications that they can rely on—such as UL listings or National Electrical Manufacturers Association (NEMA) ratings—there are no active listing classes available for a whole CMDF payload module. Since such certifications are not available, some extra education time and documentation may be required to get AHJ approval. When selecting a supplier, it is important to consider if it will perform customizations to address specific AHJ concerns on a module-by-module basis.
One particular aspect of AHJ concern is electrical safety. Since CMDF modules are factory produced and pre-wired, the inspector will want to know that the work was done according to code. For some AHJs, documentation will help or completely address this concern. That documentation may be in the form of an NRTL listing, labeling, inspection reports, or related materials. In each case, there will typically exist a certification declaration and a detailed report that includes sufficient information to answer the questions of an electrical inspector. Clear and complete documentation will also help with answering questions about any local ordinance variations to electrical code. When planning a CMDF project, pay close attention to the vendor’s documentation, certification, and related services that specifically address the geography in which a module will be installed. Some AHJs will still require a physical inspection once the module is at the installation site, so be sure to consider how easy it is to access electrical and mechanical distributions within the module in case an AHJ representative should require access.

A given CMDF module vendor should be able to provide documentation supporting the path to compliance in particular major jurisdictions. This includes architectural and engineering elements, such as compliance with:

- International Building Code (IBC) and local derivatives
- International Fire Code (IFC) and local derivatives
- International Mechanical Code (IMC) and local derivatives
- National Fire Protection Association (NFPA) 1, 101, 5000 and other codes (and local derivatives)

Some jurisdictions may require a fire-protection rating and certification. This is especially true for deployments that involve placing modules near each other or near another structure. Doing so may prompt what are known as setback requirements. Whether or not the proper fire-protection ratings are in place will directly influence the setback requirements placed on the project by an AHJ.

Another consideration is ensuring that a CMDF is not contaminated by intrusion of water or blowing debris, which is usually addressed by the specification and build with regard to an appropriate NEMA or Ingress Protection (IP) rating level. It may be important to the organization as well as the AHJ to have a certain rating level for some assurance that the CMDF will be safe to operate in various weather conditions. Since a module may need to be opened to the elements for service, this rating may be different for service than for normal operations.

In some areas, data centers are held to emissions limits to help avoid electromagnetic interference (EMI) with devices operating in surrounding businesses and homes. These types of limits are sometimes statutory and are often written into an area’s codes of conduct. A given CMDF module may also be required to be certified or tested to demonstrate that it does not inject electrical disturbances back into the power grid. This is typically
done in IT equipment as part of an NRTL listing, but modules may not be NRTL listed even though they contain all NRTL-listed equipment.

**SUPPLY CHAIN**

There are unique supply chain issues to consider when deploying CMDFs. The industry for fully integrated CMDFs is fairly new, and some suppliers are less experienced than others. It is difficult to switch from one vendor to another. Traditional equipment providers can be cast into the role of integrator. It should be clear what level of support capability is available at all stages of the CMDF lifecycle: design, delivery, deployment, operation, repair, refit, and removal. Further, seeking a CMDF vendor to partner with should involve aligning all of the expertise and capabilities required for the finished deployment, including architectural, engineering, construction management, and contractor roles. Leveraging vendors’ relationships in these areas may prove advantageous.

**CORPORATE IMAGE**

It is important to consider the public image associated with a CMDF, which can be perceived as a leading-edge method for deploying a data center. Accordingly, such a deployment can generate publicity, but this publicity can be both positive and negative. Being viewed as a forward-thinking or trend-setting organization can be advantageous, but any outage would become a highly visible event that can tarnish an organization’s reputation. This perception risk may be higher than an outage in a traditional data center, even if the actual risk of an outage is lower in the CMDF deployment.

