iSnet

iBOSS

iSnet-based Bomba Operations Safety System

Moving Bomba into the Future

The development and subsequent deployment of a state of the art

Malaysian National Fire Alarm Monitoring Solution

iSnet iSCADA NET SDN BHD

iSCADA NET SDN. BHD. No. 32-1C, Jalan 28/70A, Desa Sri Hartamas. 50480 Kuala Lumpur, MALAYSIA

Executive summary

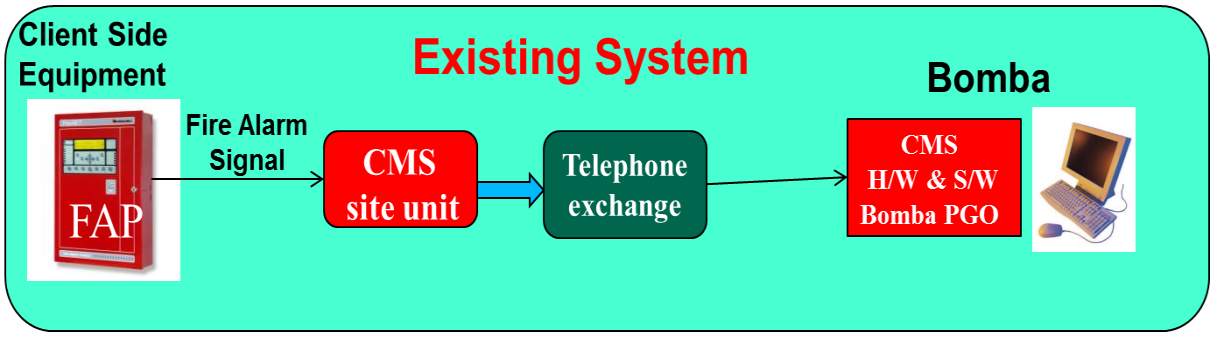
Bomba Malaysia will need to replace its Centralised Monitoring System (CMS) by 2015. Efforts made since the late 2000s had not resulted in any clear solutions. This document details the initiative exercised by Bomba upper management to plan, specify, develop and deploy the CMS replacement in an innovative and risk/cost mitigated manner. *i*BOSS, the solution that was jointly developed between Bomba and iSnet, in a novel Malaysian private public technology partnership, is the result of this effort.

Beginnings

Shortly after taking office as Director General (DG) of the Malaysian Fire and Rescue Services (Bomba) in 2010, **Dato' Wan Mohd. Nor**, began to address the vexing issue of a replacement for the Centralised Monitoring System (CMS). This CMS was deployed in the nineties by two companies operating off a concession provided by the Malaysian government via the local government and housing ministry. The purpose for deploying this CMS was to enhance fire safety in 'designated buildings' by connecting the Fire Alarm Panel (FAP) of these building to the nearest fire station (Balai Bomba). This is common practise in all developed countries. The CMS operates in the following manner :-

When a fire is detected by sensors (heat, smoke or others) or manual fire alert devices (break-glass, emergency button, etc.) connected to the Fire Alarm Panel (FAP), this FAP will generate a general fire alarm (usually triggering an audible alarm as well as a visible bright strobe). Under the Fire Safety Act (FS Act), almost all commercial and industrial buildings are equipped with FAPs. A special category of buildings known as **'designated buildings'** (designation is well defined in the FS Act) are required by law to have their FAP general fire alarm signal directly communicated to the nearest Bomba station. The CMS is the system deployed to address this requirement. Run by two independent concessionaries, this CMS deploys a hardware device (site-unit) that connects the building FAP (specifically the fire alarm signal) to an independent telephone line. In the event the fire alarm is triggered, the CMS site-unit connected to the client FAP will automatically dial up the predetermined Bomba emergency system and report the alarm to this designated Bomba facility (PGO-Pusat Gerakan Operasi) and one selected fire station.

The diagram below depicts the main components of this CMS



The CMS concession allows the two operators to deploy a site- based device at the 'designated building', connect this CMS site-unit to the existing FAP and commission the link-up into the allocated Bomba 24/7 monitoring facility (PGO). In the Bomba PGO, another system is deployed by the CMS provider to process multiple arriving fire alarm signals, identifying the origins of these signals and facilitating an appropriate Bomba response.

The three parties (organisations) involved (CMS technology provider/operator; the 'designated building' owner and Bomba) and their responsibilities are tabulated below.

Organisation	Responsibilities	Cost/benefit
Bomba	Receive incoming fire alarm signals from FAPs via CMS and decide on appropriate action. Ensure that trained Bomba personnel are available to man the PGO on a 24/7 basis	Allows Bomba to carry out its duties more efficiently. **Firefighting** and **fire safety** are two of the three core Bomba objectives (the third is **rescue**). Cost for ongoing maintenance of CMS in PGO
CMS provider	Coordinate the deployment and proper operation of CMS site-unit into designated buildings. Provide Bomba with CMS control console, maintenance / training / upgrade services and other support for CMS	Receives monthly maintenance fees from owners of designated buildings. Receives RM 2,500 for facilitating installation, testing and commissioning of CMS site-unit for building owners. Provide CMS control console at no cost to Bomba.
'Designated Building' owner	Facilitate the installation of CMS site-unit into the appropriate location (usually next to the FAP). Ensure that an independent telephone line, 240VAC power supply and dry contact (from FAP) are available for connection to CMS site-unit. Ensure that proper operation of the site unit through periodic testing.	Cost for dedicated phone line (from Telekoms). Cost for CMS site-unit installation and commissioning. Cost for periodic testing of site unit. Cost of monthly maintenance for CMS connection to Bomba. Cost for the continuous maintenance of the site-unit. FAP is directly connected to local Bomba station for fire safety

Replacement of the CMS presented many challenges to the incoming Bomba DG. Bomba had deferred the replacement decision pending the identification of a state of the art solution which Bomba can then advocate for development testing prior to deployment. The existing concessionaires and many international organisations were aware of this Bomba requirement and much was done to try to identify a solution suitable for the Bomba supervised Malaysian fire safety environment. Up until 2011, no solution emerged that satisfied Bomba's requirements. Bomba has unique accumulated end user knowledge and understanding of the strength/weaknesses of currently available CMS type solutions, having operated closely with two such systems deployed in Malaysia over a period of almost 20 years. Given this advantage, Bomba Malaysia was well placed to provide high level requirements for a National fire alarm monitoring solution that will be suitable for Bomba's Malaysian operating environment.

Bomba senior management had understood some time ago, that a CMS replacement was imperative to the continuing success of the operational effectiveness of Bomba. This is a key Bomba role, as Bomba is a proactive national organisation entrusted with Fire Safety responsibilities for Malaysia. However, because of the complexity of the issues (involving three parties – Public / Bomba / Concessionaires - with disparate objectives) and the challenges of trying to innovate in a rapidly changing technological environment, Bomba had still not realised its goal of identifying and developing (customising and innovating) a relevant solution by early 2011. Dato Wan realised that Bomba needed at least a 2 year transition period to migrate from the existing nationwide CMS to a new system and he gave priority to the identification of such a solution. This was because the existing concession expires in early 2014 and as such, Bomba needed to initiate the testing of a replacement solution in 2011.

When several senior Bomba personnel were approached by an apparently credible Malaysian organisation that claimed expertise in nationwide monitoring solutions in early 2011, Dato Wan as Bomba DG was duly informed. He prudently arranged for this organisation to present their solution to Bomba management. Based on the success of this presentation in convincing Bomba that the proposed system can evolve into a solution that can meet or even exceed Bomba's nationwide fire alarm monitoring needs, Dato' Wan challenged this organisation (**iSnet**) to study Bomba's future CMS requirements and at their own risk and effort, propose a customised solution. Dato' Wan authorised a visit by the Bomba director of Research and Development (Tuan Hamdan Wahid) and his team to review and evaluate an existing deployed system (iSCADA) in UiTM Shah Alam on the recommendation of iSnet. This proven iSCADA technology was to become the basis for the development of the dedicated Bomba National Monitoring Solution proposed by iSnet - ***i*BOSS**.

