RESEARCH ARTICLE OPEN ACCESS

Indexing Building Evaluation Criteria

ENG. TAREQ YOUSEF ALOMAIRI
Public Authority for Applied Education and Training

ABSTRACT
The purpose of this paper two fold. First and foremost it presents a background narrative on the origins, innovations and applications of novel structural automation technologies and the rarity of experts involved in research, development and practice of this field. The second part of this paper presents a rudimentary framework for a solution addressing this paucity – the creation of an interdisciplinary academic program at PAAET that will be the first ever in the region to address applied information communication technologies ICT in the design, planning, engineering and management of structural automation projects.
In doing so, we need also to define the level of implementation. This field, as all fields in ICT, have been loosely defined and most applications carry less weight in its implementation than what should be applied. This paper gives an attempt to define an indexing scheme by which we can easily classify such implementation and generate a ranking by which we can safely define its level of "Intelligence".

I. INTRODUCTION

As the Telecommunications Exchange examines the issue of "infrastructure" and "access" to advanced telecommunications technologies, consider incorporating into the definition of "infrastructure" the basic facilities in which we live and work. Those basic facilities are the structures; i.e., the physical buildings, in which we live and work. In that context, the issue of "access" should also be examined with recognition of buildings as part of the infrastructure needed for the expansion, growth and diffusion of advanced telecommunications technologies.
What we see, feel and touch in our home and work environments will inextricably influence our sensitivity to and receptiveness of advanced telecommunications technologies. By promoting the renovation and construction of those environments into "Smart or intelligent infrastructures", we may well be one of the most omnipotent and omnificent vehicles to advance diffusion and drive the demand side of the market.

iIndexing Factors

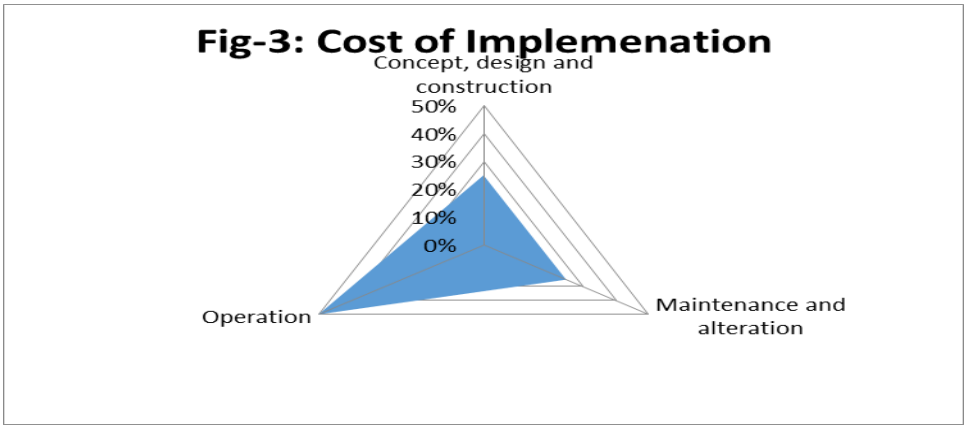
II. Reliability

Network reliability refers to the reliability of the overall network to provide communication in the event of failure of a component or components in the network. The term fault-tolerant is usually used to refer to how reliable a particular component (element) of a network is. The term fault-tolerant network, on the other hand, refers to how resilient the network is against the failure of a component.
Much research remains to be done to address network reliability in today's complex networking environment. We briefly touch on two areas in this regard: multi-service network architecture and software errors/attacks.

2.1 Networking environment is evolving to various services being provided over one IP network. Such services includes the Triple play (Voice, Video and Data) Thus, we are moving to an environment that we have coined the *multi service network* environment. In such environment, in each of these networking layers, different types of failures/attacks and responses are possible.
2.1.1 Availability: Network availability is measured to address the availability of a network in operational state.
2.1.2 Perform-ability: Measured to address the performance of a network under various failure states.
2.1.3 Capacity: The design of network survivability is extremely important for overall network reliability.
2.1.4 Fault Detection: The network capability of the alarm generation in the network to indicate the occurrence of any abnormal condition which may cause the reduction or loss of the element which is called a fault.
2.1.5 Fault restoration: The network element capability to provide the quality of services needed after the fault is occurred.
2.2 Software/protocol operations errors and software attacks encompass the other area where mechanisms are needed to provide network reliability. This subject is relatively new—research on intrusion detection mechanisms is currently being explored to determine if an attack has occurred. Also, we need to see more work that helps us understand how severely the network will be affected in terms of network performance if a software attack or protocol

failure occurs and how to recover from this anomaly. Also, the network architecture should be revisited to identify if there are ways to reconfigure the network after an attack so that parts of the network remains operational.

