Vol 8. No. 4, December, 2015
ISSN 2006-1781

African Journal of Computing & ICT


www.ajocict.net

# Re-Engineering Control System Implementation Philosophy: A Proactive Approach to Control System Security in the Face of Ever Increasing Cyber Security Threats

**[1]E.S. Mbonu & C.B. Okoye**
Process Automation, Control and Optimization Department
Shell Nigeria Exploration and Production Company, Nigeria
mbonuekenesamuel@gmail.com

**H.C. Inyiama**
Department of Electronics and Computer Engineering
Nnamdi Azikiwe University
Awka, Nigeria

**[1]Corresponding authors**

## ABSTRACT

This paper introduced the seventh element, the hardener, in the conventional control system architecture comprising the controller, final element/actuator, controlled process, feedback sensor, summing point and reference point. Given the ever increasing threats to control system security and emerging smarter ways of doing things, it seems the ICT based solutions with their identified weaknesses can no longer exclusively provide security to control system in the near future, hence the control system hardener. Implementing the mathematical model developed for the hardener entails re-engineering control system implementation philosophy. Leveraging on risk equation, this work used system analysis to identify the vulnerability/attack surface inherent in conventional control system. The mathematical model developed to reduce the attack surface to zero was tested using simulation tools within the Shell Nigeria Exploration and Production Company (SNEPCo)'s environment. The result showed that the seventh component has zero negative impact on control system's availability and integrity. This solution promises to provide zero opportunity to both internal and external threat agents even in years to come.

**Keywords**: Control system hardener, ICT based solutions, re-engineering control system implementation philosophy, attack surface, internal and external threat agents, system's availability and integrity.

**African Journal of Computing & ICT Reference Format:**
E.S. Mbonu, C.B. Okoye & H.C. Inyiama (2015) Re-Engineering Control System Implementation Philosophy: A Proactive Approach to Control System Security in the Face of Ever Increasing Cyber Security Threats. Afr J. of Comp & ICTs. Vol 8, No. 3. Pp 167-180.

## 1. INTRODUCTION

The need for easy and timely access to information has necessitated the interconnection of enterprise networks with control system networks in industrial domain [1]. Figure 1 shows a typical interconnection with respect to the existing Process Control Domain (PCD) governance architecture in Shell Nigeria Exploration and Production Company (SNEPCo) [2]. Level 0 to Level 2 represent the PCD while level 4 is the office or enterprise domain. In between levels 2 and 4 is level 3 which represents the existing security structures in the PCD. Operators' work stations reside at level 2 while the process controllers reside at level 1. The final controlled elements or actuators are resident at level 0. It is obvious from figure 1 that without reliable security measures in place, the process controllers are exposed to attack/risk which can come from threats originating from any of the levels above level1.

These threats could be insiders within the office domain, operators at the workstations (level 2), third party representatives or hackers via internet [1].
The risk equation, given by equation 1, gives a clearer view of how a control system can be attacked [3]. What can be done to reduce the risk is also implied from the equation.

$$Risk = Threat \times Vulnerability \times Consequence \qquad (1)$$

In order to facilitate the understanding of equation 1, the definitions of the elements of the equation are given below.
**Risk:** this is the level of impact on organizational operations (including missions, functions, or reputation), assets or human resources resulting from failure of an entity or system [3].

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

**Threat:** this is the potential for a threat source to successfully exploit a particular system's vulnerability [3]. Vulnerability/Opportunity: this is any weakness in a system that can be exploited intentionally or unintentionally by a threat vector or adversary to cause a specific consequence [3].

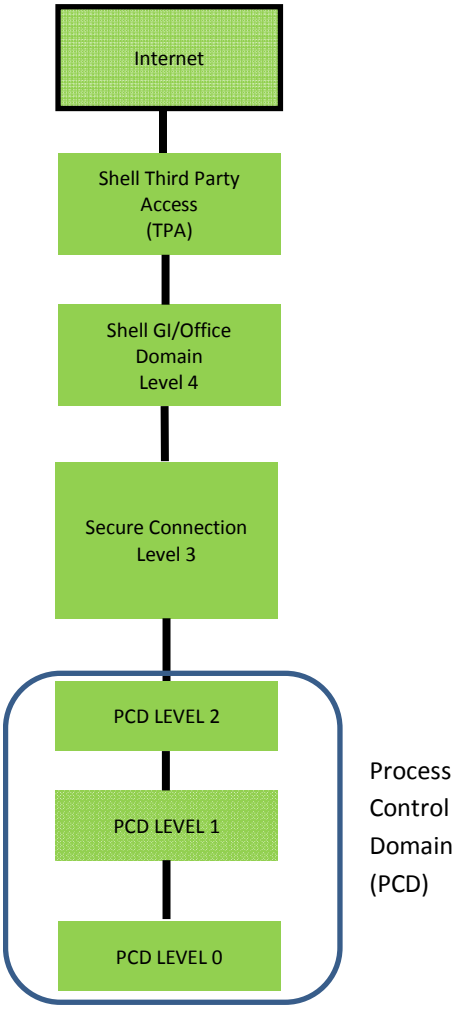


**Figure 1: PCD governance architecture, source [2]**

Consequence: this is the total amount of loss or damage that can be expected from the successful exploitation of vulnerability/ opportunity by a threat vector [3]. Following the above definitions, it can be argued that the process controller, being the heart of every control system [4], and having a recovery time objective (RTO) of zero, is one of the components that bears highest risk in automation industries.

For example, a successful attack on a process controller which led to an unplanned shutdown of an oil well that has production capacity of 200,000 barrels/day for two weeks will result in loss of 140 million US dollars at rate of 50 dollar/barrel. Depending on the particular controller that is attacked, the consequence can escalate as listed below [5].

- Fatality/health hazards to workers.
- Environmental contamination.
- Negative impact on local and national security.
- Loss of competitive advantage.
- Loss of public confidence.
- Loss of license to operate because of regulatory violation.
- Negative impact on recurrent expenditures including salary of workers, maintenance operations, etc.
- Negative impact on national economy among other things.