A straightforward informal partnership resulted from this interchange of ideas. Bomba agreed to facilitate a trial of the possible future CMS replacement if iSnet will develop, fund and deploy the proposed solution and test this solution to Bomba's satisfaction. Bomba also directed iSnet to engage with UKAS (Unit Kerjasama Awam Swasta – the government Public-Private Partnership unit) as this is the government entity that deals with potential Public-Private Partnerships. With the informal agreement of UKAS to proceed as suggested by Bomba, iSnet developed ***i*BOSS** (**i**Snet-based **B**omba **O**perations **S**afety **S**ystem). This was done completely at the risk and expense of iSnet with no obligations from Bomba.

Below is a tabulation of the key events leading to the development of iBoSS as a potential candidate for the future Malaysian National Fire Safety Monitoring Solution.

Chronology of Events Leading to The Trial of *i*BOSS

2Jun 2011 (11 am)	Information session to appraise the Bomba Director General (DG), senior Bomba officers and all state directors on the iSCADA internet based monitoring solution
6July 2011 (10 am)	Official visit by Tuan Hamdan Wahid and his team from Bomba R&D to UiTM Shah Alam to review an existing iSCADA based fire alarm monitoring solution
12Aug 2011	Information session to appraise UKAS on the proposed plan by iSnet to initiate development of the future Bomba CMS replacement
Ogos-Nov 2011	Series of meeting with senior members of UKAS / JBPM
15Nov 2011	Meeting with Director General of UKAS to convey information on proposed program methodology
23Nov 2011	UKAS informs Bomba that UKAS is agreeable for iSCADA Net Sdn. Bhd. (iSnet) to proceed with pilot ***i*BOSS** implementation
6Jan 2012	2nd. Meeting with senior Bomba officers and the DG to provide update on progress of the development of a CMS replacement
10April 2012	Official visit by Tuan Hamdan Ali (senior officer in the Bomba fire safety division) to UiTM Shah Alam to view the deployed fire alarm monitoring solution
24May 2012	Bomba approves the ***i*BOSS** solution to be deployed in a pilot implementation in the klang valley region

Future Bomba nationwide fire alarm monitoring system requirements –

Conceptualisation and design of the *i*BOSS solution

A list of the high level Bomba requirement for the future National Fire Alarm Monitoring Solution and the iSnet proposed solution is outlined below.

1) Bomba needs to upgrade existing technology and deliver better services choices to the public. Recommend to deploy a new system that meets or exceeds Bomba's needs. This allows Bomba to implement new technology and also provide the Malaysian public with wider choice of services at no additional cost or effort to Bomba.

The iSnet Solution:

The iSnet solution is based on a proven cloud computing iSCADA technology with TCP/IP (internet) protocol. This solution will be designed to address and exceed Bomba's current and as far as technologically feasible, to also accommodate BOMBA's future requirements.

2) Bomba needs to deliver a higher level of services to the public in terms of fire safety enforcement without increasing the cost burden on the public. This will be achieved through new technology systems that deliver excellent levels of performance with not additional costs.

The iSnet Solution

The iSnet solution, a web centric cloud computing platform, is a hosted system, which enables high availability, expandability, flexibility and reliability. Our solution uses the latest GPRS, 3G and 4G LTE mobile two-way communication – which is the state-of-art plus it is cost efficient. Performance is at similar levels to state of the art 'cloud solutions' deployed in technologically advanced countries. It is also able to deliver much enhanced performance at optimised costs to meet all existing Bomba needs in operations and enforcement from a technology solution perspective.

3) Bomba needs to deploy an efficient system of Fire Certificate management to enhance fire safety and also to streamline revenue collection to ensure efficient collection of fees from BOMBA provided services. A solution addressing this requirement will be an advantage.

The iSnet Solution:

Existing Fire Certification procedures demand extensive manpower and time resources; iSnet offers a system that delivers not only real time highly reliable data but also historical trending data that effectively improves the manpower and time resources available to Bomba. This is achieved via automated 24-hour intelligent monitoring and other value added components made available by the iSnet solution. In addition, a payment module can be incorporated into this 'cloud' platform to facilitate internet payment for efficiency and convenience with security.

4) Bomba needs to upgrade its nationwide monitoring system for fire alarms without any additional costs burdens to the public. Present system deployed is already over 20 years old and has very limited upgrade possibilities as technology used is now obsolete. Bomba needs to implement a new system that provides many additional features with no additional costs.

The iSnet Solution:

The iSnet's cloud computing solution deploys advanced Internet technology to deliver data anywhere, anytime. As a hosted service, updates are automatically delivered to all PCs, embedded devices and tablets. This ensures that the software is always up-to-date. Cloud solutions have very effective and efficient user interfaces which can be developed and deployed in a very cost optimised manner. Additionally, this solution ensures that urgent data is immediately transmitted to the correct recipient for effective action, wherever the recipient is. These features are key advantages of a web based cloud computing platform.

5) Bomba needs to address the fire safety requirements of the latest commercial/industrial building designs that incorporate advanced fire safety systems which presently cannot be accommodated by existing Bomba monitoring systems.

The iSnet Solution:

Technology relevance demands a solution that has the flexibility to integrate with any communications connectivity requirements. The iSnet solution is very flexible to be integrated with communication via LAN, WAN, DSL,3G, fibre optics network as well as GPRS. The same technology is used to deliver the data to BOMBA, ensuring data can be collected and received anywhere, anytime. In addition, the iSnet solution has two addition levels of deployment which can accommodate more sophisticated legacy FAP monitoring and also the latest addressable FAPs which are already being introduced into the market in increasing numbers.

6) Bomba needs to be in step with the latest internet based technologies, consistent with government objectives for an internet driven society by 2020. This will help meet Bomba's objectives in fire safety by delivering enhances services at no additional costs to the public.

The iSnet Solution:

The iSnet's cloud computing solution deploys advanced Internet technology to deliver data anywhere, anytime. The iSnet software interface works with any web browser, including those on smartphones and tablets. This is the future.

7) Bomba needs to deploy an integrated system that not only monitors fire alarms in real time but is also concurrently able to deliver fire safety systems maintenance information to Bomba. Present state of the art technology allows for such systems and Bomba will be able to specify these systems to Bomba's unique requirements at no additional cost to Bomba.

The iSnet Solution:

Existing central monitoring systems (CMS) are primarily designed to deliver fire alarms alerts to Bomba; the iSnet solution not only delivers fire alarm alerts but also provides for additional extensive monitoring of a building's Fire Fighting & Safety installations (addressable systems). This solution is also expandable and flexible. It can be enhanced to meet clearly identified Bomba needs in fire safety monitoring and fire fighting operations.

8) Bomba needs to address the issue of emergency calls (999). Existing system is nearing end of useful life and has limited coverage due to technology obsolescence. Future system will extend coverage and overcome all present limitations using proven internet and advanced mobile based technologies.

The iSnet Solution:

The iSnet solution can easily be extended to receive alerts from SMS and from apps for tablets and smartphones. In addition the iSnet solution can be integrated with any advanced emergency response platform (999 system). The flexible iSnet solution will interact and communicate with other advanced emergency systems in a seamless manner.

9) Bomba needs to have an integrated system that is able to effectively manage and control false fire alarms with minimal risk to the public.

The iSnet Solution:

iSnet Solution is designed to filter false alarms with a fail-safe mechanism before the alerts are sent to BOMBA. The parameters of our false alarm filter are highly configurable to BOMBA's requirements. Ideally this feature can be 'tuned' to eliminate false alarms with the active cooperation of the building owners.

10) Bomba needs a technology that requires minimal system and hardware maintenance (to public and to Bomba) and be able to deliver maximum uptime functionality.

The iSnet Solution:

Our solution is designed to be beneficial to both the Subscriber and BOMBA. The entire system has a self-check feature which ensures faults are automatically reported and attended to by iSnet in a timely manner. Most technical (if not all) maintenance responsibilities will be undertaken by iSnet to ensure end to end technical system reliability

11) Bomba needs a stable, reliable & proven platform that has been successfully deployed and tested over a minimum 3 years period in its intended operational environment to ensure minimum risks of long term system stability.