2.2.1 Restoration: Software capability to identify where the software attack is coming from so to stop such attack.



III. Scalability

Is a desirable property of a system, a network or a process, which indicates its ability to either handle growing amounts of work in a graceful manner, or to be readily enlarged? A system, whose performance improves after adding hardware, proportionally to the capacity added, is said to be a scalable system**.**

Scalability can be measured in various dimensions, such as:

3.1 Load scalability:A distributed system should make it easy to expand and contract its resource pool to accommodate heavier or lighter loads.

3.2 Geographic scalability:A geographically scalable system is one that maintains its usefulness and usability, regardless of how far apart its users or resources.

3.3 Administrative scalability: No matter how many different organizations need to share a single distributed system, it should still be easy to use and manage.

IV. Security

4.1 Network Security:

4.1.1 Network Scanning: The term network scanning refers to the availability of a *port scanner* to identify all hosts potentially connected to an organization's network, the network services operating on those hosts, such as the file transfer protocol (FTP) and hypertext transfer protocol (HTTP), and the specific application running the identified service, Internet Information Server (IIS) and Apache for the HTTP service. The result of the scan is a comprehensive list of all active hosts and services, printers, switches, and routers operating in the address space scanned by the port-scanning tool.

The network scanning provides the following capabilities:

- Check for unauthorized hosts connected to the organization's network,
- Identify vulnerable services,
- Identify deviations from the allowed services defined in the organization's security policy,
- Prepare for penetration testing,
- Assist in the configuration of the intrusion detection system (IDS), and
- Collect forensics evidence.

Network scanning results should be documented and identified deficiencies corrected.

4.1.2 Vulnerability Scanning: The availability of a vulnerability scanner that identifies hosts and open ports and provides information on the associated vulnerabilities (as opposed to relying on human interpretation of the results). It also provides information on mitigating discovered vulnerabilities.

Vulnerability scanners provide the following capabilities:

- Identifying active hosts on network
- Identifying active and vulnerable services (ports) on hosts.
- Identifying applications and banner grabbing.
- Identifying operating systems.
- Identifying vulnerabilities associated with discovered operating systems and applications.
- Identifying miss-configured settings.
- Testing compliance with host application usage/security policies.

- Establishing a foundation for penetration testing.

Vulnerability scanning results should be documented and discovered deficiencies corrected.

4.1.3 Password Cracking: The availability of a password cracking programs that is used to identify weak passwords. Password cracking verifies that users are employing sufficiently strong passwords. Passwords are generally stored and transmitted in an encrypted form called a hash. When a user logs on to a computer/system and enters a password, a hash is generated and compared to a stored hash. If the entered and the stored hashes match, the user is authenticated.

4.1.4 Log Reviews: System logs shall be used to identify deviations from the organization's security policy, including firewall logs, IDS logs, server logs, and any other logs that are collecting audit data on systems and networks. While not traditionally considered a testing activity, log review and analysis can provide a dynamic picture of ongoing system activities that can be compared with the intent and content of the security policy. Essentially, audit logs can be used to validate that the system is operating according to policies.

4.1.5 File Integrity Checkers: A file integrity checker computes and stores a checksum for every guarded file and establishes a database of file checksums. It provides a tool for the system administrator to recognize changes to files, particularly unauthorized changes. Stored checksums should be recomputed regularly to test the current value against the stored value to identify any file modifications.

4.1.6 Virus Detectors: All organizations are at risk of "contracting" computer viruses, Trojans and worms if they are connected to the Internet, or use removable media (e.g., floppy disks and CD-ROMs), or use shareware/freeware software. The impact of a virus, Trojan, or worm can be as harmless as a pop-up message on a computer screen, or as destructive as deleting all the files on a hard drive. With any malicious code, there is also the risk of exposing or destroying sensitive or confidential information. There are two primary types of anti-virus programs should be available: those that are installed on the network infrastructure and those that are installed on end-user machines.

The most important aspect of virus detection software is frequent regular updates of virus definition files and on-demand updates when a major virus is known to be spreading throughout the Internet. When the database is updated frequently, more viruses will be detected by the anti-virus software. If these preliminary steps are taken, the chances of a major virus infection are minimized.

The following steps are recommended:

- Virus definition files should be updated at least weekly and whenever a major outbreak of a new virus occurs.
- The anti-virus software should be configured to run continuously in the background and use heuristics, if available to look for viruses.
- After the virus definition files are updated, a full system scan should be performed.

4.1.7 War Dialing: In a well-configured network, unauthorized modems are often an overlooked vulnerability. These unauthorized modems provide a means to bypass most or all of the security measures in place. There are several software packages available that allow attackers and network administrators to dial large blocks of phone numbers in search of available modems. This process is called war dialing. Certain war dialers will even attempt some limited automatic hacking when a modem is discovered. All will provide a report on the "discovered" numbers with modems. War dialing should be conducted at least annually and performed after-hours to limit potential disruption to employees (this has to be balanced with the possibility that modems may be turned off after hours and, therefore, will not be detected). The check should include all numbers that belong to an organization, except those that could be impacted negatively by receiving a large number of calls (e.g., 24-hour operation centers, emergency numbers, etc.). Most war dialing software allows the tester to exempt particular numbers from the calling list.

