Background

Pacific Gas and Electric (PG&E) utilizes two major types of automation architecture in their substations. The first is the more "traditional Remote Terminal Unit (RTU) with hard wired inputs and outputs" based architecture, as defined in IEEE standard C37.1-2007, with the additional function of data concentration when Intelligent Electronic Devices (IEDs) are present. The second utilizes a Human Machine Interface (HMI) computer to act as the data concentrators for substation information in addition to providing an operational interface that mimics what the remote system operators would use. These are utilized when an entire building is designed to use recent standards that integrate protection, automation and control functions into the relays for each substation breaker, transformer bank or line.

Both architectures provide the base needs of obtaining supervisory control and data acquisition (SCADA) with the added benefit at HMI sites of having convenient operating platform. However, after years of being installed new challenges started to arise such as facing increasing cyber security requirements, constant patching, and a significant change to the master station systems the desire to modernize the HMI architecture became apparent. PG&E’s previous design was pretty unique in that it implemented a server that acted as a complete SCADA master within the substation. The driver for this design was the two large benefits of having the station interface screens match exactly with the remote operator screens and there being no additional work to create these screens multiple times. An employee would create the screens for the distributed master station once and the remote operators would remote desktop to that computer at the substation. This modernization effort started with defining hurdles and shedding light on the short comings of the existing design such as security issues and high cost of maintenance that was due to using an overly designed server at the substation as opposed to a simplified appliance. This modernization provided many lessons learned regarding defining minimum viable product, taking a cradle to grave approach, and the effect on existing procedures.

Scoping the Minimum Viable Product

The triggering event to begin the modernization project was a program to replace the entirety of our SCADA software to become a function of our EMS and ADMS platforms. Since the remote masters would no longer match control interfaces in the substation there would be no benefits and many risks installing and maintaining SCADA servers that used commercial server hardware, Operating System (OS), SCADA application and all the needed networking services at the stations.
The first step to finding a replacement was to find what the minimum viable product would be. After the simplest version of the solution is defined there will be plenty of opportunities to add desired features and increase the complexity to meet various needs when we look at the lifecycle of the product. In the simplest description PG&E needed to have a device that could collect station data, display that data on a screen and allow controls either locally or remotely.

This minimal definition could be achieved by many simpler devices on the market that would be described better as an appliance than a general-purpose computer. An appliance is computing device created for a specific purpose with specialized hardware and firmware with all possible applications predefined utilizing white listing. Reducing the device to this resulted in benefits like:

- **Substation Hardened Equipment**: The previous servers utilized moving parts such as spinning hard drives and cooling fans. These moving parts required the building to be climate controlled and reduced the mean time between failure. However, most vendors of substation computer appliances can provide a solution that is compliant with IEEE 37.90 and IEEE 1613.

- **Smaller Security Footprint**: A large part of securing a cyber asset is reducing the number of ports and services. By using a device that is designed for a specific task it is possible to reduce the ports and services down to only what is needed for the protocols for SCADA data and the ability to retrieve applicable logs.

- **Integrated Troubleshooting Tools**: A server has plenty of options for hardware and network diagnostics as well as serial or network analyzers for many protocols, but these are all separate applications or portions of the BIOS. A computer appliance on the other hand consolidates all these trouble shooting tools into the initial build for a consistent and dependable experience.

- **Minimized Hardware and Maintenance Costs**: Licensing and patching of a commercial OS and the separate applications needed to run a SCADA server produced a very high ongoing cost. Additionally, the life cycle of a commercial server was found to be 3 to 6 years; on the other hand, a substation hardened appliance has a lifecycle of 15 to 20 years. These two factors greatly reduce the installation and maintenance cost.

The upfront cost of researching devices, creating new standards, developing new training and socializing such a change is very large and can be intimidating for many organizations. However, by starting by defining the minimum viable product we can illustrate how over a short amount of time those cost can be recuperated by a simpler design. Over simplification at this point does have the potential to leave out desired features or become shackled to the device by not
describing how to support, maintain and replace it. This cradle to grave approach was brought through to the design and implementation of the new HMI appliance.