**RELIABILITY**

The manner in which CMDF modules are deployed will depend upon a number of key factors, including an organization’s requirements, the applications that will run within the environment, the module’s geographic installation location, and the weather at the deployment site. These, along with a number of other variables, will greatly influence the realized reliability of the CMDFs deployed. Table 4 below lists some common reliability concerns and provides an overview of the impact to CMDF deployments for each.
<table>
<thead>
<tr>
<th>Concern</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDFs have single points of failure</td>
<td>The degree of resilience, redundancy, and uptime applied in the design and deployment of a given CMDF module will vary greatly. Many payload modules, for instance, use single chilled-water distributions. That said, electrical and network services can generally be provided in a redundant fashion and the module ordered accordingly. The impact of a single chilled-water distribution may not be substantive even in environments where very high uptime is a requirement. Proper design—such as the addition of valves and bypasses necessary to support multiple chilled-water plants, as well as appropriate placement of shutoff valves to facilitate coil or other mechanical replacement—may provide an acceptable path to operational sustainability. Any engagement to determine and deploy a CMDF solution should include a thorough ROI and MTBF analysis.</td>
</tr>
<tr>
<td>CMDFs may be less secure than brick-and-mortar facilities</td>
<td>CMDF modules can be made to be as secure as traditional brick-and-mortar facilities through the use of heavy locked doors, badge systems, and alarm systems. Some organizations also may choose to install fencing around their modules, hire security guards, or use other similar measures to protect their CMDFs. In fact, in most cases, it is easier and less expensive to construct a secure CMDF than to design, build, and secure a large, fixed data center facility. Protecting the module from EMI or electromagnetic pulse (EMP) events, or from ballistics impacts, is arguably far easier and less expensive with CMDF modules because of the availability of the necessary panels and remediation components and the nature of CMDF construction itself. Other physical security concerns include fire, severe weather, earthquakes, and damage by a large vehicle (e.g., truck or crane). With an effective disaster recovery plan and CMDF design, an organization may be able to migrate its workload to other modules or sites while the CMDF vendor works to repair catastrophic issues. Often, CMDF vendors can ship another fully loaded and configured CMDF to a site that experienced a disaster.</td>
</tr>
</tbody>
</table>
Shipping reliability may be lower than with a traditional approach

<table>
<thead>
<tr>
<th>Shipping reliability may be lower than with a traditional approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depending upon where the CMDF is deployed, available transportation methods can include trucking, shipping, and aircraft transportation. (Rail shipping is a rare and problematic method.) Each of these modes of transportation will necessitate a different set of design requirements that cover, at a minimum, shock and vibration profiles, temperature ranges, humidity ranges, salt fog susceptibility, and structural integrity.</td>
</tr>
<tr>
<td>The vendor’s design should address shipping considerations. For instance, in the case of shipboard transportation, vendors should design the CMDF module to withstand significantly rough port handling, stacking, and the use of special shipping environments such as “roll-on, roll-off” (RORO) transport decks. Similarly, CMDF modules sent to developing nations should be designed to travel on the roads there, which tend to be rougher.</td>
</tr>
<tr>
<td>Reliability considerations will be substantially different if the CMDF is shipped fully loaded with IT equipment than if shipped empty. If shipped fully loaded, care must be taken to assure that the CMDF has been designed for the fully loaded weight and for appropriate shock resilience.</td>
</tr>
<tr>
<td>(See Transportation Considerations below for more detail.)</td>
</tr>
</tbody>
</table>

At a minimum, the following environmental variables will also require consideration:

- Temperature range
- Relative humidity range
- Rain, wind, and snow exposure
- Extreme weather such as tornadoes, hurricanes, gales, etc.
- Earthquake risk
- Fire risk

Sheltering the CMDF, or otherwise retrofitting the module, can address a number of the exposure items listed above. For instance, in the case of earthquakes, the CMDF can use isolation mounted racks or be placed on a seismic isolation pad. Some CMDF modules will have some of these remediation capabilities built in, although this may result in higher overall realized costs if a feature is not actually required. An organization implementing a CMDF solution will want to work closely with its selected vendor to address these issues early on.
TRANSPORTATION CONSIDERATIONS

In a CMDF approach, the modules are characterized by being initially transportable. Most types of modules can be fully manufactured in one place and deployed in another. In some cases, a module can also be moved after its initial installation for redeployment to a different location or for renovation or decommissioning at the end of its useful life.

