
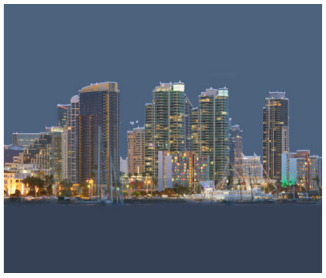

# THE BROAD DIMENSION

## the newsletter of tbd consultants - Autumn/Winter 2019


tbd consultants

Construction Management Specialists

111 Pine Street, Suite 1315
San Francisco, CA 94111
(415) 981-9430 (San Francisco office)

6518 Lonetree Blvd., Suite 164
Rocklin, CA 95765
(916) 742-1770 (Sacramento office)

600 B Street, San Diego, CA 92101
(619) 814-6793 (San Diego office)

8538 173rd Avenue NE, Redmond, WA 98052
(206) 571-0128 (Seattle office)

2063 Grant Road, Los Altos, CA 94024
(650) 386-1728 (South Bay office)

7083 Hollywood Blvd, 4th floor
Los Angeles, CA 90028
(424) 343-2652 (Los Angeles, CA, office)

1a Zoe House, Church Road, Greystones
Wicklow, A63 WK40, Ireland
+353 86-600-1352 (Europe office)

www.TBDconsultants.com


**In this Edition:**


IoT Security & SB327 .....1

Assessing Solar .....3

Blame Brexit .....4


## IoT Security & SB327

Cybersecurity has continued to hit the headlines, with recent examples including Louisiana issuing a Cybersecurity State of Emergency after three of their school districts suffered cybersecurity breaches, which also took down one district's phone system. Soon after that, we heard about the CapitalOne breach that affected about 110 million people. The rise of the IoT (Internet of Things) and the IIoT (Industrial IoT) has multiplied the number of access points that hackers can target, and these devices have become attractive backdoors for hackers because they have been left largely unprotected.

The protocols commonly used to communicate with IoT devices include Modbus, BACnet, and SNMP. Modbus has no security measures integrated into it, and BACnet has such a low-level security option that manufacturers seldom bother including it in their products. There is a new version of BACnet being worked on that will be more secure, but that is probably still a year or two away. The first version of SNMP (Simple Network Management Protocol) had no security incorporated in it, and the second version had some, but remained fairly insecure. SNMPv3 has much improved security, but as a protocol that is now 15 years old, it has also become highly vulnerable to hackers.

Does it really matter if someone hacks into your Internet-connected refrigerator and lets your milk go sour? Probably not, but what if they hack into a controller at a power station and black out your city? The recent blackout in Manhattan was due to a communications issue with the Protective Relays at a substation. These same relays have already been the subject of cybersecurity vulnerability reports and, while this incident appears to have been unintentional, it shows how serious the cyber threat is to our everyday lives.

While devices, like protective relays, can affect tens of thousands of companies and individuals, Building Management Systems (BMS) in office buildings and data centers have become more frequent targets of attacks and these can shut down an entire building and all the companies located in that facility. In addition, items like Programmable Logic Controllers (PLCs), Uninterruptible Power Supplies (UPSs) and Air Conditioning (AC) systems all represent prime targets for hackers to interrupt and sabotage critical operations at almost any type of facility.

As a general rule, manufacturers have been more interested in getting new technology onto the market as quickly and cheaply as possible, in order to undercut the competition. Security has, sadly, often been an afterthought. Yet, all these devices are effectively turning our office buildings, hospitals, data centers and homes into Internet-connected objects, and laying out the welcome mat to cybercriminals.

Enter California Senate Bill No. 327 (SB327), the first legislation in the U.S. to specifically address the security associated with IoT and IIoT devices. In addition, there are at least two bills working their way through Congress, 'The Internet of Things Cybersecurity Improvement Act' and the 'Securing IoT Act', but, at time of writing, neither of them has come up for a vote.