The iSnet Solution:

The iSnet solution is based on a solution which has been deployed in UiTM for fire safety maintenance since 2008. The same system has also been deployed for various monitoring application. This is a very stable and complete, tested solution that mitigates all known technical risks to Bomba. It can also be enhanced to address emerging technology challenges.

12) Bomba needs an upgraded system which supports an ever increasing number of designated building; and the system shall be reliable, scalable and with sufficient data logging capability including statistical reporting. System shall be well maintained and have redundancy without any effort on the part of Bomba.

The iSnet Solution:

The combination of cloud computing with TCP/IP protocol ensures that there is no system limitation on the number of subscribers and concurrent users. Our system also eliminates the issue of limitation of access via phone lines. All maintenance of this solution and its physical components will be maintained, enhanced and deployed by iSnet. It is a full feature CLOUD based solution

13) Bomba needs a monitoring and alerting system which interacts with the building owners. This is for the building owners to play the key role of maintenance and minimizing false alarms; and thus allowing Bomba to focus on fire safety monitoring enhancements and fire fighting operations.

The iSnet Solution:

Our solution includes the building owners as part of the system. Alerts are sent first to the building owners for verification before it is escalated to BOMBA for action. With the active participation of building owners in this process, the building owners will appreciate that the onus of fire safety is on them. In addition, data collected from their fire alarm panels will be shared with the building owners to improve on their maintenance culture.

14) In addition to minimum or no maintenance on the part of Bomba, Bomba needs a system that is designed to meet Bomba operational requirements, is easy to use and does not require specialist equipment or skillsets on the part of Bomba. It is best that the proposed system can be accessed by modern, yet convenient IT platforms including smartphones, tablets and laptops.

The iSnet Solution:

With a few simple clicks, BOMBA personnel and building owners can access the data using any web browser. No software installation or specialist knowledge is required. Annual maintenance, software updates and upgrades; plus system back-up and other administrative tasks are all handled at the server level by iSnet.

Bomba has evaluated such modern systems and is ready to deploy, administer and manage such a system within its present operating environment without any additional cost to Bomba or to the public it serves.

iSnet appreciates BOMBA Malaysia's consideration of its ***i*BOSS** solution and will endeavour to address all of Bomba's needs in this area, in a comprehensive and responsible manner.

False Alarm Mitigation Priority

In addition to these requirements, the Bomba DG also specifically asked for a detailed solution to the 'false alarm' issue Bomba faces with the existing CMS.

ISnet's response to this request is detailed below in the 2011 letter to the Bomba DG.

==========

INSB/JBPM/007/2011
03 November 2011

CADANGAN PENGURUSAN SISTEM PENGAWASAN KESELAMATAN KEBAKARAN ISNET DENGAN MENGGUNAKAN TEKNOLOGI iSCADA
-False Alarm mitigation and management

We refer to the meeting with YAS Dato' at your office dated 3rd November 2011 regarding to the matter above

1. We wish to respond to your well elucidated concerns over the false alarm issues related to the present CMS with clarification and some possible options:-

a) Bomba is given a high degree of CONTROL over the alarms and sirens that accompany alerts by the iSnet solution. The iSCADA based iSnet solution is a two way system (unlike the existing CMS) that will allow Bomba to make decisions (once it is established that this is a false alarm) on whether to disable the sirens remotely and subsequently initiate an investigation to the cause of the false alarm to rectify this situation.
b) If false alarms are a problem due to the Fire Alarm Panel (FAP - the origin of the alarm) or other **client side equipment**, the flexible iSnet solution will allow Bomba to set conditions which automatically flag troublesome locations that have regular false alarms and target these locations for **active Bomba directed remedial measures**
c) Bomba will be able to produce **detailed logs of false alarms** via the iSnet solution and provide these logs to motivate the building owners to rectify their system and avoid these troublesome false alarms
d) Bomba will also be able to penalize recalcitrant (those who are unwilling to rectify their faulty equipment) building owners whose system generate regular false alarms if Bomba wishes to do so under existing fire safety regulation as the iSnet solution provides detailed logs of these false alarms which are **legally verifiable**
e) Additionally, the iSnet solution can also be customized to flexibly accommodate future Bomba requirements to address this false alarm issue and provide Bomba with a range of tools to manage this problem with elegantly designed and practical solutions

I hope that this addresses the problem highlighted by YAS Dato' earlier today.

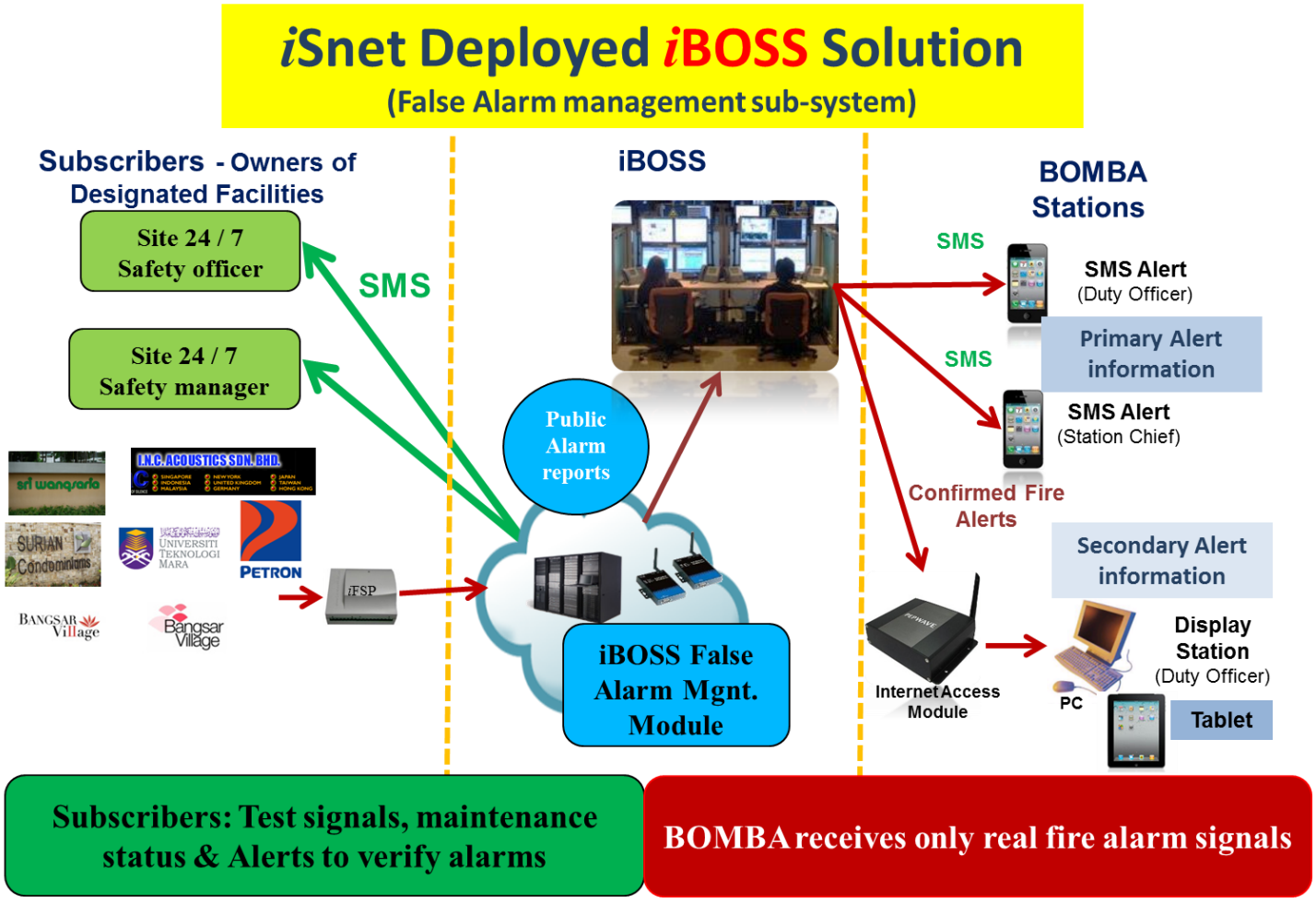
Thank you

Yours faithfully
iSCADA NET SDN BHD (iSnet)
DATO' SAIPUDDIN BIN AHMAD
Executive Chairman