A CMDF built according to ISO container specifications can be easy to transport using common freight methods. As long as ISO dimensional standards have been met during the construction of a CMDF, permits (if at all required) are straightforward to obtain. If structural features have been added to the outside of the container that add to its external dimensions, there might be a requirement for special permits due to road-width or load-length limitations. Careful consideration must be given to whether the CMDF should be shipped with IT equipment included. Similarly, modules built to have wider dimensional attributes than those allowed under ISO may be supported for most ground and sea transportation methods. Caution should be used when buying larger modules if they will be transported outside of their country of manufacturer. It is critical to understand transportation size limits for the entire transit path to the specific site to determine what is and what is not permitted.

Transport by rail is feasible but can subject modules to a high degree of shock and potential damage. Rail shipments require trucking to and from depot points, and rail shipment is subject to specific scheduling, which might add extra cost and time. Plus, shipping via rail may not be supported by a given module vendor and may void warrantees.

Containers are frequently transported on ships using two methods: cargo holds or RORO decks. These decks are used for special handling either when containers have been modified from ISO specifications or when they must be handled differently due to the value of their cargo. CMDFs transported by ship usually take advantage of RORO decks.

ISO containers that are 20 feet long and only 8.5 feet high are readily air-shippable to and from major airports worldwide. Flights are typically available once or twice per week. Some air shippers have specific requirements for CMDFs that hold “dangerous goods” such as fire suppressant gas or containers. The difference in cost for air transport is usually modest, and air transport is much quicker than any other form of international transportation. However, weight limitations and per-pound costs have to be carefully evaluated.

Any CMDF transported across national borders will potentially be subject to customs restrictions. Some CMDF manufacturers have made it easy for inspectors to enter CMDFs and have gone so far as to prepare shipping
books that explain in detail the contents of a CMDF. It might also be necessary to facilitate a customs inspection, which would mean that the module’s doors would need to be operable during the shipping process.

For any of the above-mentioned shipping methods, a key consideration is weight balance. To move containers safely, they must be relatively evenly loaded. Special care might be required if the CMDFs are internally asymmetrical.

For local movement within a facility, containers can be mounted on wheels or roller units; there are many such systems available for purchase in the robust market for container add-on products. Smaller containers may be easily moved with an appropriately sized forklift. It may be possible to move larger containers with a pair of forklifts—one on either end operating in tandem—if proper consideration is given to balance, weight, and other factors.

Modules built to the ISO container specification have top and bottom corner fittings that allow for lifting. Using a crane to maneuver a container into place is a common practice, and there are rigging companies available throughout the world to perform this service. The process is similar to lifting HVAC equipment into place in traditional data centers. In extreme situations, a helicopter can be used to lift containers into place. However, helicopters have very low weight tolerances and using them may only be practical in limited cases.

**SITE-SELECTION CONSIDERATIONS**

The use of CMDFs adds new dimensions of opportunity and consideration to the site-selection process. There are both site-selection considerations (where the facility is located geographically) and site-placement issues (where, within the total available land or facility, the CMDF is located).

Modules can be located outside the walls of a building or in the open with no facility roof overhead. This allows the use of space that might not otherwise be considered as usable space, but it can also impose some restrictions. Outside deployment support and service may be challenging when weather does not permit open-door access or easy movement of personnel and equipment to and from a CMDF module. On the other hand, outdoor placement can make water- or air-side economization methods easier to deploy and to service. Movement of personnel is an issue even in good weather if the CMDFs are not placed on solid ground or in a zone that might be free of accumulated snow or blown debris. Outdoor placement makes the structure of the CMDF a critical factor in terms of its ability to withstand stresses caused by wind, sun, precipitation, thermal fluctuation, smoke or particulates, and extreme weather events. CMDF modules can typically be placed indoors as well.
The ability to place CMDFs in relatively small spaces, outside, and in remote locations presents new opportunities for locations in which data centers can be deployed. However, traditional considerations are still important. When contemplating a remote location, one needs to carefully consider the cost and time constraints on service access and the ability to use local trade services. The availability of emergency services also requires careful thought and planning. Emergency planning involves issues of personal injury but also planning for major emergency events such as wildfires, earthquakes, tornadoes, and other random events. Remote locations can be targets for theft or vandalism. Security measures, including remote alarms or monitors, require careful consideration. Even ballistics risk can exist for some deployments where openly visible modules are often used for target practice—the ability to withstand a bullet impact may be an important feature.