4.1.8 War Driving: Wireless LANs, which may provide attackers the means to bypass Firewalls and IDS, are rapidly replacing unauthorized modems as the most popular back door into networks (if not placed outside the firewall).

The frequency for testing wireless networks will depend on several factors:

- Physical factors of the location to be tested (e.g., a building located on a secure installation thousands of feet from any public access area will need testing less often than an office located in a busy downtown office district).
- The threat level faced by the organization.
- Organizational control over network resources (e.g., an organization with tight central control over the network may need to test less often than with a very decentralized network support structure).
- The use of more robust security techniques in the network, such as the WPA (Wi-Fi Protected Access) or RSN (Robust Security Network).

- Sensitivity of the data on the organizations network.

4.1.9 Penetration Testing: The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers. Penetration testing should be performed after careful consideration, notification, and planning.

4.2 Physical Security

4.2.0 Surveillance system

4.2.1 Camera image quality Superior image quality enables the user to more closely follow details and changes in images, making for better and faster decisions to more effectively safeguard people and property. It also ensures greater accuracy for automated analysis and alarm tools, such as motion detection and other built-in intelligence functions. Camera image quality depends on many factors including light sensitivity, Level of image clarity, high quality lens and image quality when there is motion in the image.

4.2.2 Camera Compression fully compliant with JPEG and MPEG4 standards 100% compliance with a standard ensures the flexibility to use video for many different applications and guarantees that you can view the video 10 years from now or longer. If a camera uses one company's proprietary compression technology and that company goes out of business, the end user could be out of luck. Following a standard ensures that you will have long-term access.

4.2.3 System Tools for managing large deployments: The surveillance system should have tools to manage upgrades to update all the cameras in the facility and their estimates for cost and downtime should be clear and measurable upfront. The system should also be capable to automatically locate all network video devices and monitor the status of those devices.

4.2.4 Progressive Scan sensor Progressive scan involves exposing and capturing the entire image simultaneously. In a progressive scan image there is virtually no "flickering" effect, no jagged edges or blurring. In a video surveillance application, this is critical to enable users to view detail within a moving image such as a person running away. Progressive scanning consistently produces the best results in clarity and recognizing important details.

4.2.5 Power over Ethernet (PoE): gives the capability to power the surveillance system, including the cameras, from the server room and to use UPS (Uninterruptible Power Supply), keeping it operational even during power outages.

4.2.6 Distributed Intelligence: The camera intelligence is the ability to decide when to send and process the video. Network camera should act as an intelligent gatekeeper and allow for the deployment of more cameras that utilize intelligent video. By definition, a network camera is intelligent because it includes processing power and has functions such as motion detection, I/O ports and event handling.

4.3 Operations Security

Operations Security is the systematic process of denying potential adversaries information about capabilities and intentions of the organization. This is accomplished by identifying, controlling, and protecting generally non-sensitive activities concerning planning and execution of sensitive activities.

4.4 Security Policies and Procedures

The policies and procedures by which security is administered provide the basis for identifying and resolving issues, establishes the standards of reference for policy implementation, and defines and communicates roles, responsibilities, authorities and accountabilities (R2A2) for all individuals and organizations which interface with critical systems. They provide the backbone for decisions and day-to-day security operations. The policies and procedures should be reviewed to determine whether they (1) address the key factors affecting security, (2) will enable effective compliance, implementation and enforcement, (3) reference or conform to established standards, (4) provide clear and comprehensive guidance .

V. Accessibility

5.1 Connectivity: This term refers to the capacity of technology to access rich resources both within and beyond the infrastructure. "last-mile connections" from buildings to telecommunications sources must be in place if the real estate to access the wealth of free and low-cost resources on the internet.

5.2 Ubiquity: Enough computers, printers, media technologies, and other equipment must be readily available within the district and school so that all users can access them to solve problems, communicate, collaborate, and exchange data.

5.3 Interactivity: This term refers to the interaction that occurs when tenants and users teachers communicate and collaborate in diverse ways (e.g., exchanging data in different formats, publishing)

5.4 Equity of use: Educational technology should provide all students with access to rich and challenging learning opportunities and instruction that is interactive and generative.

VI. Operability

6.1 Interoperability: This term refers to the capacity of technology to easily exchange data with and connect to other hardware and software in order to provide the greatest access for all users

6.2 Open Architecture: this feature allows users to access data using different (third party) hardware and software; it also allows users to modify the system, sometimes dramatically.

6.3 Transparency: A technology is "transparent" when users are essentially unaware of the procedures used by the hardware and software for changing programs and multitasking (i.e., allowing users to work on several tasks at once).