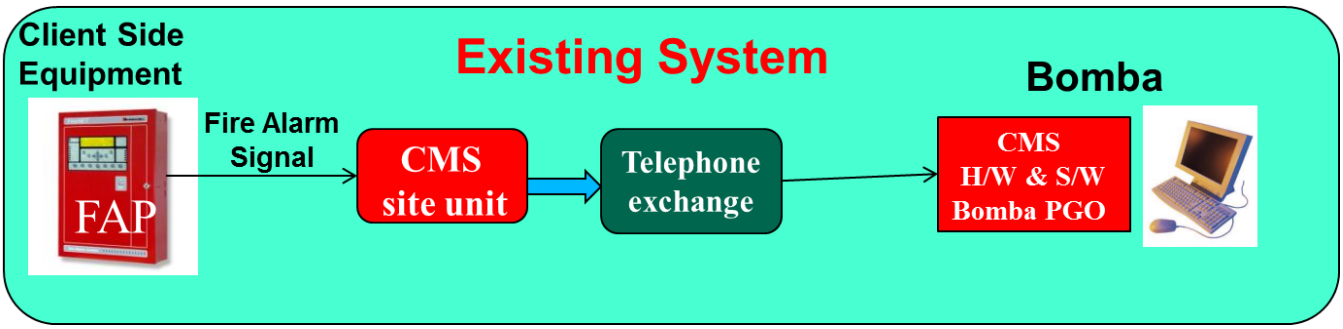
iSnet

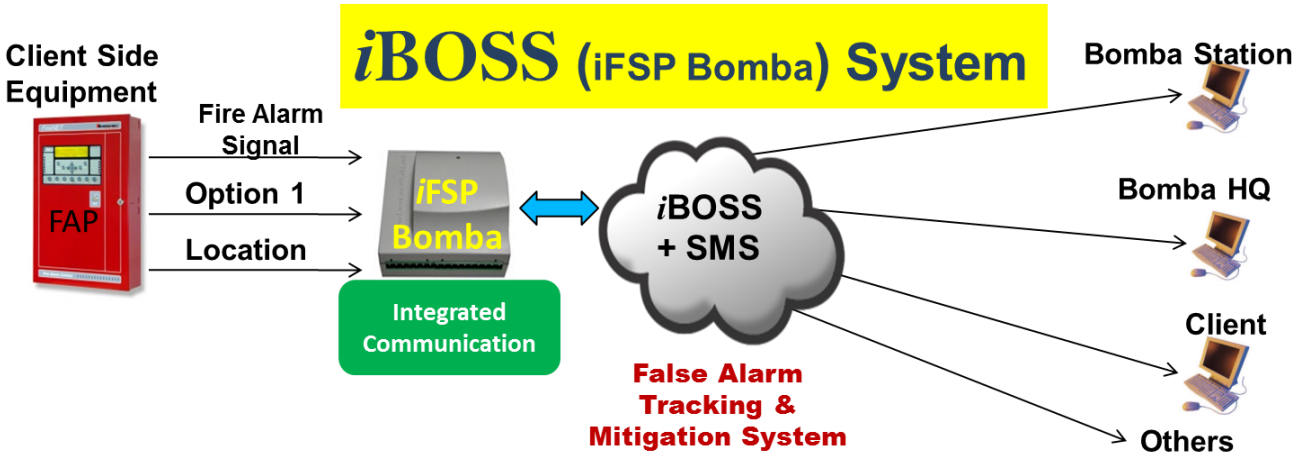
The *i*BOSS Solution

Development of the Bomba specific National Fire Alarm Monitoring Solution commenced in July 2011. This solution was named ***i*BOSS (iSnet-based Bomba operations Safety System).** This name not only reflects the Bomba centric nature of this solution but also the flexibility, adaptability and advanced technology nature of the platform. ***i*BOSS** is designed both to replace CMS and also to address other future Bomba Fire Safety requirements, specifically issuance of Fire Certificates. Beginning with the base iSCADA technology (fully licensed for development and deployment to iSnet), a concerted technology development effort resulted in a deployable version of ***i*BOSS** which was suitable for implementing in a test environment. Bomba provided the test central monitoring locations (Bomba PGO in Selangor and Putrajaya) and iSnet was responsible for system development and trial customer engagement to have several representative and diverse real customer test sites (factories, high rise residences, shopping complexes, etc.). Regular test reports (monthly) were sent to all relevant Bomba departments and the developmental ***i*BOSS** solution was enhanced, optimised and customised to Bomba Malaysia's unique requirements. Feedback on the user experience (both Bomba and the trial customers) allowed iSnet to refine the ***i*BOSS** solution and by June 2013, iBoSS had evolved into a stable, user friendly and Bomba relevant technology. An overview of the ***i*BOSS** solution is shown in the diagram below.



*i*BOSS compared with existing CMS





iBOSS & CMS features Comparison Chart

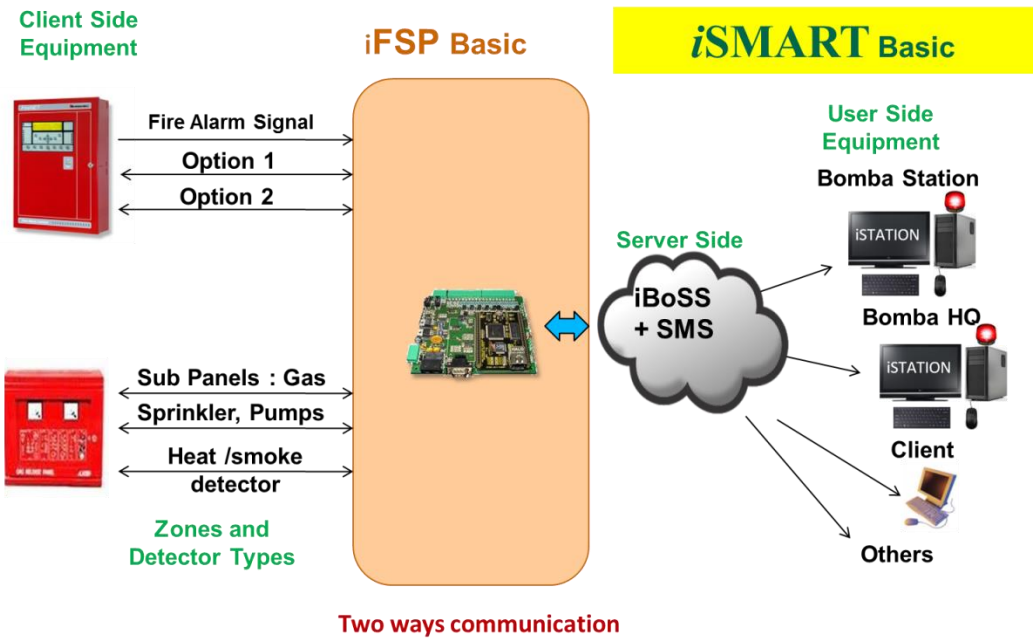
Benefits	*i*BOSS iFSP Bomba	CMS
Alarm Notification to Bomba	✓ Internet, email & SMS ✓ Anytime, anywhere, data finds users.	At control room only.
Alarm Notification to Owners	✓ Internet, email & SMS	× None
Fault Notifications to Owners	✓ Internet, email & SMS	× None
System Failure Alerts	✓ Internet, email & SMS	× None
System status reports	✓ Online	Manual
Equipment status reports	✓ Online	Manual
Maintenance Benchmark Indices	✓ Online	× None