As with any data center facility, the availability of power and cooling services is vital for CMDFs. This is no different than with traditional data center deployment models except that CMDF modules as a group tend to have relatively high power-density levels per square foot. Modules are usually self-contained, which makes them natural defined zones of resiliency. However, that should not prevent the addition of internal resiliency zones within a given CMDF module.

When considering site selection, an organization should also determine if it needs to provide a secure electrical grounding connection. Local ordinances and regulations should be checked and best practices applied. If a pad area is built for a CMDF module, then ground connectivity should be part of the design. In some areas of the world, there are special requirements due to particular ground and soil conditions.

If a CMDF module is to be located outside of a building, there may be the requirement for electrical, network, cooling, and other infrastructure to be trenched underground directly or in one or more conduits. Trenching projects can be complex and expensive and therefore merit careful consideration. Along with any project requiring an external pad will be the need to consider and account for the pad’s drainage requirements.

Whether a CMDF’s location is inside or outside a facility, it will be important to consider the load-bearing capacity of the surface on which the module sits. One must take into account the fully populated, maximum load of the module and any extraordinary loading that might result from installing or removing the unit. It is also important to consider the weight of the infrastructure equipment that may be attached to the CMDF module. Infrastructure equipment could be distribution pipe or any other electrical or mechanical infrastructure connected directly or indirectly to the module or placed in the same structural area. If there is a plan to stack modules, the total maximum weight needs to be taken into account, including any access infrastructure such as elevators, lift platforms, and catwalks.
Since CMDF modules are typically removable, consideration needs to be given to installation and removal logistics. These logistics may include access for cranes, trucks, forklifts, jacks, or heavy equipment dollies along with necessary free space and enough turning radius to bring a module in or take it out.

To optimize spatial efficiency, an organization should carefully consider a module’s placement, not only regarding service access corridors between modules, if needed, but also the best layout of infrastructure modules versus those that only carry payload. The layout of these various modules may have an impact on the resiliency of the overall data center design.

Local zoning rules as well as organizational requirements should be investigated to see what may apply in a given deployment case. For example, some instances involve requirements for a CMDF’s visual appearance; fences or landscaping may be required in order to conform to regulations, practices, or organizational guidelines.

There are some additional challenges in the CMDF approach to consider, however. When pre-engineering a module, one makes assumptions about key environmental profiles that the module may be exposed to. These can include:

- Solar intensity and daylight hours
- Wind speeds and wind risks (e.g., hurricanes and tornadoes)
- Precipitation levels and mixtures (e.g., rain, ice, and snow levels)

In typical purpose-built construction, the facility is designed largely for the specific location where construction is to take place, and thus its design accounts for the three factors above. In the CMDF approach, each module is designed to a particular set of values for each of these factors, which may be overkill or inadequate for a given site.

Therefore, the CMDF solution proposed for a given location must be evaluated for local site condition factors and how they affect:

- Energy efficiency
- Efficacy and resiliency of the cooling and power systems
- Operational sustainability

Furthermore, the selection of particular modules in a CMDF solution may vary according to site conditions. An organization may select an alternative to the cooling module to take advantage of, for instance, local free-
cooling conditions. In other circumstances, site remediation may be needed, such as locally installed sun-shading platforms to reduce potential solar load on a module.