SB327 was signed into law in September 2018 and, in simple terms, says that from January 1, 2020, all new IoT devices sold and installed in California must have security appropriate to the type and use of that particular device. 'Appropriate' means that the more critical the device is and, the more essential the use to which it is put, the more demanding the security must be. The wording does give plenty of room for lawyers to argue about it and for case-law to define it, but in a rapidly changing field of technology like IoT, it is about as good as lawmakers could come up with. It can certainly be said that SB327 is better than any similar law that has been enacted, if only because there are no other laws yet that relate specifically to security on these kinds of devices.

There are some specific requirements in SB327, such as those related to passwords used to access such a device. No more default passwords, so loved by hackers worldwide. Each device must either have a unique password, or it must force a user to change the password the first time they use it. But that brings little help to Modbus and BACnet devices which do not even offer secured passwords. It's fair to say that, for these protocols, no security is not "appropriate security".

With this law coming into effect at the start of next year, it is an issue that designers will need to be addressing now. Using SNMPv3, with all its security features implemented, for the communication protocol may meet the requirements of SB327 in most instances, as would the forthcoming version of BACnet (whenever it's available). If the IIoT device was, say, controlling a critical piece of equipment in a power station, something better than SNMPv3 would almost certainly be needed to make the security level 'appropriate'. However, if the device being sold past 1/1/20 is using Modbus or the current version of BACnet, then a dedicated security device would be needed in order to be compliant with the law. This law can include fines and penalties, and any such events would likely generate wide-ranging headlines that would embarrass the engineer, manufacturer and the end user. This all makes it paramount for all designs to include the proper security systems for each new project in California.

*Our thanks to Bob Hunter of AlphaGuardian (www.alphaguardian.net) for his help with this article.*

# Assessing Solar

We all depend on electricity for so much of what we do, but utility costs keep rising. PV (photovoltaic) panels convert sunlight directly into electricity, so doesn't it make sense to go solar? Well, there are a few things to consider first.

For a typical solar installation on a single-family home, you would need the panels to produce the electricity and an inverter to convert that DC (direct current) power

to the AC (alternating current) that you need to run your lighting and appliances. There are times when the sun isn't shining, so you will still need to be connected to the utility's power grid, and you'll need something to automatically switch between the grid and the solar power. In recent years, battery technology has improved to the point where a solar installation can economically include a bank of batteries to provide backup for times when the sun isn't shining. Other associated costs include the design of the installation and obtaining permits.

Being connected to the utility grid also means that when you are producing more power than you are using, you can feed that power back into the grid and get paid by the utility company. With a battery backup, the system can store the excess power and feed it into the grid at times of peak demand, so that you can get a higher price for it. There are a couple of ways that the utility might buy power from you. With net metering, the utility pays the full retail value per watt, using a single meter that can count up and down, depending on whether power is being drawn from or fed into the grid. Feed-in tariff utilizes a second meter to separately record the power fed into the grid, and then a different rate can then be charged for taking power from the grid and for feeding it back in.

There are a variety of companies offering solar installations, and, as with any construction project, obtaining multiple bids is worthwhile. The larger companies will probably not show an economy of scale as far as cost is concerned, but there can be other things to consider in that regard. For instance, you may be offered a 20 or 25-year warranty with the installation, and you need to consider the odds on whether the company will still be there for that duration. You might also want to consider what the technology will be in 25 years' time. There are already roofing shingles available that can generate solar power. If it is likely that your building will need reroofing during the next 20 years, will the roofing material be incorporating solar power generation anyway?

When comparing quotes from different suppliers, some describe their systems in kWh (kilowatt hours) and others in kW (kilowatts). They might sound very similar, but kW reflects the rate at which the electricity is being produced, while kWh is the total amount of electricity used and is what you see on your utility bill. As a rule of thumb, 1 kW equates to about 4.25 kWh if you have a good location for your solar installation.

We are now in 2019, which is the last year that the Federal rebate for residential solar installations will be at 30%. So what are the economics of residential solar installations today? There are many things to consider, including how much power you consume, what make of panel to choose, and how much battery backup you want to provide. Different regions can expect different amounts of sunshine, so the same number of panels will produce differing amounts of power, and installation costs can vary substantially from one region to another. One advantage of installing solar on residential buildings is that the roofs are normally sloped at an angle that works well for the panels.