In view of the huge consequences associated with a successful attack on process controllers, it is just sensible that proactive measures be taken to avoid such occurrence. Equation 1 gives a clue on how to develop such measures. For example, if any of the elements on the right hand side of equation 1 becomes zero, the risk will become zero as well. Now, it may not be feasible to make the threat vector or consequence to become zero. For example it is generally believed that the highest threat to control system security is the operator or the system user who has a good working knowledge of how the control system works [6]. Also hackers' community steadily learns and improves its hacking prowess [7]. Thus the most reasonable and easier thing to do is to reduce the opportunity available to the bad elements whether they are external or internal to the control system. If one succeeds in making the opportunity/vulnerability zero, equation 1 then becomes

$$Risk = Threat \times 0 \times Consequence$$
$$Risk = 0$$

This is what this research achieved within the context of control system converging point which appears to be the only surface through which an attacker can destabilize a control system through a work station.

The rest of this work is organized as follows. Section II is a review of the security of efforts to prevent unauthorized access to PCD, highlighting the strengths and weaknesses (if any) of each approach. In section III, the basic principle of automatic control system was presented with a view to determining the attack surface of a control system while section IV introduced the prerequisite for the control system re-engineering philosophy: the concept of control system hardening. The mathematical modeling of control system hardening was done in section V while section VI is the test plan to validate the model developed in V.

Vol 8. No. 4, December, 2015
ISSN 2006-1781






Test results and discussion of the results are shown in section VII. The relevance of this solution in the face of emerging technologies like cloud computing, internet of things (IOT), internet protocol version 6 (IPv6) was discussed in section VIII before concluding in section IX.

## 2. OVERVIEW OF EFFORTS/SOLUTIONS TO PREVENT AND REMEDIATE SECURITY INCIDENCE IN PROCESS CONTROL SYSTEM

A number of measures are already in place to prevent and/ or remediate security incidence in process control system interconnected with enterprise network in industries. These measures can be categorized into five major areas namely: network segmentation, access control, operational policies, event log management and back up strategies [2]. A brief description of each approach is given below.

### A. Network Segmentation.

In network segmentation, group of hosts with similar attributes are grouped together so that only the group members can communicate with one another. For example, there are control, service, safety, integration, etc, networks [2]. There can also be sub-group within a group, a concept referred to as demilitarization. Inbound and outbound traffics to and fro groups are usually restricted or controlled. The network elements usually employed to achieve network segmentation are basically switches, routers and firewalls [2], [8]. One of the major benefits of network segmentation is that it prevents unauthorized access to information. Also in the event of security incidence like virus attack, it helps in remediation as it prevents the escalation of the incidence or attack beyond the originating domain [8].

The weakness of network segmentation lies in the logic employed in the network elements used in the implementation of the segmentation. Virtual Local Area Network (VLAN) for example is used to create multiple domains in layer 2 switches by placing group of hosts within a network in a separate subnet [8]. Thus only hosts within the same VLAN can communicate with each other. This logic assumes that the user in each legitimate host will always do the right thing. It assumes for example that the operator connected to distributed control system (DCS) controller via control network will always give the right command to the controller. It did not consider that a saboteur or a disgruntled element may intentionally or unintentionally not do the right thing, including choosing to die in the process. Although firewalls could be deployed to checkmate the activities of the user within a VLAN, the check is not usually in-depth. In other words, firewalls check either the Internet Protocol (IP) address of the host or the port number of the application passing through it [9].

The real data that can manipulate the behavior of a control system is not checked. Although there are firewalls with deep packet inspection features, they are not designed for control system operations [10], and as such cannot be deployed in process control domain.

### B. Access Control

Access control determines who has access to information. It entails physical and logical access control. Access control has similar advantage with network segmentation; however, it further helps to create more layers of security within a given domain [2], [8]. For example, an operator and a vendor working on the same host may not have the same level of privilege to certain information. Thus, access control helps in achieving role based access to information. All the same, it does not address the issue of legitimate users' misbehavior with respect to control system operation.

### C. Operational Policies

Policies are laid down rules that should be followed in order to achieve a defined task [11]. Good policies help in achieving organizational goal at a minimum risk. In the context of control system security, policies are formed for example to ensure that good practices that will protect control elements from threats are upheld. Ensuring that every flash stick is scanned with up-to-date antivirus software before using it on a workstation is an example of a good policy. There are usually controls in place to make sure that policies are implemented as stipulated. Good policies when implemented to the letter will reduce the likelihood of security incidence occurrence. The issue with policy is that it is based on the philosophy that people should do the right thing. So it gives a false sense of security as one might intentionally or unintentionally do the wrong thing. One can even do the wrong thing with a resolve to face the consequence. One way to prevent such a scenario is by reducing or removing entirely the opportunity the bad element has.

### D. Event log Management

Event logging is the ability to monitor and record the activities of system users [2], [5], [10]. What transpired within a given system for a period of selected time can be reviewed. Event could be managed locally or centrally. Central management helps to retain evidences after a security incidence occurred. In other words, event log management aids forensics. Thus, it is more of reactive measure than proactive measure. While event logging can influence an individual to do the right thing, it may not be an effective measure for an individual who is determined to face the consequences of his actions. Also it will not prevent a user from inadvertently doing the wrong thing.

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

### E. Backup Strategies

This is reactive measure put in place to remediate a security incidence. Every system or device usually has recovery point objective (RPO) and/ or recovery time objective (RTO). While RPO drives data backup strategies, RTO drives hardware/software recovery strategies [12]. Although restoring a system from a backup can help to mitigate a security incidence, it is not without consequences as some recovery procedures usually take time and some may even require a shutdown.

Having reviewed some of the measures taken so far to protect control system, the weakness that is common to all of them is that none of them can stop a legitimate user from illegal manipulation of a control system. This is essentially because these solutions were originally ICT based but now adopted in process control environment. The next section examined the principle of automatic control system which is the basic of industrial control system, and identified a single factor/element which can be manipulated to make a typical control system uncontrollable. The rest of the paper is dedicated to developing a solution that will make it difficult, if not impossible for a legitimate user to manipulate this element beyond the controllable limit.

## 3. THE BASIC PRINCIPLE OF AUTOMATIC CONTROL SYSTEM

Automatic control system can be represented in a block diagram as shown in figure 2 [13]. It is a closed loop system that has set point adjustment, controller, actuator/final control element, process output and sensor/feedback circuit. The origin of the feedback signal, b is a sensor attached to the process output, y. The feedback circuit returns a signal to the controller. The controller is fed by a summing circuit that compares the set point input, s and feedback signal. The set point value, s is adjusted by the operator according to the needs of the system. The actual value of the process output is determined by the sensor. If the actual output is the same as the set point value, the controller indicates system balance, and the actuator or final control element remains unchanged.