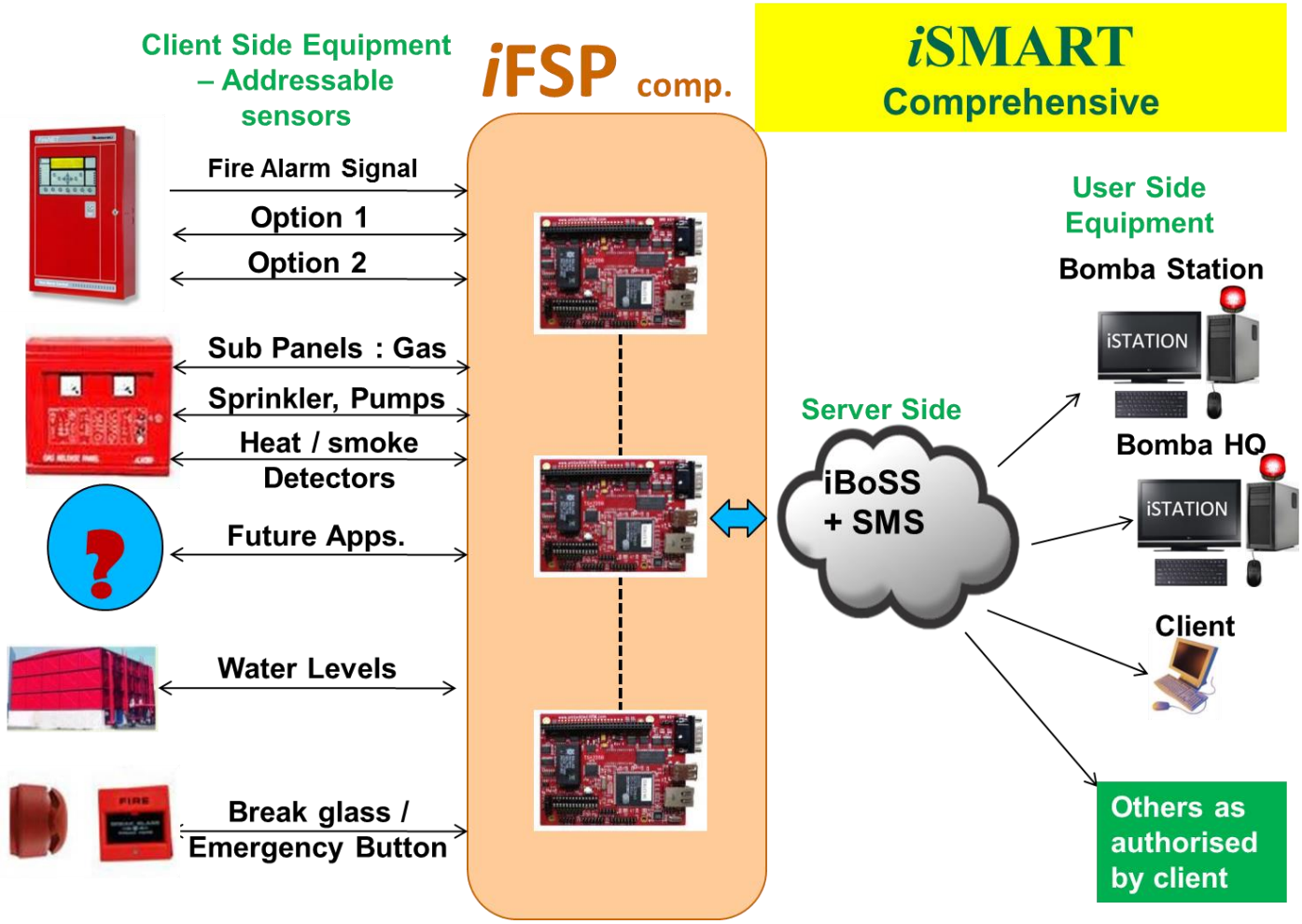
*i*BOSS - Technology Architecture, Operations, Interfaces and Advantages

***i*BOSS** is an integrated cloud computing platform incorporating the most recently deployed internet based technology. It has a very modular architecture that engenders upgradability and operational flexibility. Excellent user interfaces is a key feature of ***i*BOSS**.

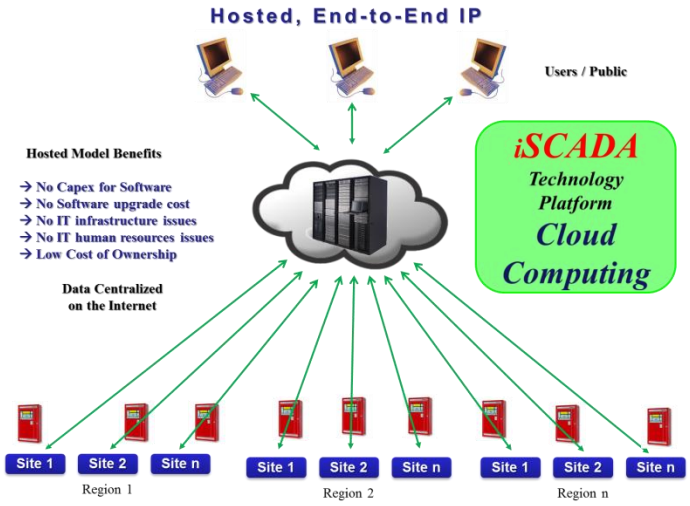
This ***i*BOSS** solution will initially complement existing fire alarm monitoring systems (***i*BOSS** - Bomba), and eventually replace the existing CMS (a 20 years old platform which has reached the end of its useful life). Bomba has planned to allow for a smooth transition from the CMS to this flexible cloud platform (***i*BOSS**) with all its inherent advantages. ***i*BOSS** will also allow Bomba to deploy new fire safety related monitoring services and in future largely automate the renewal of fire safety certificates for designated buildings. In addition, Bomba will also benefit from reduced maintenance as the cloud platform model will allow Bomba to use existing PCs without need for additional equipment. This ***i*BOSS** technology platform can additionally be adapted to address current and many future Bomba fire safety monitoring and fire fighting operational requirements as they evolve.

One such requirement is to perhaps extend fire safety monitoring to include fire-fighting and fire detection systems. Such a monitoring system will ensure that all installed fire safety systems are well maintained and periodically tested as per internationally accepted standards. With hosted data acquisition systems evolving from ***i*BOSS** and to avoid confusion with this Bomba optimised solution, iSnet has developed ***i*SMART (*i*Snet Monitoring And Response Technology)** to complement the Bomba centric ***i*BOSS.** ***i*SMART** is an enhanced version of ***i*BOSS** and is fully compatible with ***i*BOSS.** All monitored systems using ***i*SMART Basic** will have verifiable availability status that can be used for certification and maintenance purposes. Coupled with addressable fire safety devices (***i*SMART Comprehensive**), monitoring can be directed to individual devices level, providing an unprecedented degree of fire safety awareness. This feature will also significantly enhance fire fighting operations as the origins of the fire can be clearly identified by the sensors activated by the fire and assistance will be directed to this specific location immediately. Building plans and other relevant data can also be incorporated into the information stream received by Bomba in the event of a fire.

