RESEARCH ARTICLE OPEN ACCESS

# A Survey on Cyber Security for Smart Grid Communications

Lusi Dalai, Tapan Kumar Sahoo
*Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*
*Capital Engineering College, Bhubaneswar, Odisha, India*

**ABSTRACT—**A smart grid is a new form of electricity networkwith high fidelity power-flow control, self-healing, and energyreliability and energy security using digital communications andcontrol technology. To upgrade an existing power grid into asmart grid, it requires significant dependence on intelligent andsecurecommunicationinfrastructures.Itrequiressecurityframe-works for distributed communications, pervasive computing andsensingtechnologiesinsmartgrid.However,asmanyofthecommunicationtechnologiescurrentlyrecommendedto usebya smartgridis vulnerable in cyber security,it couldlead tounreliable system operations, causing unnecessary expenditure,even consequential disaster to both utilities and consumers. Inthis paper, we summarize the cyber security requirements andthe possible vulnerabilities in smart grid communications andsurvey the current solutions on cyber security for smart gridcommunications.
Index Terms—Smart grid communication, cyber security, vul-nerability,reliability.

## I. INTRODUCTION

POWERindustryisintegratingtheelectricaldistributionsystemwithcommunicationnetworkstoformatwo-directionalpowerandinformationflowinfrastructure, whichiscalledasmartgrid[1].Theintegrationnotonly movespowerautomationsystemsfromoutdated,proprietarytechnologytotheadvancedcommunicationtechnologies,butalsochangestheclosedpowercontrolsystemstothepublicdatanet-works [2]. By adding significant new functionality, distributedintelligence,andstate-of-the-artcommunicationcapabilitiestothepowergrid,thesmartgridinfrastructurecanbemoreefficient,moreresilient,andmoreaffordabletomanageand operate[3],[4].

However, it brings not only great performance benefit to thepower industry, but also tremendous risks as well as arduouschallenges in protecting the smart grid systems from cybersecuritythreats[5].Considering thevastscaleofasmartgrid,itisreasonabletoexpectthat thecumulativevulnerabilityof the smart grid communication system might also be vast.Virtuallyallpartiesagreethattheconsequencesof asmartgrid cyber security breach can be enormous. New functionssuchasdemandresponseintroducesignificantnewcyberattackvectorssuchasamalwarethatinitiatesamassivecoordinatedandinstantaneousdropindemand,potentially

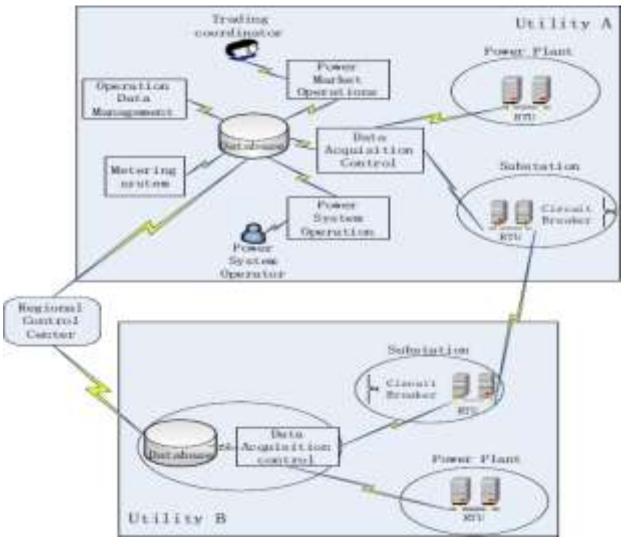


Fig.1.ASmartGridCommunicationSystem[7]

causing substantial damage to distribution, transmission, andevengenerationfacilities[6].
Atypical smartgrid communication system,asillustratedin Fig. 1, is a horizontal integration of one or more regionalcontrolcenters,witheachcentersupervisingtheoperationofmultiplepowerplantsandsubstations.Asmartgridcommunication system has a layered structure and performsdata collection and control of electricity delivery. A regionalcontrol center typically support metering system, operationdatamanagement, powermarketoperations,power systemoperationanddataacquisitioncontrol.SubstationscontainRemote Terminal Units (RTUs), circuit breaker. Human Ma-chine Interfaces (HMIs), communication devices (switches,hubs,androuters),logservers,dataconcentrators,andaprotocolgateway.IntelligentElectronicDevice(IEDs)arefield devices, including an array of instrument transducers, tapchangers, circuit re-closers, phase measuring units (PMUs),andprotectionrelays[7].