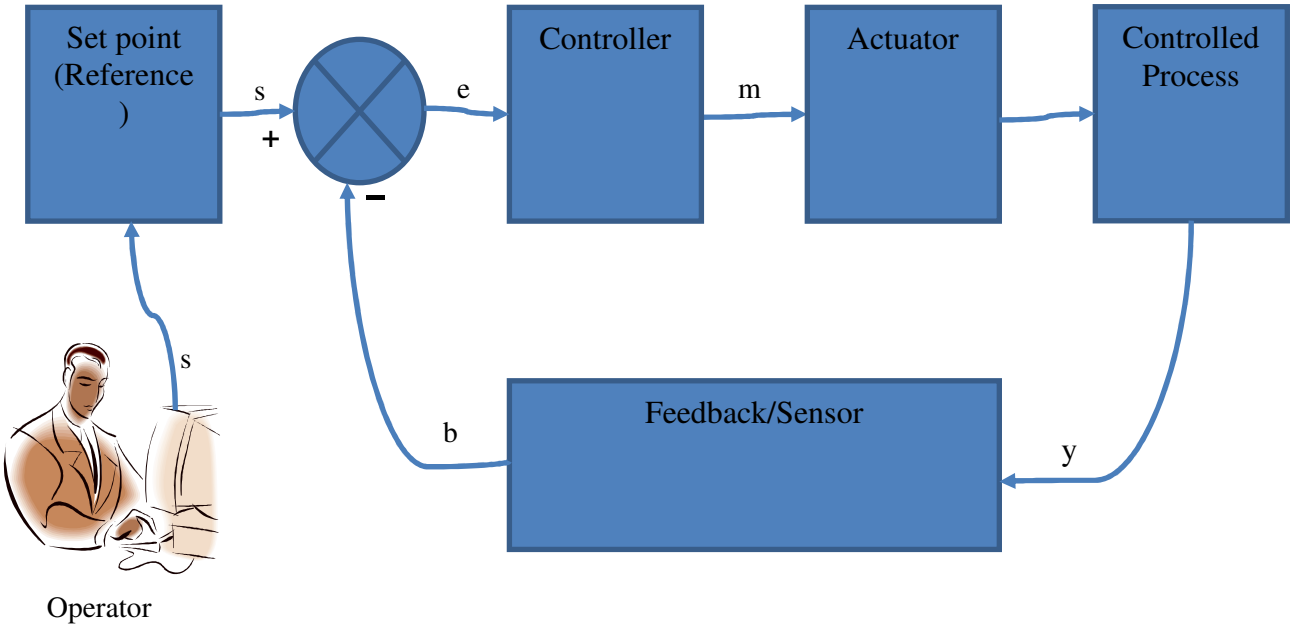


**Figure 2: Block diagram of basic automatic control system**

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

If the actual output deviates from the set point value, signal applied to the controller is no longer in balance, and this causes a correction signal, m, to be developed by the controller. The correction signal, proportional to the error e, is directed to alter the actuator or final control element [13].
Now it is clear from figure 2 that the only way the system could be manipulated by the operator is by changing reference point. It is therefore logical to investigate the effect changing reference point will have on typical control system. In other to do this, a temperature control system was considered. Now, the dynamic model of a temperature process can be described as first order transfer function [14], [15] as shown in equation 2

$$G(s) = \frac{K}{(\tau s+1)} e^{-Ls} \qquad (2)$$

Where
$K$ is the gain defined as the ratio of output signal to input signal.

$G(s)$ is the transfer function of the forward system.

$$K = \frac{y(\infty)}{u(\infty)} \qquad (3)$$

$y(\infty)$ = final steady state value of the output

$u(\infty)$ = input to the system

$\tau$ is time constant when the output reaches the 63% of the final value.

L is the time delay, the time required for the system to start responding to the input change [15].

Equation 2 was modeled in Simulink using a proportional-integral-derivative (PID) controller as shown in figure 3. The optimal parameters of the controller were automatically generated using auto tuning tool in MatLab as shown in figure 4. The model in figure 3 was then simulated at different set points of 35, 50, 65 and 100 degree centigrade. The response characteristics of the system at the respective set points were plotted as shown in figure 5. The response characteristics as deduced from figure 5 are tabulated in table 1.