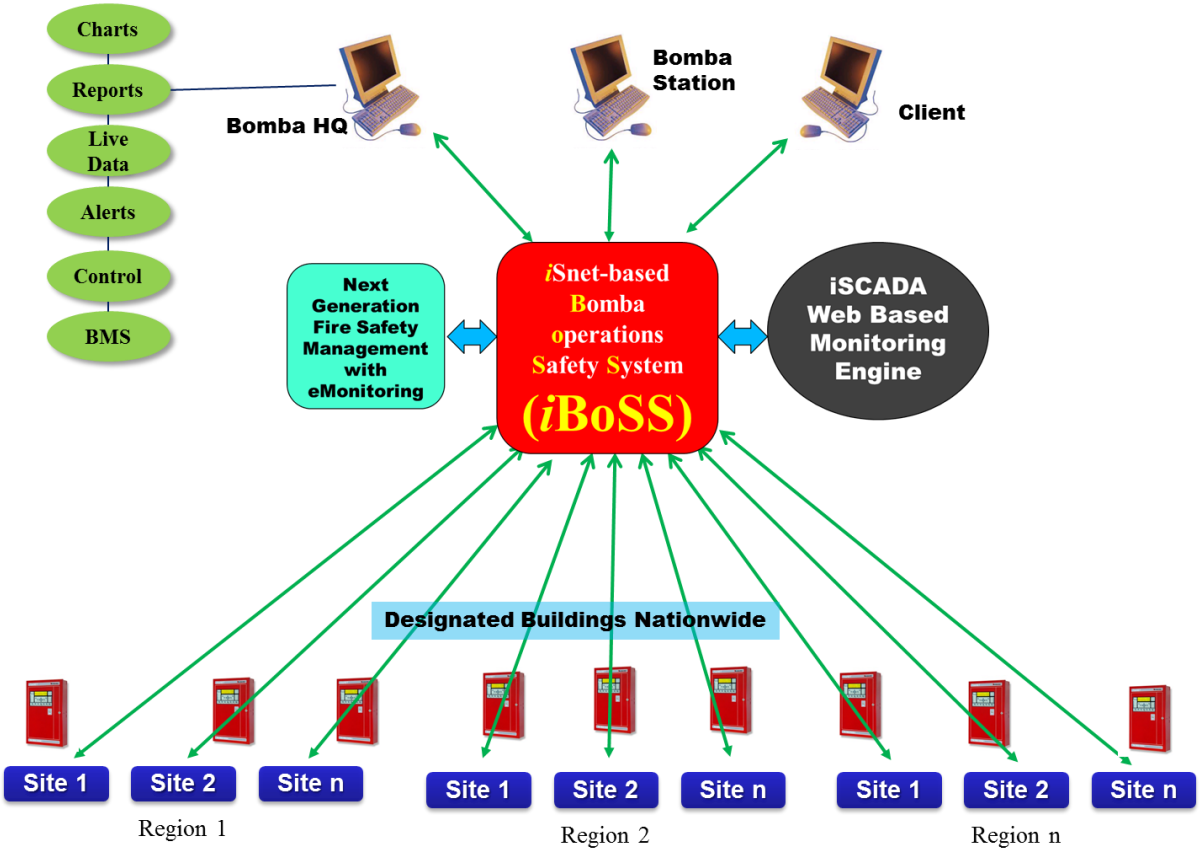




The technology platform used for the development of ***i*BOSS** is **iSCADA – internet-based Supervisory Control And Data Acquisition. iSCADA** was conceptualised and developed in Malaysia over a 12 year period beginning in 2000. Initially designed to monitor fire alarms (dry contacts only) on a nationwide basis, this web based technology platform has evolved to address many similar requirements in disparate industries and environments. Today, this platform is proven and is widely deployed to bring cost effectiveness, reliability and efficiency solutions into safety, security, environmental control and energy mitigation situations.



From *iSCADA* to *iBOSS*



Future proofing the key components of *i*BOSS

An important consideration of any advanced technology platform is the assurance that the platform will be able to serve well into the future with planned upgrades. The two key components of this ***i*BOSS** platform are designed to accommodate technologies which will become available in future. iSnet is a company that is well experienced with the implementation and integration of the latest internet (web) based technologies. As such, iSnet has developed a clear roadmap for the future enhancements of the key components of this ***i*BOSS** platform.

1) The iSnet Fire Safety Portal (iFSP)

This is the hardware located in the client premises. It consists of a power supply, protection relays, battery backup, data input channels (multiple data configuration capability), data storage (local), clock, data output channels and modem for internet connection. Several levels of iFSPs are available for accommodating the whole range of user requirements. iFSP Bomba is the base level unit for connection to fire alarm panels (FAP) with dry contact outputs only. iFSP Basic accommodates up to 10 inputs (analogue and digital or pulse signals) and 2 outputs. This is suitable for more sophisticated master FAP receiving signals from several slave FAPs. iFSP Comprehensive accepts digital serial signals and is suitable for FAPs with advanced addressable features using the industry standard ModBus protocol. All these are Type A iFSPs. The next generation Type B will feature advanced internet based communication interfaces that are only just being deployed in the mobile telephony industry.

2) *i*BOSS enterprise cloud computing technology platform

This is the software developed by iSnet based on the proven iSCADA cloud (internet) computing platform. It is essentially an enterprise level SCADA (supervisory control and data acquisition) platform which has been optimized to meet the unique requirements of Bomba Malaysia as their future national fire alarm monitoring solution. ***i*BOSS** has been extensively tested in a 'live' environment and meets or exceeds all of Bomba's specifications for such a platform. ***i*BOSS** is modular in its architecture and incorporates all features and functionalities found in generic SCADA systems but is customized to provide high resilience service as a national fire safety platform. Its web centric design allows for easy integration into the latest web based technologies especially the public user interfaces. A noteworthy feature of ***i*BOSS** is the flexibility of the platform and its upgradability. Version 1 of ***i*BOSS** is now stable and tested for almost 2 years in its intended usage environment. Version 2 is presently under development and will be largely browser based, incorporating the latest web technologies that are currently being rolled out.

iSnet

Technology & Product Evolution (*i*SCADA) in the Past

Server Version 1 | Gateway 1000 Series

2003

Server Version 2 | Gateway 2000 Series

2006

Server Version 3 | Gateway 3000 Series | Real time processing SW

2010

Technology & Product Evolution (*i*BOSS) in the Future

Server Software	Customer Hardware	
*i*BoSS Version 1	*i*FSP Type A	2012
*i*BoSS Version 2	*i*FSP Type B	2016
*i*BoSS Version 3	*i*FSP Type C	2020

In Summary

***i*BOSS** meets all the requirements of a National Fire Alarm Monitoring solution that is urgently needed by Bomba as a replacement for the technologically obsolete CMS. ***i*BOSS** was developed as a private initiative to address Bomba's very challenging requirements at no cost, risk or commitments from Bomba. It was the foresight of key Bomba and UKAS personnel that allowed ***i*BOSS** to reach its present state of maturity as a notable Malaysian technology accomplishment.

We believe that ***i*BOSS** is very beneficial to Bomba and the fire safety priority that Bomba has to deliver to the Malaysian public (individuals, business, government and industry). This proposal not only address all existing needs from Bomba but also address all clearly identified emerging requirements in a technologically responsible manner. Given the vast but unfortunate experience that Bomba has had with existing centralised fire alarm monitoring systems (acquired over 20 years of operation), this ***i*BOSS** system represents a breakthrough in fire safety technology for Bomba. This is a system that not only meets all existing identified Bomba requirements but will also allow Bomba to move forward into the future with full confidence that its adoption of this ***i*BOSS** solution has little or no risk as ***i*BOSS** is tested and proven. Bomba is additionally assured that ***i*BOSS** will address all of Bomba's emerging needs in the area of fire safety solution to be implemented in future without a need to change the underlying technology platform since 'cloud' computing is the future. We also need to recognise that this system was conceived and fully conceptualised in Malaysia to accommodate the unique needs of Bomba Malaysia. ***i*BOSS** is therefore a Malaysian system, fully developed, deployed and tested in its intended operating environment. As such, we have demonstrated that a smart private-public partnership can and has resulted in a significant technology accomplishment for Malaysia.