6.4 Operating System and Applications: The operating system of the Servers and the workstations in the building including the license of that operating system, in addition to the applications installed in the system to serve the business requirements.

VII. Organization of resources

7.1 Distributed resources: Organizations assume (1) that intelligence does not reside in individuals but is socially constructed through collaborative efforts and (2) that the resources that shape and enable activities (to build socially constructed knowledge) are distributed across people, environments, and situations (pea 1993, p. 50). This feature allows users to access resources from anywhere in a local system (i.e., local area networks) or from external sources, such as the internet.

7.2 User Contributions: Users can contribute information, products and services to a system from multiple sources in order to share common data sets or problem spaces. Such systems have "Distributed logic" – the logic of preparing documents and artifacts for the systems resides in the user who must comprehend and build links within and among documents or data sets. Thus users must understand how the resources are distributed. In such as system, users control when they make contributions and what those contributions are.

7.3 Collaborative projects and Co-Investigations: Examples of this capacity include on-line conferences and bulletin boards with asynchronous communications capability, access to remote files and joint products, and the ability to communicate synchronously with two or more computers that are accessing the same file at the same time. All of these examples also promote collaboration. Other examples include programs that help groups from consensus, brainstorm, outline, develop plans, schedule meetings, monitor programs on group objectives, and develop joint products. Such systems inherently afford the user the opportunity to examine data, problems, and decisions from multiple perspectives.

VIII. Engagement

8.1 Provide challenging tasks, opportunities and experiences: The system has the capacity to:

- Present complex problems and cases, links to challenging activities, and unique repositories from information as well as opportunities to examine contrasting events or data sets
- Access experts, peers, community members, and/or other users who can guide, mentor, tutor, mediate, broker, share, inform, and involve users in productive and meaningful ways.
- Use the richest media resources (e.g. images, audio, video, 3D, Virtual reality) for data manipulation and for presentations.
- Provide tools for interactive browsing, searching, and authoring.

8.2 Learning by doing: Tools that use authentic, goals-based scenarios; problems anchored or embedded in challenging narrative situations; or simulations allow users to develop expertise using real world problems and resources, Such tools let the user plan, reflect, make decisions, experience the consequences of actions, change directions, and examine alternative solutions and assumptions.

8.3 Guided participation: Some software uses Socratic questioning, intelligent usage, and diagnosis and guided analysis of errors. Such systems often respond to users responses by customizing their content to the particular interests or usage style of the user. These tools allow the users to anticipate problems, subsequent events, and others' thoughts.

8.4 Just in time and Just enough: Systems such as Hypertext call for nonlinear learning and thinking, and they provide multiple points of entry so that users can quickly access specific chunks of information. These systems also may be customized for users with different levels of expertise by adapting information access, help commands, and user control. For example, a system can be designed so that people with little time and immediate problems have easy access to simple, useful information, while people with time for reflection and exploration can access more complex information.

IX. Ease of Use

9.1 User Friendliness and effective help: Technologies with these characteristics are truly informative, well organized, and context specific.

9.2 Speed: Systems that process information quickly and provide feedback about delays are easier to use than systems that are slow and do not provide such feedback.

9.3 User Control: This term refers to a user's ability to access tools, information resources, experiences and opportunities on demand and use them to solve

problems, make decisions, and create products. These features motivate users and promote exploration.

9.4 Training and support: Users must be trained to use a technology to solve problems, create products, and so on. Further, training and support shold be available both on-and off-site.

X. Functionality

10.1 Multimedia Technologies: Users should have access to equipment such as color printers, video cameras and editing equipment, facsimile machines, audio recording and editing equipment, and various graphics.

10.2 Generic Tools: users should also learn to use such basic or generic tools as databases, spread sheets and word processing systems.

10.3 Project design and Implementation: the most functional software help users to set goals and benchmarks, create and monitor budgets, conduct research and development, prepare analysis and presentations, develop dissemination skills, and market.

10.4 Tools that Create New Tools: Some tools, such as wizard and Mosaic, help users to develop programming and authoring skills so they can create new programs and tools for others to use. The development of these abilities contrasts sharply with traditional approaches to technology in which students learned outmoded programming languages.

XI. Manageability

11.1.0 Network Management

11.1.1 Performance Management: The goal of performance management is to measure and make available various aspects of network performance so that inter-network performance can be maintained at an acceptable level.

Management entities continually monitor performance variables and when a performance threshold is exceeded, an alert is generated and sent to the network management system.

When performance becomes unacceptable because of an exceeded defined threshold, the system reacts by sending a message. Network simulation can be used to project how network growth will affect performance metrics. Such simulation can alert administrators to impending problems so that counteractive measures can be taken.

11.1.2 Configuration Management: The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Each network device has a variety of version information associated with it. Configuration management subsystems store this information in a database for easy access. When a problem occurs, this database can be searched for clues that may help solve the problem.