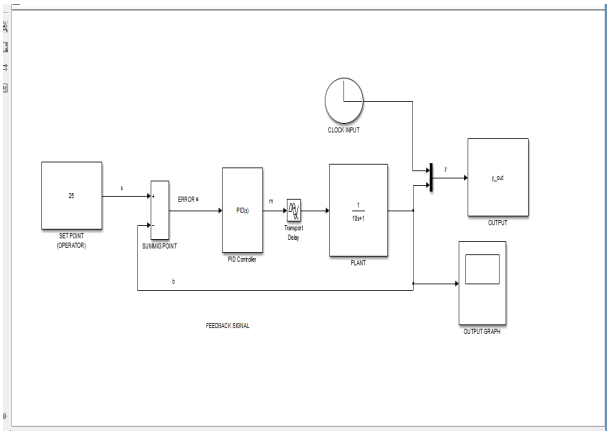


**Figure 3: Model of a PID temperature controlled system**

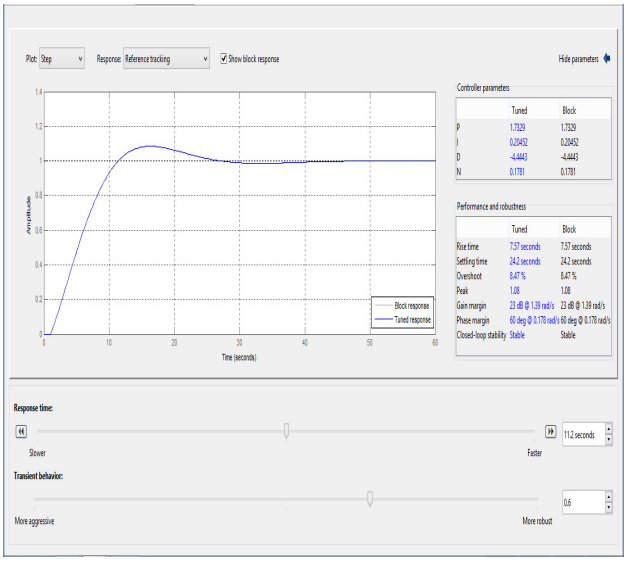


**Figure 4: auto tuning of PID a controller**

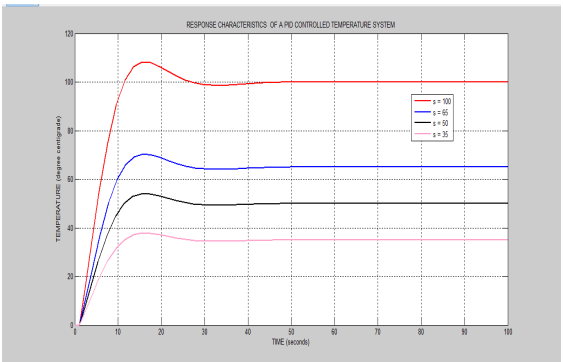


**Figure 5: the response of a PID controlled temperature system at different set points**

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

Table 1 reveals that changing the reference/set point of a stable control system does not affect the stability of the system. As shown in table 1, the steady state error for each case is approximately zero within the range of temperature considered. The point of convergence changes to the new set point, a desirable feature of every feedback control system. In fact this is the primary objective of every control system. However, when considered in terms of security, the converging point becomes a vulnerability which can be exploited by an attacker. Just consider a scenario where by a man-in-the- middle attack is in operation between the operator's workstation and the DCS controller. The attacker can manipulate the system at will depending on the motive simply by changing the reference point. In the worst case, a huge loss can even be triggered by the attacker just by driving the set point beyond limits so that instrumented protective system (IPS) will initiate a shutdown. Unfortunately, firewalls and TCP/IP security measures employed between the work stations and DCS controllers cannot detect this kind of attack as it involves manipulating the real data! The media access control (MAC) address, logical address; TCP header and frame check sequence (FCS) are not altered. This kind of attack when successfully executed could run for months without anybody discovering it. Stuxnet is a good example [6]. The next section considered the concept of control system hardening as a proactive measure against manipulation of reference point which incidentally is a universal characteristic of every control system.

**Table 1: the response characteristics of figure 5**

| Set point ($^oC$) | Delay time (sec) | Rise time (sec) | Settling Time (sec) | Maximum Over shoot | Steady State error | Peak time (sec) | Converging Point |
|---|---|---|---|---|---|---|---|
| 100 | 1.5 | 7 | 48 | 8.2294 | 0.0022 | 15 | 100 |
| 65 | 1.5 | 7 | 48 | 5.3333 | 0.0014 | 15 | 65 |
| 50 | 1.5 | 7 | 48 | 4.0565 | 0.0011 | 15 | 50 |
| 35 | 1.5 | 7 | 48 | 2.8582 | 0.0008 | 15 | 35 |

## 4. THE CONCEPT OF CONTROL SYSTEM HARDENING

Hardening as security concept involves reducing the attack surface which can be exploited by an attacker. In ICT domain, it involves blocking unused universal serial bus (USB) ports, removing all soft wares and applications that are not needed for a specific task, e.t.c. Industrial processes usually have operating points which fall within the domain of real numbers (DRN) from negative infinity (-∞) to positive infinity (+∞). The region of operation of industrial processes is usually negligible compared to the DRN. This is because industrial processes usually deal with manipulation of physical properties of substances to achieve a desired result. To get a steam from water for example, it requires maintaining the temperature of the water at 100 $^o$c [16]. So a good control system will work to maintain the water within this specified temperature. This is achieved by maintaining the reference point within this range of temperature. The idea of hardening control system implies making the undesired range of temperature inaccessible to a threat agent. That is, from -∞ to 99 and from 101 to +∞. The result is that this undesired range will no longer exit for the specific process, thus reducing the opportunity of the attacker to barest minimum. Table 2 shows some selected industrial processes and their operating temperature ranges. The list is not exhaustive. The essence of the table is just to demonstrate the concept of control system hardening. In the pasteurization of milk for example, it is required that the temperature be maintained at 63$^o$ c for optimum result to be achieved. This definitely requires precise control. The hardening range as shown in table 2 is -∞ to 62, and 64$^o$c to +∞. When hardened, the control can no longer be driven to this undesired region whether intentionally or unintentionally!

Having discussed the concept of control system hardening, the next section dealt with the mathematical model of the hardening.

**Table 2: selected industrial processes and their operating temperature range [17].**

| Industrial Process | Mini Range | Max Range | Typical Operating point | Hardening Range |
|---|---|---|---|---|
| Reflux accumulator chamber in fractional distillation of petroleum | | | 45 $^o$c | -∞ to 44, 46$^o$c to +∞ |
| Thermal cracking of ethane, butane and naptha into ethylene e and benzene | | | 480 $^o$c | -∞ to 479, 481$^o$c to +∞ |
| Gas-phase Polymerization of ethylene | 75$^o$ c | 100$^o$ c | | -∞ to 75, 101$^o$c to +∞ |
| Injection molding of thermoplastic | | | 200 $^o$c for the machine cylinder; 80$^o$ c for the mold | -∞ to 199, 201$^o$c to +∞; -∞ to 79, 81$^o$c to +∞ |
| Forging of aluminum | 320$^o$ c | 455$^o$ c | | -∞ to 319, 456$^o$c to +∞ |
| Alkaline cleaning | 50$^o$ c | 90$^o$ c | | -∞ to 49, 91$^o$c to +∞ |
| Pasteurization of milk | | | 63$^o$ c | -∞ to 62, 64$^o$c to +∞ |

Vol 8. No. 4, December, 2015
ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

## 5. MATHEMATICAL MODELLING OF CONTROL SYSTEM HARDENING

### A. The model equation

The mathematical model for control system hardening is given in equation 4.

$$s = s_{new} \text{ for } S_{min\_setpoint} \leq S_{new} \leq S_{max\_setpoint}, \text{ at } t = t_i$$
$$= S_{new-1} \text{ at } t = t_{i-1} \text{ for } \mu = 1$$
$$= S_{default} \text{ at } t = t_0 \text{ for } \mu = 0 \quad (4)$$

Where i = 1, 2, 3,…, n

Equation 4 states the new set point $S_{new}$, of a feedback control system at any time $t = t_i$ must fall within a defined range otherwise the system will assume the immediate last correct value at time $= t_{i-1}$ if $\mu = 1$ or default value at time $t = t_0$ if $\mu = 0$. $\mu$ is a decision operator that decides whether system should go back to the last valid value of set point or fall back to the default value. n is the total number of changes made to the set point parameter throughout the controller life cycle.