Cradle to Grave Design

Once the minimum viable product was defined and the justification of the initial cost complete the design could begin. The ideal situation would be to gain the improvements from going to an appliance, reducing maintenance cost and planning for the eventual removal of the device while minimizing change to standard drawings, user interfaces and external wiring. To accomplish these goals the following considerations drove the design:

- Remove all proprietary protocols at the port: Many devices in a substation use protocols that are designed to only work with matching hardware. This quite often provides a much more efficient method of communication or can provide additional information about the communication channel. The downside of these protocols is that it creates an interdependent relationship for data controller, slave devices and/or master servers. These interdependencies make it very hard to replace or upgrade one element of the SCADA system without affecting the rest. It was decided that if all ports on the HMI utilized industry standard protocols as opposed to proprietary ones that we would have a vendor agnostic design and thus have greatly increased our future flexibility.

- Exclusively Ethernet: The previous HMI design utilized Ethernet connections on many of the IED's and the ones that needed serial were connected via a terminal server so that from the HMI's point of view it had no direct serial connections. This allowed a new device to come in and make connections before breaking the connections to the old HMI and needed no physical change to wiring other than an Ethernet connection from new HMI to the Ethernet switch. This flexibility was desired so despite an abundance of serial ports the new HMI used no serial connections.

- Mimicking the machine interface: To minimize procedural errors, there was an intent to replicate the screen visuals and operation of those screens as close as possible. This was necessary due to the fact there will be a large amount of time with both designs being in place. Template based configuration was heavily relied on to reduce time for time for installation and to drive consistency of these interfaces. Creating templates took a marginal amount of initial set up time but greatly reduced future configuration time.

Once the design that was based on these considerations was complete a pilot site was selected. As with any aggressive pilot we found some lessons learned, faces some scope creep and made selective sacrifices.
Lessons Learned

Implementation at the first site was successful and displayed the feasibility of installing these devices on a large scale. That is not to say that it did not come with hurdles and lessons learned. Some of the inflight realizations that were made were:

- **Selective Sacrifices:** Any engineering effort will present several options with conflicting benefits, risks and drawbacks. For instance, substation HMI’s previously had speakers and printers connected to them but transitioning to an appliance that utilized white listing meant that the drivers for these peripheral would not work. After a short discussion it was realized that they were rarely to never utilized and that the benefits of security were much greater than the drawbacks of losing these peripheral devices.

- **Reconsidering Testing strategy:** It is standard testing procedure to retest any points that are changed in a database to confirm that alignment is kept all the way from the operator’s screen to the electrical element. This requires electrical clearance of all major electrical equipment and can be very difficult to accomplish and coordinate. Seeing this hurdle sparked a discussion on how to improve the testing strategy by defining the point of change and testing alignment from operator screen to point of change. A change to the testing strategy would reduce testing hours and reduce liabilities of having the unnecessary clearances.

- **Utilizing vendor for initial templates** - As with any device there is an initial learning curve that can hinder work. When faced with this PG&E utilized the opportunity to bring in the expertise of the vendor to not only configure the device and screens but also use that commission testing as a training opportunity and initial creation of templates. Once the templates were in hand and there was some internal experience on the device subsequent jobs were handled internally with confidence.

Going Forward

After the achievement of the pilot it was decided to continue the replacement of all substation HMI servers with appliances. As these replacements happen the templates for the interface are being improved in both efficiency of being built and based off user feedback. The reduced amount of ports and services has lowered the security footprint without sacrifice to usability. The substation hardened nature and removal of licensed software has greatly reduced the annual maintenance cost projections.

In addition to meeting the current needs of replacing HMIs this new design being more secure and vendor agnostic will also be able to meet the everchanging needs of future initiatives. The power industry is changing dramatically with distributed generation, microgrids, ground fault neutralization,
automatic wide area fault isolation and reclosing schemes and the distributed energy management systems to control them. With a simple design that is not bound to proprietary or serial communication PG&E is much more able to provide a data collection and control solution to meet the needs of these initiatives.

Due to all these factors the reevaluation and modernization of the HMI, as well as the process of defining minimum viable process followed by defining the needs of the device from installation to removal, showed to be a great success to the point that the same process was applied to our RTU design as well.