Currently, a PV array can increase the value of your house. In future, having old tech up there may not be as attractive.

The Federal solar rebate goes down to 26% in 2020, 22% in 2021, and disappears in 2022, but solar panel costs have also been dropping and are likely to continue doing so, while utility bills rise. You may also be fortunate in having local credits available for solar installations.

For this study, we are looking at a solar installation for a house in California, which has ample sunlight but where labor costs are high. The annual power consumption is approximately 5,500 kWh for a total bill of about $1,300/annum. The quotes for the solar system came to around $18,500 (of which about $7,000 is for the battery) to purchase the system outright, about $875/annum over 25 years to purchase it through a lease, or $15,000 to prepay for 25 years' electricity generation from the system. With that last option, the system remains the property of the company supplying it, and they would monitor and maintain the system, including the battery, for 25 years. The quotes include the allowance for the 30% federal rebate, but no local rebate was available.

The payback period worked out at around 14 years for the direct purchase, and 11 years for the lease and prepay options. That is assuming a 3% per annum increase in the electrical utility charges, which is probably on the low

side. The lease and the prepaid generation options have the same payback period because the total for the prepaid option ($15,000) is equal to the lease payments when using the formula for Cumulative Present Value.

The CPV formula calculates the capitalized costs of a series of future amounts (basically, what you would have to invest initially to finance the future payments). The formula is P = S/((1 + i)^n) where P is the present value of S for year n, S is the future value amount, i is the interest rate, and n is the year that S is due.

# Blame Brexit

This article is being written at the start of September as the UK's new Prime Minister, Boris Johnson, has parliament rebelling against his plans, or lack of them, for withdrawing from the European Union. There seems to be total confusion about what is going on, but there is fear that a no-deal Brexit will throw the UK into recession. Germany is already on the verge of a recession as their export-driven economy suffers under the slowdown in international trade, and there are concerns that a messy Brexit would only compound matters. Italy is also suffering economically.

In Asia, China's growth has dropped to around the same as it did during the depth of the Great Recession. Other Asian countries that are verging on, or already in, recession include Hong Kong, Singapore, and South Korea. Japan appears to be doing well at present, but, like Germany it is dependent on international trade, and that is in flux with the on-and-off trade wars.

In the US, the bond market inversions (when it becomes cheaper for the government to borrow for ten years, rather than two) has been getting people talking of recession. The AIA's Architectural Billings Index (ABI) has predicted the last two recessions by dropping below the 50 mark (the breakeven point, meaning billings are neither increasing nor decreasing), and it has been bouncing around that mark for months, after starting out the year strong. The stock market went on a steady rise until the start of 2018 as it recovered from the Great Recession. Since the start of 2018, it has been basically going nowhere, in steep jumps up and down, but doesn't seem to have any real sense of direction. And the US manufacturing sector is said by some to have already fallen into recession.

That said, there does not appear to be any real reason for thinking that recession is coming to the US in the near future. There is always the possibility that the trade war or some international hotspot, like Iran, might upset markets enough to trigger a recession, but that is something that can't be predicted ahead of time. When a bond market inversion has preceded a recession, the inversion has lasted for months, not just days. When the ABI has foreshadowed a recession, it has done it by remaining consistently below 50, not just bounced around that mark. The stock market may have been taking some big hits recently, and then recovering on news of talks about talks, but it has still been hitting new highs along the way as the economy keeps growing at around 2%.


The most important sign is that consumer confidence has remained high. The fact that the last round of tariffs on Chinese goods will affect prices on consumer goods is of some concern, but while unemployment remains at historic lows and wages are rising, confidence shouldn't be adversely affected much. With consumer sales making up almost 70% of the U.S. GDP, you can see how important that is.

With so many signs at home and abroad that might indicate an upcoming recession or a continuation of the bull market, it is easy to understand the confusion that many people are in. With the confusion surrounding the markets being mirrored so extensively by the antics in the U.K. parliament, whatever happens with the markets here, let's just blame Brexit.

*Geoff Canham, Editor, TBD San Francisco*

*Newsletter designed by Katie Levine*