### B. Implementation of the model equation

Implementation of feedback control system used to be hardwired [18]. Thanks to advancements in software engineering and embedded systems. Figure 6 shows the existing way of implementing automatic control system using proportional-integral-derivative controller as a case study [19]. The algorithm that implements the flow chart of figure 6 usually resides in the controller. It can be seen from figure 6 that if by any means the set point is changed at the workstation or in transit between the workstation and the controller, the effect will be unquestionably implemented by the controller.

Now, control system has zero tolerance to compromise with respect to availability and integrity of data [2]. This is due to high risk that is usually associated with control system failure. Thus, every security solution being deployed to control system must be validated with emphasis on data availability and integrity.

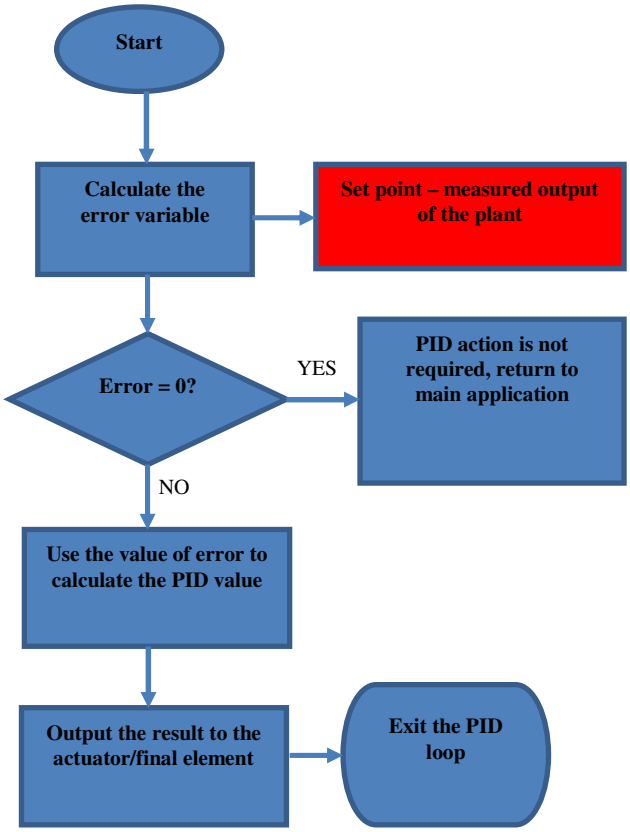


**Fig. 6: High level Flow Chart for the Implementation of Automatic Control System**

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

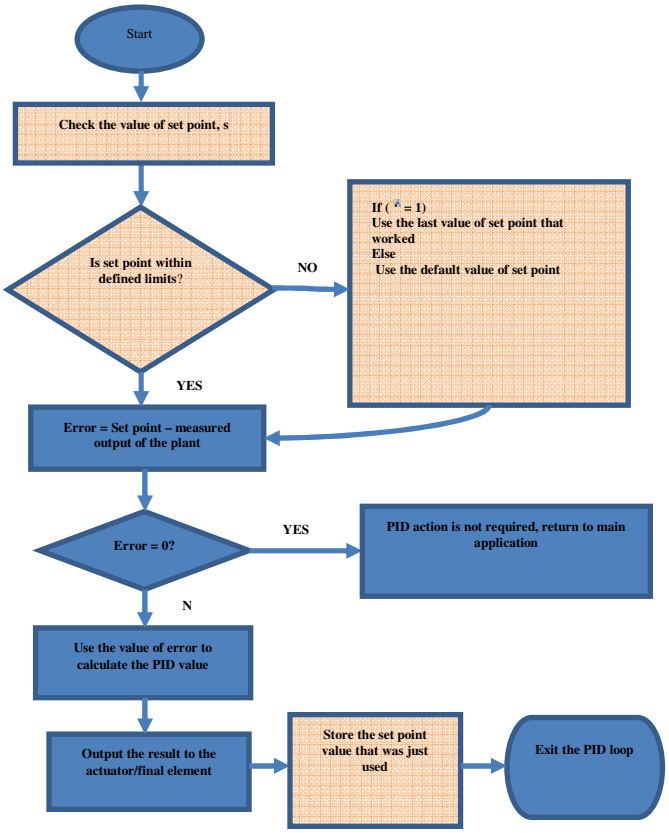


Figure 7: flow chart for implementation of hardened control algorithm in automatic control system

**Fig.7: Flow Chart for the Implementation of Hardened Control Algorithm in Automatic Control System**

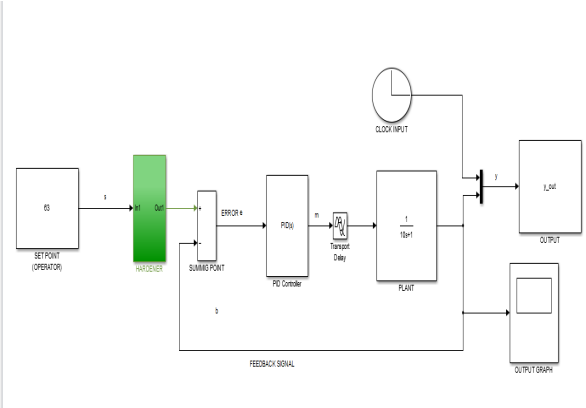


**Figure 8: the hardened PID temperature controlled system**

Figure 8 is a model of PID temperature controlled system earlier shown in figure 3 but now has additional element included in-between the reference and summing point. The additional block, the hardener, implements the hardening blocks shown in figure 7. The logic elements that implement the hardening are embedded in the hardener. Next section highlighted how the system will be tested.

## 6. THE TEST PLAN

To investigate the effect the additional block will have on the system's availability and integrity, the following test plan shall be followed.

### A. The test procedure

1. Select the process to be tested, and set the operating range and the default set point in the hardener.
2. Simulate the process at different set points (within and beyond limits) without the hardener, and record the response characteristics of the process for each case.
3. Introduce the hardener as shown in figure 8, and repeat the experiments as in (2) above.
4. Tabulate the results and plot necessary graphs

### B. The expected results

The following results are expected from the experiments.

1. The output of the control system without the hardener should converge at the new set point for every case and other characteristics of the system should follow a similar pattern as shown in table 1 in section III.

2. The output of the control system with hardener should not converge at a point beyond the region defined in the hardener. Also the response characteristics of the system should be the same even if the set point chosen is
3. beyond the limits defined in the hardener.

## 7. TEST RESULTS AND DISCUSSIONS

### A. Test results

Pasteurization of milk was selected as a test process. The operating point is 63 $^{o}$c as shown in table 2. Thus the operating range T is: $(-\infty$ to 62) < T < (64 to $+\infty)$.