11.1.3 Fault Management: The goal of fault management is to detect, log, notify users of, and automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

Fault management involves first determining symptoms and isolating the problem. Then the problem is fixed and the solution is tested on all-important subsystems. Finally, the detection and resolution of the problem is recorded.

11.1.4 Security Management: The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem can monitor users logging on to a network resource and can refuse access to those who enter inappropriate access codes.

Security management subsystems perform several functions. They identify sensitive network resources (including systems, files, and other entities) and determine mappings between sensitive network resources and user sets. They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources.

11.2 Cabling management

11.2.1 Labeling: This term refers to the definition of the connection by using the labeling technique at faceplates, patch panel and cable.

11.2.2 Guidance: The cabling infrastructure system capability to senses the insertion and removal of patch cord plugs. So, when a cord is added, the System registers the connection, ensuring up-to-the-minute information on connectivity is always available.

11.2.3 Protection: This phrase refers to thecable protection consideration in term of fire prevention and MUD resistance for the cable coating jacket and interference protection produced from many sources by using the appropriate grounding technique.

11.3 WLAN Management

11.3.1 Discovering the WLAN devices: WLAN Management software has the capability to discover the WLAN devices, but the effectiveness varies with the approach taken. Few software depend purely on the wired side information resulting in partial discovery of the WLAN devices. The wired side information help in discovering high-end access points, which have

proper SNMP support, but not those SOHO grade ones that often bring security problems. To overcome this problem, WiFi Manager employs multiple techniques such as ICMP, SNMP, Telnet, CLI, AP Scan, RF Scan, CDP etc., to discover devices in your WLAN. The dedicated RF sensors that come as additional hardware components with WiFi Manager perform the RF scan and discover every element that is transmitting on the air and ensures a 100% complete discovery of WLAN devices.

11.3.2 Monitoring the WLAN devices: It can be several folds starting with the basic availability monitoring to fault monitoring, performance monitoring, and service monitoring. WLAN management software includes detailed monitoring functions such as:

- **Trap reception:** When the WLAN device sends a trap, WiFi Manager will receive it and alert the operator
- **Severity based color-coded alarms:**WiFi Manager assigns severity to every network failure and generates color-coded alarms
- **Email-based notification:**WiFi Manager notifies operators through email when a fault occurs
- **Threshold monitoring:**WiFi Manager allows you to set threshold values for key parameters and alerts you when the actual values exceed the set threshold levels.
- **Service monitoring:**WiFi Manager monitors the services running in your Access Points such as the web service.
- **Performance monitoring:**WiFi Manager monitors the WLAN devices for various parameters such as Tx/Rx traffic and utilization, data rate, channel usage, errors etc.
- **Periodic assessment:**WiFi Manager sends reports at a specified time periodically.

11.3.3 Configuring the WLAN devices: The WLAN management software supports configuration from any Web browser. But as the WLAN grows in size the number of access points increases resulting in more UIs to look at. Hence the biggest value that WLAN management software can give is BULK configuration of access points. Operators should be able to group access points and apply configurations at one click. WiFi Manager addresses this problem in two ways. First it supports group based configuration. Second it supports template-based configuration. Operators can pick a template, fill in the relevant values, and then apply the template to a selective access points.

WLAN Management software should also enable operator to upgrade the access point firmware with as much as ease as configuring the SSID or channel settings.

11.4 Building Management

11.4.1 Equipment Monitoring: here are two fundamental reasons to monitor equipment. One is to alert the operator in the event of a failure or potential failure; the other is to gather data to evaluate maintenance and operational effectiveness.

11.4.2 Environmental and Energy Reporting :

Just as equipment monitoring provides information vital to operating the equipmentbeing monitored, it is necessary for the environmental and energy consumption information within a single building or campus to be effectively communicated.

The ability to access and communicate both real-time and historical data between energy-using end devices and environmental monitoring devices (the building management system)—and enterprise computing applications—had not kept pace with other IT developments. Convergence provides the pipeline to deliver this information anywhere, anytime by using Web technologies as the delivery mechanism and avoiding the use of dedicated workstations that confine users to a chair in a control room or office.

11.4.3 Alarm Transmission: The purpose of an alarm is notification. In this era of mobile work environments and multiple task assignments, it is important for alarms to track the intended recipient via any communication media such as cell phones, pagers, wireless laptops, PDAs and other multimedia enhanced personal devices. The system shall have the ability to communicate and share vital information with individuals or groups of individuals across the globe. And those same individuals can find a computer terminal or Wi-Fi hot spot to get additional information about an alarm that they have received.

11.4.4 Database Sharing: Database of the building management system using Oracle or Microsoft SQL database structure is easily exchanged throughout the enterprise.