ENVIRONMENTAL ISOLATION CONSIDERATIONS

When one designs and constructs a purpose-built, traditional structure, the building will contain several layers, such as an outer shell, doors, hallways, inner doors, and rooms. When looking at CMDF modules, especially the payload module, consideration should be made to ensure that environmental isolation issues, where valid, are addressed as part of the overall solution. For example, if one deploys a payload module outdoors, some degree of isolation may be necessary so that when the doors are opened, the internal environment is not substantively affected by conditions outside.

The importance of environmental isolation will differ widely from circumstance to circumstance. For instance, if an organization deploys a CMDF payload module in a mild climate with minimal precipitation, and the module is only entered for occasional maintenance events, then the exposure to the outside environment may not be much of an issue. However, if the CMDF payload module were placed where the local climate varies greatly (or where there may be extreme hot or cold periods), where there may be considerable outdoor pollutants or dust, or perhaps where precipitation is fairly common, then this issue may be significant enough to justify ensuring that the module has (or can be otherwise provided with) the necessary degree of isolation, such as with an airlock, vestibule, or “mud room.”

ENERGY EFFICIENCY CONSIDERATIONS

As discussed earlier in this white paper, the CMDF approach enables the use of prefabricated and pre-engineered modules. The process of pre-engineering, when applied appropriately, can result in more efficient and repeatable designs. In effect, end users can (and should) demand that the modules that are selected for the given solution are:

- Highly efficient when measured against alternative designs and approaches
- Highly efficient when used for their intended purpose(s)

This implies that each module should be:

- Highly efficient as a component of the solution (individually efficient as expressed by pPUE)
- Highly efficient when aggregated into the overall solution (as expressed by PUE and by total energy consumption)

Another important factor to consider when looking at the long-term energy efficiency of a CMDF deployment is the ability to more easily introduce newer and more efficient modules or components of modules as part of an
ongoing refresh cycle. Assuming the selected CMDF module is designed to allow exchanges and upgrades of equipment, it may be easier to swap or upgrade a module than a traditional facility. These upgrades can further be aligned to IT refresh cycles, enabling both more efficient facilities and IT architectures to be deployed as they are adopted.

There are complexities as to how a given CMDF solution or individual CMDF module performs (or will perform) and how this performance may be contrasted by other components. Therefore, it can be difficult to directly compare one solution with another solution on equal footing.

Among The Green Grid’s goals for its efforts around PUE metrics is to help make it easier to understand the PUE, measurement how the PUE value was calculated, and if that PUE applies to a given module or to the entire CMDF solution. If looking at a CMDF module that is entirely self-contained—meaning that it provides all of the power and cooling services needed for supporting the payload installed within it—PUE is an appropriate measure. However, if only looking at an individual portion of the overall CMDF solution—one module of several—then the pPUE metric is far more appropriate.

The Green Grid’s pPUE metric can be used to compare, in an apples-to-apples fashion, the energy use within a common boundary, such as a payload module. Regardless of which boundaries are used, the most important factor is to ensure that the measurement is comparable when evaluating different solutions.

SECURITY CONSIDERATIONS
A CMDF located outside of a facility (or inside a facility but in an unusual location such as a warehouse) should have a defined security zone, just like traditionally located IT assets in a fixed facility. Access control, live video feeds for monitoring, and other aspects of a security architecture deployment should be taken into account, noting the constraints and advantages that a CMDF offers. Modules will likely have a different overall security design than a fixed facility. The new CMDF context may necessitate some reconsideration of typical deployment architectures as standardized within an organization. For instance, all of a module’s edge security devices likely will have to withstand exposure to external environmental conditions.

In determining a CMDF’s basic physical protection, an organization first needs to consider the nature of the content being stored in the payload module and the value of that content (in terms of both stored data and business risk). Organizations must develop a good security protection plan for the assets, data, and network connectivity in the CMDF environment.