Thelegacycybersecuritytechniques forenterprisenet-works canhardlyfitwellfor therequirements ofasmartgrid communication system to operate securely in the publicdatacommunicationnetworkssuchasinternet.Comparedwithregular enterprise network systems, smart grid communica-tion systems have different goals, objectives and assumptionsconcerning whatneedtobeprotectedincybersecurity.Itisimportanttoguaranteetherealtimeperformanceandcontinuous operation features in a smart grid communicationsystem.Thoseapplications arenotoriginallydesignedforthe general enterprise network environment. Therefore, it isnecessary toembrace the existing security solutions wherethey fit, such as communication networks within a controlcenter and/or a substation, and develop unique solutions to fillthe gaps where traditional enterprise network cyber securitysolutionsdonotworkorapply[8].
Updating a system as complex as the smart grid commu-nication infrastructure has the potential of introducing newsecurityvulnerabilities intothesystem.In[9]theauthorpresented a review of the work related to smart grid cybersecurity. The work reviewed is separated into five categoriesthat make up different components of the smart grid: ProcessControl System (PCS) Security, Smart Meter Security, PowerSystem State Estimation Security, Smart Grid CommunicationProtocol Security, and SmartGridSimulation forSecurityAnalysis. A smart grid is a large complex system, and it stillrequiresalotofcybersecuritydesignwork.
In this paper we present a summary of vulnerabilities andpotential cyber attacks on smart grid communication systems,andthemajorchallengesofcybersecurityinsmartgridcommunication systems. It also surveys the existing solutionsforcybersecurityinsmartgridcommunications.
The rest of this paper is organized as follows. In Section II,the background of smart grid communication security is de-scribed. Section III discusses the cyber security requirementsfor smart grid systems. Challenges and current solutions arediscussedinSection IV andV respectively. Finally, SectionVIdrawstheconclusion.

## II. BACKGROUND

A smart grid communication system is comprised of severalsubsystems.Itiseventuallyanetworkofnetworks.SCADAis not only a controlling system but also a communicationnetwork in smart grid. The communication networks in smartgrid systems could include dedicated or overlayed land mobileradios (LMR), cellular, microwaves, fiber optics, wirelinessuch as power line communications (PLC), RS-232/RS-485serial links, wireless local area networks (WLANs) or a versa-tile data network combining these media [10]. In this section,we briefly discuss the background of a smart grid system inseveralaspects:SCADAsystem,communicationnetworksanddeploymentsofsecuresmartgridcommunications.

### *A.* SCADA

Core to the monitoring and control of a substation is theSCADAsystem.ItisutilizedforDistributionAutomation(DA) and computerized remote control of Medium Voltage(MV)substationsandpowergrids,andithelpselectricutilities toachieve higher reliability ofsupply andreduce operatingand maintenance costs. In the past, Sectionalizer Switchgears,Ring Main Units, Reclosers and Capacitor Banks were de-signedforlocaloperationswithlimitedremotecontrol. Today,usingSCADAover reliable wirelesscommunication links,RTUsprovidepowerfulintegratedsolutionswhenupgrad-ing remotely installed electric equipment. In a DistributionManagement System (DMS), RTUs seamlessly interface viaSCADAwithawiderangeofhighperformancecontrolcenters supplied by leading vendors worldwide. Connection tothese Enterprise Management Systems (EMS) and DA/DMScontrol centers istypicallyprovided viaahigh performanceIPGatewayorasimilarnode[11].

*B.* CommunicationNetworks

Theoperationalandcommercialdemandsofelectricutili-tiesrequireahigh-performancedatacommunicationnetworkthatsupportsbothexistingfunctionalitiesandfutureopera-tionalrequirements. Suchacommunication networkconsti-tutesthecoreoftheelectricsystemautomationapplications.Thedesignofacost-effectiveandreliablenetworkarchitectureiscrucial.In[12],theopportunitiesandchallengesofahybridnetworkarchitecturearediscussedforelectricsystemautomation.InternetbasedVirtualPrivateNetworks(VPNs),powerlinecommunications,satellitecommunicationsandwirelesscommunications(wirelesssensornetworks, WiMAXandwirelessmeshnetworks)arediscussed.It provides abriefsurveyonthehybridnetwork architecture thatcansupporttheheterogeneouselectricsystemautomationapplicationrequire-ments.Asmartgridcommunicationnetworkasastructuredframeworkforelectricutilitiesisplannedtoutilizenewcommunicationtechnologiesforautomation,andhence,tomakethedecision-makingprocessmoreeffectiveanddirect.Different scale and structure of the smart grid systems adoptdifferent communication networking solutions. Advanced me-teringinfrastructure(AMI)solutionscanbemeshedorpoint-to-point,withshortlocalcoverageorlongrangecommuni-cations[13],[14].Optionsforbackhaulsolutionsmightbefiber,wirelessbroadband,orbroadbandoverpower-line.Thepossible solutions include WiMax, WLAN, WSN, cellular andLMR,dependingonthereliability,throughput,and coveragedesiredbytheutility.Thewirelesscommunicationsolutionscanbeeitherlicensedorunlicensed,againdependingontheneedsoftheutility.Forthehighestreliability,licensedshouldbechosen.Eachoftheaboveoptionshastheiradvantagesanddisadvantages,butwhatisconsistentlytrueofanyandallofthesolutionsistheneedtohaveascalablesecurity solution[15].