11.4.4.1 Equipment Time Sharing

When all building systems are truly interconnected and can speak the same language, it is possible for computers and devices to serve multiple purposes. For example, a television camera can be used for more than just security. That same camera also can monitor a device that indicates whether a sump is high or low. A small box in the corner of the sump will have a raised flag if a problem in the unit needs attention. Monitoring this via the security camera eliminates the need for visual inspection, thus increasing employee productivity.

Occupancy sensors that turn lights on could be synchronized with the security system. The same could be true for air quality, by pumping the right amount of fresh air into a building at the right time. We could also determine whether a particular area within a facility is using too much energy based on the occupancy.

11.4.4.2 Remote Access

Connecting a computer to the Web with a cell phone, wireless access of a PDA to the network in a hotel, or simply walking into the Internet café gives anyone access to this capability. Care must be taken by systems providers to ensure a capable and straightforward user interface to leverage these capabilities.

11.4.5 Inventory Management: This term refers to the documentation of the property technology assets including Hardware and Software and the process of keeping the inventory up-to-date.

11.4.6 Network Management for IP Telephony environments:

11.4.6.1IP Telephony Environment Monitor

- Monitors the health of IP telephony environments including underlying IP fabric, IP telephony infrastructure and applications.
- "Out of the box" intelligence about events and issues that can impact IP telephony reliability and operations.
- Support of all current IP telephony components: soft switch, Media Servers, Gateways, Gatekeepers, IPT applications and IP telephones.

11.4.6.2 QoS Policy Manager

- Centralized and automated QoS analysis, reporting, and provisioning
- Traffic monitoring for setting and validating QoS, with real time QoS feedback for top applications and service classes.
- Enables classification and enforcement in a converged voice/video/data network by selectively activating QoS mechanisms on intelligently grouped LAN and WAN interfaces.
- Ensures strict priority for voice traffic with step-by-step wizard that intelligently maps network devices to pre-defined IP Telephony templates based on QoS design recommendations.

11.4.6.3 Voice Manager

- Creates and maintains dial plans on voice-enabled routers.
- Provides a tool to gather call statistics and other performance information for VOIP, VoFR and VoATM implementations.

XII. Mobility

12.1 Voice Over WLAN: This term refers to the possibility to send and receive telephone calls over a Wi-Fi network which offers mobility, coverage where a cell phone can't reach and potential cost savings over cellular phones, while making use of existing wireless networks.

12.2 GSM Integration: The integration of the GSM mobile phone with the IP telephony system.

12.3 Wireless Access Points: This term refers to the wireless networking that allows users to access network resources from nearly any convenient location within their primary networking environment and can access the internet even outside their normal work environment.

12.4 Storage

12.4.1 Capacity: The capacity of the storage available and how much it can expands.

12.4.2 Consolidation: Storage Consolidation refers to the activities associated with increasing the number of devices (servers, storage arrays, tape drives, etc.) that have access to the storage infrastructure while simplifying existing storage topology layouts.

12.4.3 Security: Storage Security refers to processes and solution features that protect the integrity and availability of data stored on storage networks. There are four aspects to a comprehensive Storage security solution:

1. Secure roles-based management with centralized authentication, authorization and logging of all changes
2. Centralized authentication of devices connected to the network to ensure that only authorized devices can be connected to the network
3. Traffic isolation and access controls that ensures that a device connected to the network can securely send/receive its data and is protected from activities of other devices in the network
4. Encryption of all data leaving the storage network for business continuance, remote vaulting and backup

12.4.4 Disaster Recovery: Business Continuance and Disaster Recovery refers to the processes and procedures organization puts in place to avoid mission-critical business interruption or data loss during any type of disaster.

12.4.5 Bandwidth: This is the speed of the storage network. The problem is that everything in the path always slows down to the speed of the slowest part in the path. In order to reduce issues with speed negotiation between components, set all the components at a fixed speed.

12.4.6 Distance and Connections: Distance issues can be the cause of all kinds of flaky intermittent gremlin-type problems. In a 1 Gb SAN, there can be no more than 500 meters between devices. Two Gb limits you to 300 meters; 4 Gb is even shorter. When

upgrading from 2 Gb to 4 Gb, you need to make sure the distance between your hosts and SAN storage is still within the appropriate range.

When using a patch panel, signal loss is a concern. Each patch can lose about .5 decibels (db) per connection, Try and keep total loss under 4.0 db for all connections per link. Limiting signal loss is key, so try not to use more than two patch panel connections between your server and the storage in a SAN.

12.4.7 Latency: Is caused by too much distance or too many hops between your servers and storage. A hop is defined as a connection through a switch. If you connect a server through one switch, that equals one hop. Hops can add milliseconds of delay through the fabric.

12.4.8 Congestion: occurs when there are too many things happening at once over the same connection. Congestion in a Storage system is usually called "over subscription". The storage system infrastructure is designed with separate backup fabric to avoid congestion and to provide enough connections to satisfy the bandwidth's requirements.

12.4.9 Cable Issues: Using the proper design and standards for the storage system cabling to avoid signal losses caused by mismatched cable size (core size) or excessive crimping or bending.