To illustrate, a CMDF security zone might include:
- A perimeter fence roughly 50 feet outside of all dimensions of the installed modules
- Crash barriers to prevent a car or truck from intentionally or accidentally hitting any CMDF module or affecting the service equipment placed onsite
- A high-height security perimeter fence
- Single and/or two-stage badge readers, used as one enters different security zones
- Cylinder-controlled locks on gates and doors to permit or prevent entry into a security zone or between zones
- Zone-based, high-definition cameras with infrared and analytics-enabled backend recording and monitoring
- Outdoor security lighting
- Guards
- Similar other measures

The CMDF’s network cabling must also be protected from both damage and unauthorized access/earwesdropping. Network cabling that is wired overhead from a nearby building or that runs through an unsecured trenching system or between CMDF modules must be protected.

The inherent containment found within most CMDF modules may reduce the security risk present across all of these elements. Some organizations may find that a CMDF’s security implementation costs are lower than those of a traditional fixed facility.

ECOLOGICAL (“GREEN”) CONSIDERATIONS

A CMDF can potentially contribute to an organization’s sustainability efforts in some key ways. By leveraging factory build processes and more efficient supply lines, a CMDF may take significantly fewer resources to construct and deploy than a site-constructed, purpose-built facility. But to maintain this advantage, there are issues that need to be considered as part of the local construction, preparation, and installation phases; during the operational lifetime of the unit; and during de-installation. This is particularly the case if the use of a CMDF solution will become an issue of corporate pride or public scrutiny.

It is important to understand that most ecological-impact measures, such as LEED, are not specifically designed to account for the installation and use of CMDF modules. While it may be possible for a data center project that leverages one or more CMDF modules to become LEED certified, much will depend upon the

3 Leadership in Energy and Environmental Design (LEED) is an internationally recognized green building certification system.

©2011 The Green Grid. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted, or stored in any retrieval system of any nature without the written permission of the copyright owner.
definition of the project and the skill of the project manager in fulfilling LEED requirements. It is also likely that while the overall project may potentially be certified, the treatment of the modules themselves is debatable. A qualified LEED-accredited professional—preferably part of a trusted architectural firm with containerized/modular product installation experience—should be engaged to help guide the overall project.

During the preparation phase for a CMDF project, there are many opportunities to employ ecofriendly practices. For instance, excavation and grading may be required to create level space for the CMDF modules. Proper environmental practices should be employed, including, but not limited to, the appropriate importing or disposal of fill material, runoff control, and awareness of the drainage patterns and their effect on local environments. The Green Grid urges strict review of any project being placed within or near a designated resource area.

While control of construction waste and incidental environmental damage are normal parts of construction projects, the use of a CMDF module may help mitigate some troublesome issues because the module is manufactured in a controlled environment prior to its delivery to the final site. Transportation to the site has an environmental impact, and low-impact methods should be considered.

During the operational life of the CMDF, care should be taken to minimize the discharge of coolant or fire-suppression chemicals. A catch basin for coolant may be necessary to avoid an unplanned discharge in the case of a coolant leak. Technology refresh in a CMDF module can involve either an onsite de-integration and reintegration or a full de-installation and reinstallation of a refreshed module. During such an upgrade, care should be taken to avoid coolant or chemical discharge, and proper consideration of the packaging waste stream should be well managed.

OPERATIONAL DISCIPLINE

The nature of CMDF modules is such that they tend to impose a certain discipline and a higher maturity level on their owners and operators. As discussed earlier in this paper, the pre-engineered and prefabricated nature of a CMDF module enables much tighter, more efficient approaches to the space and the underlying services. However, these tighter tolerances and higher performance levels also tend to impose certain limitations and requirements.

A payload module built according to ISO shipping container specifications, for instance, can be expected to impose different spatial and non-spatial operating limits than one would expect in a traditional purpose-built facility, such as narrow aisles or specific procedures for how to service payload equipment.
A highly mature organization may have few practical challenges in dealing with many of these advantages, limitations, and differences. For instance, an organization that is focused on high-quality procedures and documentation may be able to easily adapt to a CMDF because its team members likely are already used to creating and following documented procedures and work rules. Adding to those procedures and rules to align with the nature of the CMDF deployment, and requiring staff to adhere to them, may be a simple adaptation. This may be especially true if the team’s existing processes are built around lights-out data center management and operations approaches. Most CMDF modules involve the same, or similar, lights-out approaches, making it easier for the team to handle the modules because that kind of remote management is already part of the team’s existing organizational culture.