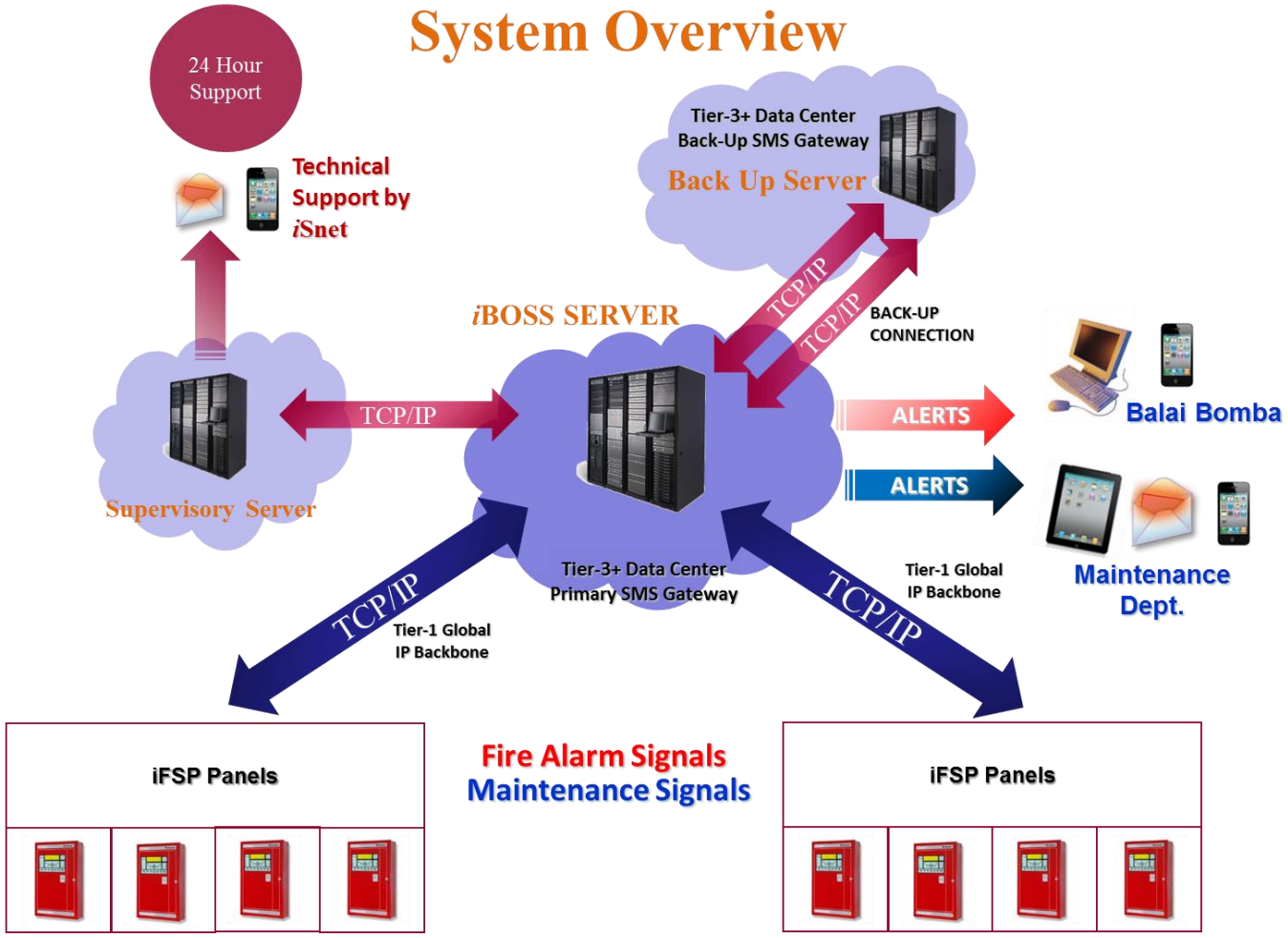
Bomba needs to replace the existing Centralised Monitoring System (CMS) within the next few years and this has become an urgent issue. With ***i*BOSS**, Bomba now has a solution that it can confidently move forward with to meet its commitments to the Malaysian public well into the future.

December 2013

*i*BOSS in March 2016 - Update

In Dec 2015, iSnet was awarded the contract for deploying the complete ***i*BOSS** solution as a replacement for the CMS. This award followed an open tender exercise by Bomba and iSnet is presently the only company providing this service. Bomba has named this new system the **SISTEM PENGAWASAN KEBAKARAN AUTOMATIK (SPKA).**

The **SPKA** will be deployed throughout the country after a short transition period where new processes and procedures will be introduced to ensure the smooth implementation of this fourth generation nationwide fire alarm monitoring solution. Version 2 of ***i*BOSS** will be ready by May 2016 and this is an advanced browser based design using the latest web tools. A system overview diagram is displayed below.



Security of *i*BOSS cloud computing platform

The security of cloud computing platform is very important in this day and age, as many corporations' most valuable data is being stored on servers all across the globe. Keeping ***i*BOSS** data safe and secure as well as ensuring the integrity of this data is of utmost importance.

In view of this, iSnet has made sure that the ***i*BOSS** data stored on the cloud platform is enveloped within highly secure and practically impenetrable physical and digital security systems. Constant upgrades of server security ensures that ***i*BOSS** is equipped with the latest such tools in the market. Complemented by continuous monitoring of server security integrity to detect and prevent all attempts to gain unauthorized access, this underlying ***i*BOSS** security environment is a best-in-class implementation.

Physical Security

While web servers host data that is in a 'cloud', there still needs to be physical servers for that data to be hosted on. These physical servers are susceptible to physical damage, theft, failure, etc.

In a cloud platform, it is tough for anyone to know where exactly the complete data set resides, as the data is usually spread across different servers in different locations or data centers.

Each data center is guarded by well trained, 24 hour security teams. In addition to this, there is a highly secure, 2-factor authentication process that needs to be completed before anyone is even allowed into the facility, ensuring that only authorized personnel have access to the server banks.

Due to the nature of the cloud platform and tight security in data centre, it is very hard for anyone to pinpoint the location of a particular server, and that means it is near impossible for anyone wanting to physically steal or download the data.

Digital Security

Cloud Servers are, by design, meant to be connected to the internet. This presents many potential dangers to the ***i*BOSS** data being saved on those servers. They could be susceptible to hacking, theft, deletion, data corruption, etc. However, the ***i*BOSS** data that is kept in our servers are protected by some of the best, state of the art digital security in the world.

Passkey Protection

***i*BOSS** data will be secured behind a passkey protected system that will only allow access to those who have the exact, unique passcode that is generated when the server is set up. The server provider then immediately deletes their copy of the passkey, making it impossible for anyone to hack in and steal your passkey from the server provider. The protection is not like username and password log-in systems that can be compromised in a brute attack by hackers as no hacker can access your data without the passkey. This is currently the most advanced methodology for internet based access control. iSnet constantly monitors all developments in server security and will adopt the latest protection technology in our servers.

Individual Firewall Settings

An additional security system in place is the ability to choose which digital access ports are open to public access. There are designated ports that handle various different types of traffic into the server, and the cloud computing platform allows individual control over which of these ports are open and which are closed off. This effectively limits the options for hackers to attack our systems. The ***i*BOSS** platform has a unique port assignment that severely limits options for hostile penetration attempts. This is a high security and high resilience platform incorporating all the industry best practises for security and reliability.

Data from Devices is Not Human Readable

The data that is transmitted from the device to the server is encrypted, which means that you need to possess the correct encryption key to decipher it. However, even if you were able to obtain the correct encryption key, the decoded data would not be understandable to humans. The data is not transmitted in simple terms, for example a triggered event could be transmitted as number 128, and then another different event could be transmitted as 80. This 2 factor security ensures that data cannot be intercepted and stolen on route to the server. The data will be translated by the server into readable data.

Database Protection

The database in ***i*BOSS** is protected behind a three layers of protection.

The first layer is a public firewall. This firewall prevents any unauthorized personnel from accessing the Virtual Private Network (VPN) without the proper certification or port.

The second level is the VPN itself. Within this VPN sits the ***i*BOSS** Application Server. To access this server, users will be prompted to enter a username, password, and IP address.

The final level is a Private Firewall that can only be accessed once the user has entered the ***i*BOSS** Application Server. To bypass this final level of security, the user will have to enter a username, password, IP address and the correct port. Only when all 4 criteria are correct, will the user be granted access to the Database.

Cloud Computing Platform Certification

The ***i*BOSS** servers operate in a data centre environment which conforms to the following internationally accepted certifications.