XIII. Administration

13.1 System Administrator: Defining the duties, responsibilities and the authority of the network administrators in addition to their background, training and knowledge.

13.2 System Maintenance: The procedure for proactive monitoring of the capacity and performance as well as the procedure that is followed when maintenance is required.

13.3 Problem Management: The processes and procedures of the problem identification, reporting, recording, investigation, escalation and resolution.

13.4 Change Management: The procedure of requesting, approving, testing and installing changes in the network whether for software or hardware.

XIV. Backup and Recovery

14.1 Data Backup System: This term refers to the kind of backup system used in the property including the medium and techniques used for data backup as well as the location of the backup media store.

14.2 Backup Processes and Procedures: The procedure followed for the automated and manual backup and the process of testing backups periodically for restoration.

14.3 Connection Recovery: the consideration of a different route for the connection to cater as a backup connection incase of the main connection failure.

14.4 Infrastructure Recovery: The duplication of the major hardware equipments in the infrastructure to cater as a backup incase of the main equipment failure.

14.5 Recovery Plan: The availability of a recovery plan for Hardware and data in case of any disaster occurs including the details instruction for restoring the network components as well as the applications and data.

XV. Communications

15.1 IP Telephony: IP telephony is the combination of voice, data, video, and wireless applications into an integrated enterprise infrastructure that offers the reliability, interoperability, and security of a voice network, the benefits of IP, and the efficiencies, mobility, and the manageability of a single network. IP telephony is based on circuit-switched and TCP/IP technologies and protocols; it removes the limitations of proprietary systems and provides increased productivity, scalability, mobility, and adaptability.

15.2 Media Gateway (E1/ISDN Based): The media Gateway is the signaling interface between the PSTN (ISP) and MCCR network. The Media Gateway shall consist of a series of ISDN line cards and appropriate signaling protocols (MGCP) to link the core VOIP fabric with the Soft Switch infrastructure and the core switching fabric.

Media gateway shall have the following features:

- The IP Telephony must have ISDN/E1 cards to be connected to Five (5) E1 digital links (150 digital channels) that is connected from the ISP to the tower.
- Media Gateway must have Three extra (3) E1 connection for expansion needs
- Supports Virtual Private Network (VPN) module for advanced encryption services.
- Redundant capabilities
- Connects users across public or private network
- Interoperable and network agnostic
- High-performance physical connectivity concentration

15.3 Soft-Switch: It is a software-based call processing agent, extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VOIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through Soft-Switch open telephony application programming interfaces (APIs).

At least 2 Soft- Switches must be deployed in the network in a redundant client-server fashion; where the required number of extensions can be supported over a wide area network covering wide regional geographies if necessary.

The Soft-Switch supports Call Detail records, call routing and packet processing as well as advanced voice features such as Conference Bridging, Gateway Trunk, User Authentication and Voice-mail Interfacing.

The Soft-Switch supports clustering and single entity administration. The Soft-Switch also supports a Web-browse interface to the configuration database, enables remote device and system configuration. HTML-based online help shall be available for users and administrators.

The Soft-Switch must support H.323 enhancements and Q.SIG signaling to expand the range of interoperable interfaces to which Soft Switch can connect to standard-based systems.

15.4.0 10/100/1000 Mb Ethernet switches with 802.3af inline power modules

15.4.1 IP Phones and Soft phone: IP Telephones are devices which feature embedded high speed which allow a diversity of compression protocols to be supported as well as integrated 802.1q dual port Ethernet switch, allowing the end user to plug a laptop or desktop computer into the phone directly in a serial fashion, thus saving Ethernet jacks. A separate input per device (PC and phone) is not needed; a single wall jack is all that is necessary. Power is supplied to the phones from a switch or Power Port on a switch providing 802.3af – inline 48v DC power over Ethernet, therefore individual power transformers will not be necessary.

15.4.2 Analog Phone Connectivity: The network shall be designed to accommodate analog devices that will be integrated with the IP telephony system. The number of ports and devices should be decided based on the number of KNET, analog phone and Fax machines in the building. The PBX must have Central Office (CO) analog cards to support the required number of analog lines in each floor of the building.

15.5 Digital Call Recording

15.5.1 Record: phone calls according to flexible policies. You can record every call and keep only what is important. Rules and filters can be defined to categorize calls by phone number or user name patterns.

15.5.2 Review, Adnotate and e-Mail: phone call recordings. Search by caller ids, phone numbers, adnotations, time. Everybody can access their own calls by default, but only designated supervisors can access other phone calls.

15.5.3 Call Retention Policies: Recordings can be kept for a period of time or until the hard-drive is filled. Some calls are more important than others, so rules can be set to manage each category differently.

15.5.4 Scalable: When using multiple servers. Calls can still be browsed & searched from a central server. The actual recordings storage is distributed amongst servers.