Conversely, a less mature organization may have some difficulties in adapting to operating within a CMDF framework. This may be because of a lack of existing focus on operational discipline, a lack of change control and management, or even an established culture where systems management is largely performed physically (hands-on) rather than remotely.

This is not to suggest that organizations that currently lack good operational discipline should not take advantage of CMDF solutions. On the contrary—those organizations may have the most to gain by deploying a CMDF, presuming they put in place the proper planning, training, and operational support services. For instance, selecting a CMDF may make sense for an organization seeking to improve operations and reduce costs. Transitioning from a less mature current state to an operationally disciplined CMDF solution (especially if it is a greenfield deployment) may be far easier and more cost-effective than trying to reinvent or develop maturity within its current environment. A CMDF may be an organization’s catalyst for service improvement or a means of moving to the next maturity level in the services provided to internal or external customers. A CMDF deployment may enable the installation of a new, efficient, and more effective IT and service architecture, which would replace or augment the organization’s legacy environments.

**Working in confined spaces**

Another area of consideration is the nature of the space within a module. Some modules may have limited aisle and other spaces available in which personnel can work. These limitations (which may or may not be relevant given the particular circumstances) should be considered, and operational procedures established, to ensure that the work environment remains safe and effective.

**Training and education**

To help ensure a successful deployment and effective, resilient operations, it is crucial that those responsible for general operations, as well as those who will be working within the CMDF modules, be properly trained and
provided with the operational tools to be effective. Similar to when an organization acquires an expensive and complicated piece of machinery, successful CMDF operations will require proper education and training on how the platform operates, how it is serviced, and how to properly to work with and within the modules.

This underlying need for training and education is similar to that of any environment with high-power equipment and density, areas where there is mechanical equipment that may cause injury if operated improperly, and areas where safety and operational sustainability practices are key success factors.

VII. Conclusion

The CMDF approach can enable organizations to deploy IT equipment, capacity, and services in less time, for less cost, and under new and more business-appropriate delivery and costing models. The prefabricated and pre-engineered nature of a module can significantly reduce the potential quality and time risks typically found in traditional fixed-facility, site-constructed approaches. The CMDF architecture has become an increasingly viable and robust alternative when considering a data center build, as long as organizations take into account a CMDF’s particular needs and engage proper expertise and capabilities from trusted partners. Organizations should carefully weigh their needs against the advantages, risks, and challenges that a CMDF deployment may present.

VIII. References

   http://www.thegreengrid.org/en/Global/Content/white-papers/WUE
   http://www.thegreengrid.org/en/Global/Content/white-papers/ERE

©2011 The Green Grid. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted, or stored in any retrieval system of any nature without the written permission of the copyright owner.
IX. About The Green Grid

The Green Grid is a non-profit, open industry consortium of end users, policy makers, technology providers, facility architects, and utility companies collaborating to improve the resource efficiency of data centers and business computing ecosystems. With more than 175 member companies around the world, The Green Grid seeks to unite global industry efforts, create a common set of metrics, and develop technical resources and educational tools to further its goals. Additional information is available at www.thegreengrid.org.
X. Appendix A. Understanding Reliability and Resiliency

When looking at data centers and data center design, one would normally evaluate how the design and operation of the facility enables the installed IT equipment to continue operating with a “minimal and acceptable” level of planned and unplanned outages. Of course, what is minimal and acceptable will vary widely from organization to organization, site to site, system to system, and application to application. Part of the promise and attraction of the CMDF approach is that the pre-engineering and prefabrication of the modules help drive down the potential for unknown faults to be realized as unplanned outages, with the promise of potentially minimizing planned outages for maintenance and other activities.