Deploying the Sistem Pengawasan Kebakaran Automatik (SPKA)

A. *i*BOSS – Moving Bomba into the future

B. Introduction: What is SPKA

- Background

  Under the Fire Safety Act 1988 all 'designated buildings' are required to have their Fire Alarm System (FAS) directly linked to and monitored by Jabatan Bomba dan Penyelamat Malaysia (JBPM - Bomba). The issuance of a Certificate of Fitness (CF) including Bomba Fire Certificate requires the 'designated building' to be in compliance with the Fire Safety Act, in line with the guidelines described in the Uniform Building By-Laws 1984. As the authorized statutory organization vested with fire safety responsibilities, BOMBA implemented the Centralised Monitoring System (CMS) for Fire Alarm Monitoring service to 'designated building' owners under a concession that was awarded more than 20 years ago.

  Moving forward, with the rapid advancement in Information and Communications Technology over the years, and also to meet and exceed excellence in fire safety and firefighting operations, BOMBA initiated the Sistem Pengawasan Kebakaran Automatik (SPKA) project to replace the CMS.

- The SPKA project development

  Requests for Proposals (RFP) were sent out by BOMBA based on stringent specifications to procure, select, test and approve for deployment of a state-of-the-art technology (with capability to keep up with future technology advancements) that meets Bomba's needs.

- The ***i*BOSS** technology

  BOMBA subsequently identified and approved the iSNET-based Bomba Operations Safety System (***i*BOSS**) from the RFP as the selected SPKA.

- The ***i*BOSS** advanced features

  ***i*BOSS** is a 100% Malaysian MSC based (conceptualised, developed, designed and deployed) technology that operates on a Hosted Service platform fully supported, managed and supervised by the technology provider (iSnet – iSCADA Net Sdn.Bhd.).
  The Hosted Service solution operates within an advanced cloud computing platform, supporting the latest communications technology e.g. EDGE, LTE, HSPA, 3G, and GPRS, etc. and comes with enhanced (upgradable/expandable) capabilities to address future requirements from BOMBA.
  ***i*BOSS** incorporates a superior tested and proven False Fire Alarm original design feature (patent pending) that will effectively benefit designated building owners on fire safety and also BOMBA operations.
  ***i*BOSS** has excellent user interfaces to allow designated building owners to directly view and receive real-time information on the maintenance effectiveness of their fire safety systems.
  ***i*BOSS** allows designated building owners to directly update critical fire safety information from their individual accounts and comply with statutory regulations at no additional cost.

C. Why implement SPKA

- Technology evolvement

  Obsolescence of the CMS was a key concern. Although the original design was suitable for conventional Fire Alarm Systems, it is no longer capable of meeting current requirements. CMS is not technologically upgradable for advanced addressable Fire Alarm Systems or web based services. In addition, fixed line communications has gradually been replaced by more advanced communications solutions e.g. fiber optics and mobile networks.

- ***i*BOSS**

  Bomba took on the challenge of implementing a state of the art solution for nationwide fire safety monitoring by being innovative without compromising the fire safety responsibility Bomba has been entrusted with. Several years ago, Bomba initiated a search for a fire safety solution that will meet Bomba's needs well into the future. This has resulted in a Bomba optimised, Malaysian developed solution which is ***i*BOSS**, the technology behind SPKA. iBOSS is a solution comprehensively tested over 3 years in its intended operational environment so Bomba has no risk in deployment and implementation.

- More than just Fire Alarms

  Moving into the future, fire safety services is not just about fire alarms but must include a holistic condition monitoring of installed Fire Alarm Systems that demands and delivers effective maintenance; a concept being introduced by BOMBA called e-Maintenance.

- Social responsibility on Fire Safety

  Fire safety cannot just be the responsibility of BOMBA even though they are tasked with fire safety and firefighting responsibilities as a public service.
  Designated Building owners also have a major role to play in ensuring fire safety in their premises as a social responsibility to the public.

- Legal responsibility

  The Fire Safety Act & Uniform Building Bylaws describes the mandatory requirement for designated buildings to be certified for conformance. The annually conducted certification will significantly improve fire safety awareness with clearly demarcated roles (Bomba and designated building owners) and responsibilities for ensuring fire safety.

D. Who needs SPKA

- All 'designated buildings'

  With the introduction of the CMS more than 20 years ago many 'designated buildings" have complied with BOMBA fire safety regulations as required by law. All these CMS will now need to be replaced with the SPKA.
  Other 'designated buildings' that were constructed in the course of national development will require the SPKA to be included.

- 'Non-designated buildings'

  Those buildings not categorised as 'designated buildings' but fall under the general public fire safety considerations e.g. Universities, Hospitals, Government buildings, etc. will also require the SPKA

  Special category buildings and premises that will also require the SPKA are e.g. Heritage buildings, Royalty premises, religious buildings, critical high security / technology buildings.

E. What about the existing CMS

- CMS validity

  The CMS service including its technology, installations and concession shall cease to be applicable and valid for its intended use and purpose upon implementation date of SPKA. This is now an obsolete system.

- Conversion to SPKA

  Conversion from all existing CMS to SPKA is mandatory. Fire safety is compromised unless all designated buildings are upgraded to the SPKA. Bomba will, at its discretion provide relief for building owners with justifiable reasons for delay in upgrading to the SPKA under Bomba directions.

  During the transition period required for replacement of SPKA by the existing designated buildings (already with valid CMS service contracts), BOMBA will consider granting validity period waivers (just for this SPKA service) on Fire Certificates for the respective premises until they install the SPKA within a reasonable timeframe. However, Bomba will insist on verifiable evidence of additional vigilance in fire safety to approve this delay in deploying SPKA. This is in the best interest of all parties involved in fire safety monitoring – Bomba; designated building owners and the SPKA technology supplier.

- **Cost of Conversion**

  The site unit (iFSP - Bomba) will be deployed at the same cost as the existing CMS equivalent unit. The monthly monitoring/maintenance cost remains the same although building owners enjoy much enhanced services. An additional benefit for building owners is that the previously onerous task of having to install a fixed communication line has been removed. The iFSP incorporates the latest mobile telecommunication technology which is integrated into the iFSP. Maintenance and testing cost of the iFSP is the responsibility of the designated building owner. Maintenance is undertaken by the SPKA technology supplier and testing is conducted by the fire alarm service provider. Overall, the cost to the building owners to deploy SPKA remains the same as with the obsolete CMS. A remarkable achievement considering that the existing cost structure was implemented more than 20 years ago.

The three parties (organisations) involved in the SPKA operation (***i*BOSS** technology provider/operator; the 'designated building' owner and Bomba) and their responsibilities are tabulated below.

Organisation	Responsibilities	Cost/benefit
Bomba	Receive incoming fire alarm signals from FAPs via iFSP and decide on appropriate action. Ensure that trained Bomba personnel are available to man the PGO on a 24/7 basis	Allows Bomba to carry out its duties more efficiently. **Firefighting** and **fire safety** are two of the three core Bomba objectives (the third is **rescue**). Cost for ongoing maintenance of iSTATION in PGO
SPKA provider *i*Snet ***i*BOSS**	Coordinate the deployment and proper operation of iFSP-Bomba site-unit into designated buildings. Provide Bomba with iSTATION, maintenance / training / upgrade services and other support for ***i*BOSS** solution. Deploy the ***i*BOSS** solution nationwide and maintain the Back end ***i*BOSS** server based infrastructure. Upgrade to ensure technology relevance.	Receives monthly maintenance fees from owners of designated buildings. Receives RM 2,500 for facilitating installation, testing and commissioning of iFSP site-unit for building owners. Provide iSTATION control console at no cost to Bomba.
'Designated Building' owner	Facilitate the installation of iFSP-Bomba site-unit into the appropriate location (usually next to the FAP). Ensure that 240VAC power supply and dry contact (from FAP) are available for connection to iFSP-Bomba site-unit. Ensure that proper operation of the site unit through periodic testing by fire alarm contractor.	Cost for dedicated communication line. Cost for iFSP site-unit testing, installation and commissioning. Cost for periodic testing of site unit. Cost of monthly maintenance and services for ***i*BOSS** connection to Bomba. Cost for the continuous maintenance of the site-unit. FAP is directly connected to local Bomba station for fire safety