*C.* Deployments

Smart grid deployments must meet stringent security re-quirements.Strongauthenticationwillberequiredforallusersanddeviceswhichmayaffecttheoperationofthegrid. With the large number of users and devices affected,scalable keyand trust management systems,customized tothe specific needs of the Energy Service Provider, will beessential. What has been learned from years of deploying andoperatinglargesecurenetwork communicationsystemsisthat the effort required to provision symmetric keys into thousandsof devices can be too expensive or insecure. The developmentof key and trust management systems for large networks isrequired; these systems can be leveraged from other indus-tries, such as land mobile radio systems and Association ofPublic-Safety Communications Officials (APCO) radio sys-tems.SeveralAPCOdeployedsystemsprovidestate-widewireless coverage, with tens of thousands of secure devices.Trust management systems, based on public key infrastructure(PKI) technology, could be customized specifically for smartgrid operators, easing the burden of providing security whichadheres to the standards and guidelines that are known to besecure [16]. Within three years there are expected to be over1000 PMUs installed. There will be many more installed indistribution networks to help accommodate intermittent powerfrom rooftop solar and electric vehicles. Additionally, PMUswill begin appearing at the terminals of generation equipment,transformers, and large motors. They will be used in largecommercial and residential facilities. One of the key reasonsfor redundancy inPMUsystems insmart gridis tosupportthe requirements to be able to make security patches to thesoftware without lost data. These software patches must bemade with no loss of data. The energy company experienceduring the Hurricane Gustav power island event is a clearexample of the value of PMUs for real time operations of thegrid[17].

## III. REQUIREMENTS

Thereliabilityof asmartgriddepends onthereliabilityof the control and communication systems. In the develop-ment of smart grids, communication systems are becomingmore and more sophisticated, allowing for better control andhigher reliability. Smart grid will require higher degrees ofnetwork connectivity to support the new features. Meanwhile,the higher degree of connectivity should have correspondingsophisticated security protocols to deal with the cyber secu-rity vulnerabilities and breaches. Table I lists some securityprotocols adopted by different layers in communication net-workswiththespecificsecurityrequirements, moredetailsare summarized in [18]. In this section, we discuss the highlevelsecurityrequirements ingeneral andthemajorsecu-rity requirements and vulnerabilities in privacy, availability,integrity,authentication,authorization,auditability,nonrepudi-ability, third-party protection, and trust components for smartgridcommunications.

*A.* HighLevelSecurityRequirements

According to the Electric Power Research Institute (EPRI),oneofthebiggestchallengesfacingthesmartgriddeploymentis related to cyber security of the systems [19]. According tothe EPRI Report, cyber security is a critical issue due to theincreasing potential of cyber attacks and incidents against thiscritical sector as it becomes more and more interconnected.Cyber security must address not only deliberate attacks, suchas from disgruntled employees, industrial espionage, or ter-rorists, but inadvertent compromises of the information in-frastructure due to user errors, equipment failures, and naturaldisasters.Vulnerabilitiesmightallowanattackertopenetrate anetwork, gainaccesstocontrol software,andalterloadconditions to destabilize the grid in unpredictable ways. Thehigh level requirements for smart grid communication securityare conducted in various organizations and the correspondingstandardsindetails.

There are many organizations working on the developmentof smart grid security requirements including North AmericanElectrical Reliability Corporation-Critical Infrastructure Pro-tection (NERC-CIP [20]), International Society of Automation(ISA [21]), IEEE 1402 [22], National Infrastructure ProtectionPlan(NIPP[23]),andNationalInstituteofStandardsandTechnology (NIST), which has a number of smart grid cybersecurityprogramsonproceeding.

One prominent source of requirements is the Smart GridInteroperability Panel (SGiP) Cyber Security Working Group,previously the NIST Cyber Security Coordination Task Group(CSCTG) [24]. The NIST CSCTG was established to ensureconsistency in the cyber security requirements across all thesmartgriddomainsandcomponents.Thelatestdraft documentfrom the Cyber Security Working Group, NIST InteragencyReport (NIST-IR7628) [25], entitled Smart Grid Cyber Se-curity Strategy and Requirements, continues to evolve at thetime of this writing. NIST and the DoE GridWiseArchitec-ture Council (GWAC) [26] have established Domain ExpertWorking Groups (DEWGs): Home-to-Grid (H2G), Building-to-Grid(B2G),Industrial-to-Grid(I2G),TransmissionandDistribution(T&D)and BusinessandPolicy(B&P).