The experiments were carried out as per the test plan. The results without the hardener are tabulated in table 3. The plots of the output response with time for each case are shown in figures 9 to 11. Figure 12 shows the outputs at different set points in one graph.

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

**Table 3: the response characteristics of the control system without the hardener**

| Set point (°C) | Delay time (sec) | Rise time (sec) | Settling Time (sec) | Maximum Over shoot | Steady State error | Peak time (sec) | Convergence Point |
|---|---|---|---|---|---|---|---|
| 63 | 2 | 8 | 47 | 5.7119 | 0.0012 | 16 | 63 |
| 45 | 2 | 8 | 47 | 4.0799 | 0.0009 | 16 | 45 |
| 70 | 2 | 8 | 47 | 6.3465 | 0.0014 | 16 | 70 |

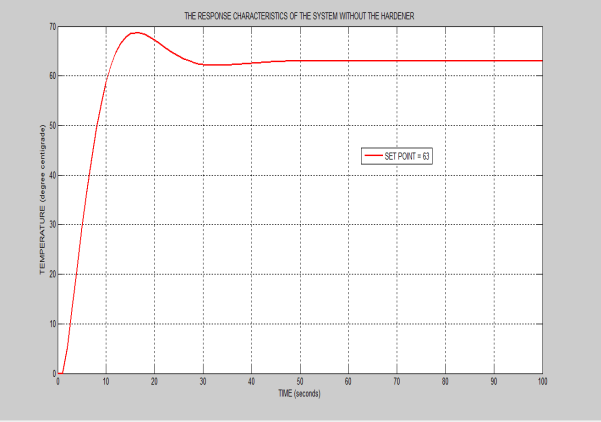


**Figure 9: response characteristics of the unhardened control system at set point = 63**

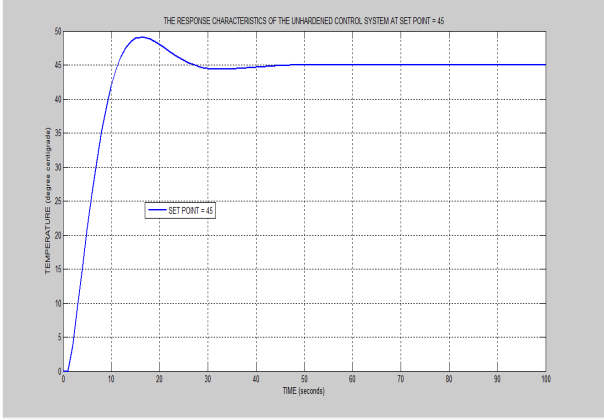


**Figure 11: response characteristics of the unhardened control system at set point = 45**

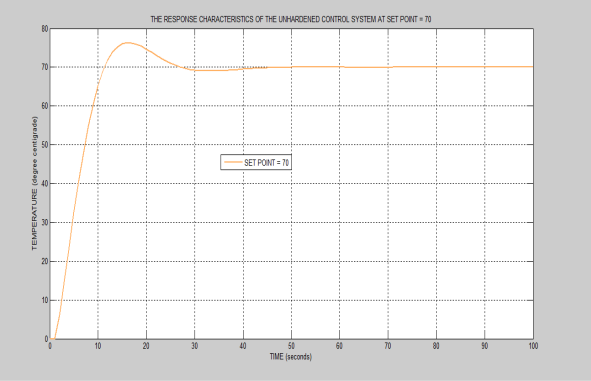


**Figure 10: response characteristics of the unhardened control system at set point = 70**

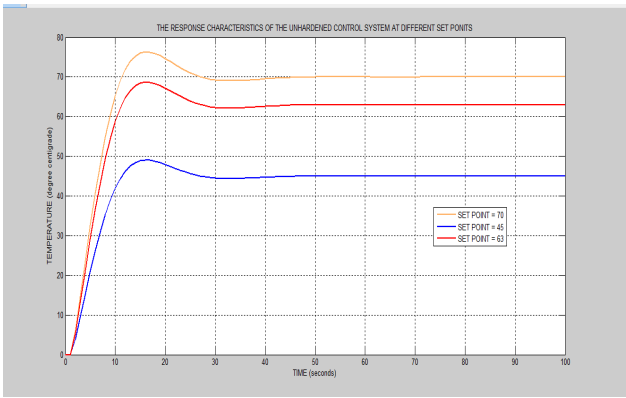


**Figure 12: response characteristics of the unhardened control system at different set points**

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

**Table 4: the response characteristics of the hardened control system**

| Set point (°C) | Delay time (sec) | Rise time (sec) | Settling Time (sec) | Maximum Over shoot | Steady State error | Peak time (sec) | Convergence Point |
|---|---|---|---|---|---|---|---|
| 63 | 2 | 8 | 47 | 5.7119 | 0.0012 | 16 | 63 |
| 45 | 2 | 8 | 47 | 5.7119 | 0.0012 | 16 | 63 |
| 70 | 2 | 8 | 47 | 5.7119 | 0.0012 | 16 | 63 |

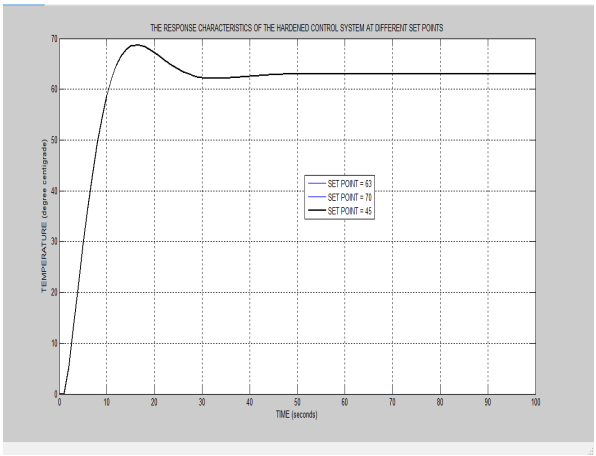


**Figure 13: response characteristics of the hardened control system at different set points**

Table 4 is the response characteristics of the hardened control system at different set points while figure 13 is the plot of the outputs of the system with respect to time at the different set points. Figure 14 is the response of hardened control system superimposed on that of unhardened control system at set point = 45 Celsius.