Recognizing that most organizations would like to implement some level of uptime assurance with the deployment of CMDF modules, it is important to identify and fully understand the core influencers on possible downtime. To do so, the key concepts of resiliency and reliability need to be explored.

Arguably, the most important measurable factor in this discussion is availability. Stated in simple terms, availability refers to the proportion of time that the solution continues to provide continuous services to a hosted payload. Availability expressed as uptime generally refers to the proportion of time that the solution does not experience an unplanned outage. Thus:

![Figure 5. Availability versus uptime](image)

This distinction (shown in Figure 5. Availability versus uptime) is quite important. When selecting modules and designing the overall solution, projected availability and uptime may both (or individually) be essential decision factors. For instance, if availability were a decision factor, an organization would want to account for the level of resiliency and the level of reliability, as well as the maintenance requirements. The organization may decide that it would rather select a CMDF module that has low maintenance needs and a strong likelihood of resilience and reliability than a solution that has a very high degree of uptime but requires a lot of maintenance to achieve it.

©2011 The Green Grid. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted, or stored in any retrieval system of any nature without the written permission of the copyright owner.
Resiliency refers to the solution’s ability to withstand both the failure of component parts or subsystems and the impact of known outside risk factors. Achieving a particular degree of resiliency is a function of design for which cost, regulatory, and other considerations must be accounted. For instance, designing a highly resilient chilled-water distribution system may entail:

- Using materials, pumps, and other pieces of mechanical equipment that are individually highly reliable and of a high demonstrable quality
- Optimizing a design to reduce the potential of any one component failing and causing an outage
- Using multiple installations of key components (which is an implementation of redundancy)
- Implementing proper maintenance procedures and controls
- Applying controls, monitoring systems, and analytical platforms to identify and proactively address outage risks

In contrast, redundancy is simply the application of duplicate components in a solution. Merely applying redundancy does not in itself result in resiliency or a high degree of uptime. However, a resilient design would normally be expected to contain some degree of redundancy (particularly at very high uptime design levels).

Why is this important for CMDF solutions? The pre-engineered nature of the CMDF approach enables a deeper level of engineering and reduces the impact and occurrence of potential faults. Part of the value proposition for deploying CMDF modules is that they enable an organization to expect and demand that the products will demonstrate a higher degree of uptime than a comparable fixed and purpose-built facility.

However, there are some limitations. While many risks can be reduced or eliminated through more detailed product engineering efforts, some CMDF modules may have inherent limitations that may make it comparatively difficult to achieve a particular level of resilience and uptime. For instance, closely coupled cooling demonstrates much higher levels of efficiency than traditional mechanisms (such as computer room air conditioner [CRAC] and computer room air handler [CRAH] units), but when applied in a containerized environment, it can be more difficult to design in the redundancy necessary to achieve very high levels of uptime. This difficulty may be caused by spatial or other limiting factors that are more acute in a module than in a fixed facility.

Consider, for example, chilled-water-based cooling doors. The normal approach to cooling of this type would include a single (non-redundant) water connection to the cooling door and the use of one cooling coil within the door itself. To achieve a high degree of resilience, an organization must consider its overall method for
distributing chilled water within and to the module, and it must also consider how cooling is distributed across all racks and within the ambient space.

Given the above limitations, an organization that wanted a particular degree of redundancy as part of its cooling design may not be able to achieve that redundancy at the rack level, but it may be possible at the module level. Space limitations in the module may prevent the implementation of additional redundancy, while in a fixed facility those limitations may not exist. Different cooling approaches would have differing levels of limitations and possibilities. Depending on the CMDF’s resiliency and uptime requirements, its underlying design, engineering, and redundancy elements can directly influence which (if any) CMDF modules are available to meet particular resiliency and uptime goals and requirements.

In many ways, the CMDF approach can enable organizations to take a fresh look at how they architect their IT environments, how and to what level they establish resiliency and uptime requirements, and how the underlying facilities can support their needs.