15.5.5 Integrated Authentication: Authentication is integrated with Soft switch, directory server, so user accounts and passwords need to be set only once.

15.5.6 Call History: follow a call as it is transferred, put on hold or parked.

15.5.7 Audit Replays: prevent recordings abuse by browsing the list of accesses to a call.

15.5.8 Scalable: when using multiple servers. Calls can still be browsed & searched from a central server. The actual recordings storage is distributed amongst servers.

15.6 Unified Messaging: Voice Mail is considered to be an essential voice service for businesses. One of the advantages of integrating voice mail over an IP Telephony network is that messages and content such as fax may be delivered over a variety of media and modalities for the end user.

Voice mail can be retrieved in the following manner:

- Retrieval by phone from the users' extension in response to a MWI (Message Waiting Indicator)
- Retrieval from a remote location by phone – mobile or landline any where in the world by dialing into the voice mail servers IVR menu system and exchanging a Mailbox number and password to allow remote access to messages.
- Voice Mails can be forwarded to an email box as an audio attachment, or simply as a notification that a message from a captured Caller-ID is waiting.
- Web based access –voice and fax messages can be accessed through and internal web based Portal – or accessed over the public Internet through a secure web site.
- Notification via SMS – as with the email notification system, an SMS message can be forwarded to the subscriber's desired mobile handset to notify them that a message is waiting in the voice mail queue.
- As part of the overall integrated design goal for the GLOBAL IP Telephony network we are recommending the following unified Messaging Server platform:
- Provides advanced, convergence-based communication services on a platform that offers the utmost in reliability, scalability, and performance.
- It integrates with the desktop applications -- such as Microsoft Outlook and Lotus Notes -- that are used everyday to improve communications, boost productivity, and enhance customer service capabilities across the GLOBAL organization. It allows listening to the e-mail over the telephone, check voice messages from the Internet, and forward faxes to any local fax machine increasing organizational productivity.

15.7 Voice Quality: The leading subjective measurement of voice quality is the Mean Opinion Score (MOS) as defined in the International Telecommunications Union (ITU) recommendation P.800. Mapping between network characteristics and quality score make MOS valuable for performing network assessments and tuning. A MOS score can range from 5 (very satisfied) to 1 (not recommended), but keep in mind that each voice codec has a benchmark score based on several factors, including packetization delay and the inherent degradation that occurs when converting the voice to a digital signal. The highest MOS rating any codec could receive is 4.5. Each codec is given a MOS value based on any known impairments for the speed of the conversion, speech quality, and data loss characteristics. Below is a listing of the most common codecs used today for VoIP and their theoretical maximum MOS value?

Indexing Factors Weights

Evaluation Area	Weight
Reliability	10%
Scalability	5%
Security	10%
Accessibility	5%
Operability	10%
Organization of resources	5%
Engagement	4%
Ease of Use	5%
Functionality	10%
Manageability	10%
Mobility	5%
Administration	6%
Backup and Recovery	5%
Communications	10%
Total	100%

CONCLUSION :

This paper addresses a significant framework of measurements for S.M.A.R.T. implementation. The merit behind this is to establish a benchmark for indexing such implementation. The subject field itself is relatively new, and affect rather a traditional field. In such cases, a base reference has to be created. What this paper is attempting to do is to create such reference. By no means is this framework complete and/or holistic. It is made for researchers to contribute to this framework and build on it.In this attempt, we have carried many significant factors of such implementation. The paper addresses all of them. Ranking and index for each category is open for implementation view. Obviously, Healthcare infrastructure is different from residential and more so when it comes to secure buildings. The paper addresses all these in a generic framework. It is our intent to have this paper construed the basis upon which future ranking is made. Moreover, as this field is new, most of the reference material is structured on classical implementations (such as BMS, Structural, and electrical). None of the literature references have similar indexing means. Our paper represents our effort to define a relatively new, yet critical, indexing mechanism.

REFERENCES :

[1] IlyaGertsbakh, YosephShpungin (2011) Network Reliability and Resilience
[2] Clements-Croome, D. (2004). Intelligent Buildings: Design, Management and Operation. Thomas Telford Ltd, London.
[3] NiteshDhanjani, Justin Clarke - O'Reilly Media, Inc. ,(2005) Network Security ToolsAlexander Clemm, (2006) by Cisco Press. Network Management Fundamentals
[4] Karmi, N. (2005). MEDCOMM Market Report on Applied Information and Communication Technologies in Gulf Real Estate Markets. MEDCOMM Journal of Smart Technologies. Issue B.
[5] John G. Proakis, (2014) Fundamentals of Communication Systems
[6] Harris, S. (2005). Access Controls and Secruity Components. Third Edition. McGraw Hill, California.
[7] Younge, G. (2005). Building Intelligence Quotients and How to Calculate It. Computerworld: Networking & Internet. Volume 33. Issue 2.