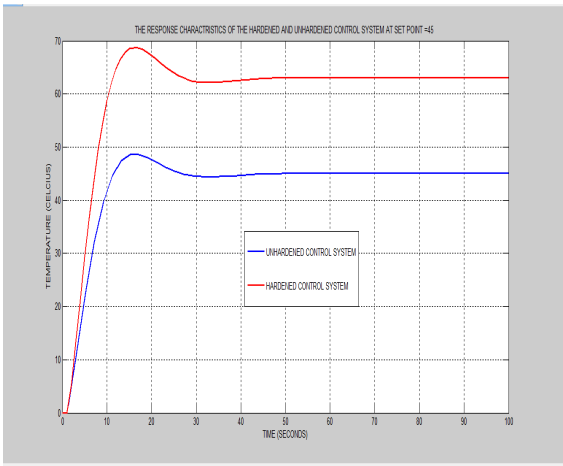


**Figure 14: superimposition of output of hardened and unhardened control system at set point = 45 degree Celsius**

### B. Discussion

From figures 9 to 12 and table 3, it is seen that the following response characteristics of a hitherto stable control system, namely: the maximum overshoot, steady state error and convergence point, are affected by changing the set point of the control system. While change in maximum overshoot and steady state error could be tolerated for some processes, change in set point cannot be tolerated. This is because a change in set point has more pronounced direct effect on product quality generally. In fact, what makes a control system perform control function is the stability of its set point. So a control system whose set point cannot be controlled automatically becomes uncontrollable control system! On the other hand, the introduction of the seventh element, the hardener, in the control system architecture, eliminated the possibility of altering the set point beyond the accepted region. This is seen on the output characteristics of the hardened control system as shown in table 4 and figure 13.

From figure 13, it can be seen that the outputs at the different set points superimposed on each other showing that the introduced element has zero negative impact on the performance of the control system. Besides, figure 14 showed that the hardener maintained the set point at 63 even when the reference point was changed to 45. Comparing tables 3 and 4 also confirmed that the hardener has zero impact on the system's availability and integrity as the delay time, rise time, peak time and settling time were all unchanged. Now before concluding this work, let us examine how the concept developed in this paper will be of help given the emerging ICT technologies like cloud computing, internet of things (IOT) and Internet protocol version 6 (IPv6).

## 8. CONTROL SYSTEM HARDENING AND THE EMERGING ICT TECHNOLOGIES

Necessity is mother of invention. The need for easy and fast access to information led to development of internet, which is an internet protocol (IP) based technology leveraging on IP address. IP version 4 (IPV4) is an address scheme that is based on 32-bit number giving a total of $2^{32}$ or 4.3 billion possible addresses [8]. It was a huge address when it was invented but as more people and organizations began to connect to internet, it became obvious that IPv4 would soon be exhausted despite all the techniques employed to manage the bandwidth optimally.

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

This led to development of IP version 6 (IPv6), a 128-bit addressing scheme [8]. With IPv6, a total of 3.4 x $10^{38}$ items can be connected on line [8]. Thus, it is anticipated that everything on earth can be IP-based. In other words, everything can be interconnected via internet, a concept described as Internet of Things (IoT) [20]. IoT promises a lot of benefits as enumerated in [21], but also has a major challenge that should be considered now before the IoT gets fully implemented [22]. The authors of [22] argued that it will be difficult to provide one central security platform for IoT. This is because IoT involve several objects in different technology areas using the same communication medium, the internet (the cloud), for exchange of information. Just imagine cars, oil rigs, refrigerators, fans, medical devices, human beings, etc., becoming IP-connected. Definitely security would not mean the same thing for every item listed above.

Another issue with IoT is that every IP-based object should have an operating system (OS). The implication is that every object should have OS embedded in them. These would require regular updating. This will definitely not be an easy task, and these OS when not updated make the objects vulnerable. This work recommends multi-layer security for IoT. While the first layer of security should be resident on the cloud (secure cloud), the second should be resident on the object (secure object). The first layer of security as expected should be a general ICT based security solution while the second layer should be application specific security solution developed by the professional in the respective fields. The second layer of security is very important because the cloud security being managed by a third party can be compromised and there can be delays in patching the embedded OS. What this means is that every designer irrespective of the field of endeavor should begin to think of security beginning from the design level, and not just the functionality of the design. In this regard, this work has developed a security solution that will be relevant in automation industry in years to come within IoT environment. Figure 15 shows how the solution fits into the IoT architecture within the context of industrial and home automation. If the security of the cloud is compromised for any reason, the control system will still be safe.

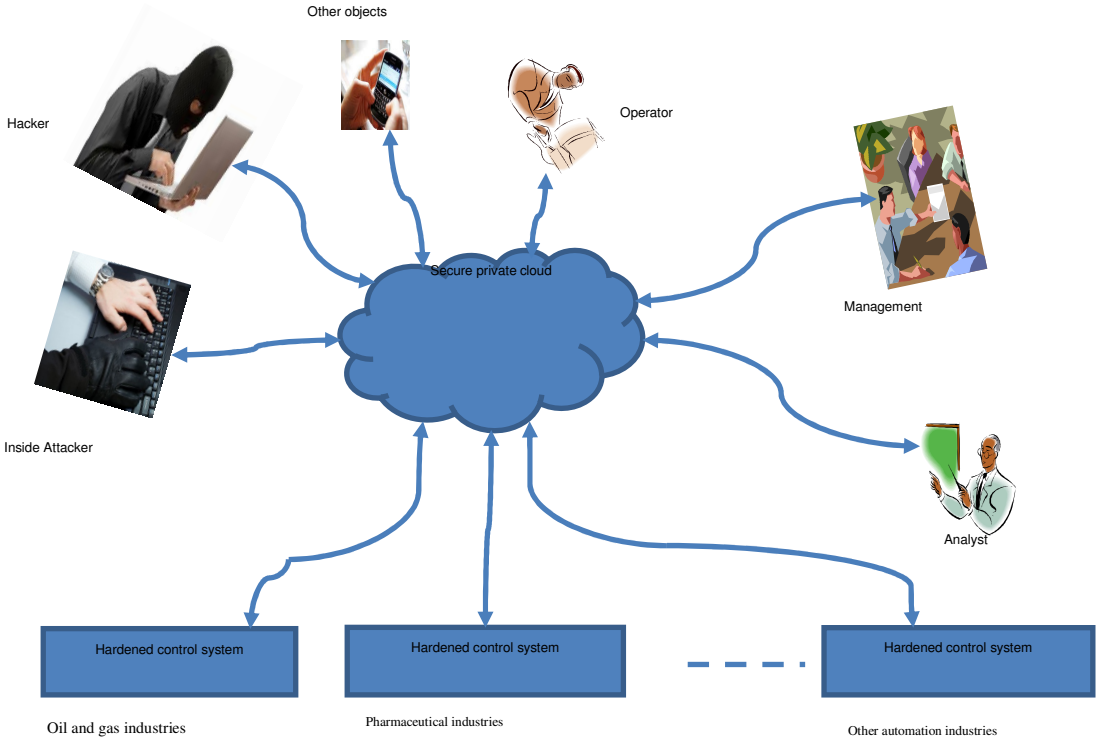


**Fig. 15: The Position of Hardened Control System with IoT Environment**

Just imagine what will happen if the security of secure private cloud of a nuclear plant is compromised and a hacker decides to raise the set point temperature of the unhardened control system above the set limit! With the security solution developed in this work, it is practically impossible to attack the control system in such a manner.

## 9. CONCLUSION

This work proposed re-engineering control system implementation philosophy as a proactive approach to militating against ever increasing threats to control system. The re-engineering process introduced the seventh element, the hardener in the conventional control system architecture. The introduced component has zero impact to control system availability and integrity, besides having minimal implementation cost since it is software based. The solution promises to provide security to control system not just in the present but also in years to come.

**Acknowledgements**
The authors wish to express deep gratitude to Shell Petroleum Development Company of Nigeria for providing the internship opportunity to carry out this research. We also wish to acknowledge the support of SNEPCo's PACO engineers during the research period.

## REFERENCES


[1] Eric D. Knapp, "Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems", Elsevier publisher, U.S.A., 2011.

[2] Shell Global Solutions International, "Design and Engineering Practice: Process Control Domain-Enterprise Enterprise Industrial Automation Information Technology and Security, 32.01.20.12-gen (DEM1),2015

[3] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),USA, https://d36spl5w3z9i0o.cloudfront.net/dcd/scormapi_v60/launcher.html?host=ics-cert-training.inl.gov&id_user=22129&id_reference=203&scorm_version=1.3&id_resource=24203&id_item=111&idscorm_organization=111&id_package=111&id_course=17&launch_type=popup&auth_code=0887a32f-36a8-4f8d-9eed-2850b4fa9c10

[4] Reddy Y. J., "Industrial process automation systems: design and implementation", Elsevier 2015.

[5] ANSI/ISA-62443-3-3, "Security for Industrial Automation and Control Systems, August, 2013

[6] Kim Zetter, " Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Crown publishers New York, U.S.A., 2014 http://searchsecurity.techtarget.com/resources/Hacker-Tools-and-Techniques-Underground-Sites-and-Hacking-Groups

[7] Wendell Odom, "Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide", Cisco press 2013

[8] Juniper Networks, "Firewall Evolution from Packet Filter to Next Generation", retrieve from http://www.juniper.net/techpubs/en_US/learn-about/LA_FIrewallEvolution.pdf on 30/09/15

[9] ANSI/ISA-TR99.00.01, "Security Technologies for Industrial Automation and Control Systems", 2007

[10] ANSI/ISA-62443-2-1, "Security for Industrial Automation and Control systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program", 2009

[11] Shell Global Solutions International, "IRM 3.318 Risk Profile Process Control Domain", 2014

[12] Dale, R. P.; Stephen W.F., "Industrial process control system, 2nd edition", Fairmont press, Inc. India, 2009.

[13] Appuu K.K., "Introduction to mechatronics", Oxford University Press, 2013.

[14] Rash A., "Measurement & control of temperature system", retrieve from http://engineering.ju.edu.jo/Lists/Announcements/Attachments/46/exp.3Temperature.pdf, May 20, 2015

[15] David Halliday, Robert Resnick, "Principles of Physics, 10th Edition International Student Version", 2014

[16] James G. Bralla, "Hand Book of Manufacturing Processes: how products, materials and components are made", 2006.

[17] Hasan S. S., "Automatic Control Systems", S.K. Kataria & Sons publisher, 2012

[18] Chris V., "Implementing a PID controller using a PIC18MCU", microchip technology Inc, retrieved from http://ww1.microchip.com/downloads/en/AppNotes/00937a.pdf on May 26,2015

[19] Ajay Kumar, "Seven IoT Risks you Must Consider", 2014

[20] Chen Zhao, Xisheng Li, Junsong Chen, "Study on the Application of Internet of Things in the Logistics in Forest Industry", 2011

[21] Ajay Kumar, Kevin Beaver, Shamus Mcgillicuddy, "Securing the Internet of Things", 2014, retrieved from http://pro.techtarget.com/Global/FileLib/targeted_downloads/ISM_InsideEdition_final.pdf on 02/10/2015

Vol 8. No. 4, December, 2015
ISSN 2006-1781




www.ajocict.net

## Authors' Briefs

**Mbonu, Ekene Samuel** is a Control System Security Expert and R&D Consultant. Presently he is a Ph.D Research Intern at Shell Nigeria Exploration and Production Company Limited (SNEPCo), Lagos. He obtained Bachelor of Engineering in Electrical/Electronic Engineering from Nnamdi Azikiwe University in 2005. In 2012, he was awarded Masters of Engineering in Computer Engineering. He is currently pursuing Ph.D in Control Engineering. He is a member of COREN and IEEE. His Research interest includes but not limited to industrial control system security and cloud based automation. He can be contacted through Email: mbonuekenesamuel@gmail.com

**Okoye Chiedu Basil** is an Expert in Process Control and Automation. He was awarded Bachelor of Engineering in Electrical and Electronics Engineering in 1990 at University of Benin, and has more than 20 years of industrial experience in Process Control and Automation. Presently, he is the Head of Process Automation, Control and Optimization (PACO) department of Shell Nigeria Exploration and Production Company Limited. He is a member of COREN and ISA

**Professor Hyacinth Chibueze Inyiama** is a seasoned computer scientist and Engineer, with a wealth of experience in both industry and academics. He obtained his Bachelor's Degree in Computer Technology from the University of Wales, University College of Swansea, U. K. (1978) before going over to the University of Manchester, Institute of Science and Technology **(UMIST U.K.)** for his Postgraduate Studies. He obtained his Ph.D **(UMIST)** in December 1981. Since then he has held several posts nationally and internationally in the field of computer and information technology. He is duly registered professionally as both computer scientist and computer Engineer.