Workingwithstandardsbodies,suchasNISTandothers,willbeextremelyimportanttoensureahighlysecure,scalable,consistentlydeployedsmartgridsystem,asthesestandardsbodies willdrivethesecurityrequirementsofthesystem[27].Onethingisconsistent amongthevariousstandardsbodies,the security of the grid will strongly depend on authentication,authorization,andprivacytechnologies.Privacytechnologiesarewellmatured.FederalInformationProcessingStandard(FIPS)approvedAdvancedEncryptionStandard(AES)[28]andTripleDataEncryptionStandard(3DES)[29]solutions,offeringstrong securityandhighperformance,arereadilyavailable.Thespecificprivacysolutionrequiredwilldependonthetype ofcommunication resource beingprotected.Asaspecificexample,NISThasdeterminedthat3DESsolutionwill likely become insecure by the year 2030. Considering thatutilitycomponentsareexpectedtohavelonglifetimes,AESwouldbethepreferredsolutionfornewcomponents.However,itisreasonabletoexpectthatundercertaincircumstanceswherelegacyfunctionalitymustbesupportedandtheriskof compromiseisacceptable,3DEScouldbeused.

Wirelesslinkswillbesecuredwithtechnologiesfromwell-known standards such as IEEE 802.11i [30] and IEEE802.16e [31]. Different wireless protocols have varying de-greesofsecuritymechanisms.WiredlinkswillbesecuredwithfirewalIs,virtualprivatenetworks(VPNs)andIPSectechnolo-gies. Higher layer security mechanisms such as Secure Shell(SSH)andSSL/TLSshouldalsobeused[32].

System architects and designers often identify the need forand specify the use of secure protocols, such asSSH andIPSec,butthenskiptheimplementation detailsassociatedwithestablishingsecurityassociationsbetweenendpointsofcommunications.Suchanapproachislikelytoresult

TABLEI
LAYERED SECURITYPROTOCOLS

| Layer | SecurityProtocol | Application | Confidentiality | Integrity | Authentication |
|---|---|---|---|---|---|
| Application | WS-Security | Document | Yes | Yes | Data |
| | PGP/GnuPG | Email | Yes | Yes | Message |
| | S/MIME | | Yes | Yes | |
| | HTTPDigestAuthentication | Client-to- | No | No | User |

| | | | | | |
|---|---|---|---|---|---|
| Transport | SSH | Server | Yes | Yes | Server |
| | SSL/TLS | | Yes | Yes | |
| Network | IPSec | Host-to-Host | Yes | Yes | Host |
| Link | CHAP/PAP | Point-to-Point | No | No | Client |
| | WEP/WAP/802.1X | WirelessAccess | Yes | Yes | Device |

in a smart grid communication system where the necessaryprocedures for secure key management can quickly becomeextremely hugeandcomplicatedanoperational nightmare.This is due to the fact that, when system architects do notdevelop anintegrated and comprehensive key managementscheme,customersmaybeprovidedwithfewkeymanagementoptions, and often resort to manually pre-configuring symmet-ric keys. This approach is simple for the system designers, butitcanbeveryexpensiveforthesystemowners/operators.

*B.* Privacy

Privacyissueshavetobecoveredwiththederivedcustomerconsumption dataas theyarecreated inmetering devices.Consumption data contains detailed information that can beusedtogaininsightsonacustomer'sbehavior.
Smart grid communications have unintended consequencesforcustomerprivacy.Electricityusageinformationstoredatthesmartmeteranddistributedthereafteractsasaninformation-rich side channel, exposing customers' habits andbehaviors. Certain activities, such as watching television, havedetectable power consumption signatures. History has shownthatwherefinancialorpoliticalincentivesalign,thetechniquesfor mining behavioral data will evolve quickly to match thedesiresofthosewhowouldexploitthatinformation[33].
Utilitycompaniesarenottheonlysourcesofpotentialprivacy abuse. The recently announced Google PowerMeterservice [34], for instance, receives real-time usage statisticsfrominstalledsmartmeters.Customerssubscribingtotheservice receive a customized web page that visualizes localusage. Although Google has yet to announce the final privacypolicyforthisservice,earlyversionsleavethedooropentothecompanyusingthisinformationforcommercialpurposes,suchas marketing individual or aggregate usage statistics to thirdparties. Although services such as Google PowerMeter areoptional,thecustomershavelesscontrolovertheuse ofpowerinformation delivered to utility companies. Existing privacylawsintheUSareingeneral apatchwork ofregulationsand guidelines. It is unclear how these or any laws apply tocustomerenergyusageyet.

*C.* Availability

Availability refers to ensuring that unauthorized persons orsystems cannot deny access or use to authorized users. Forsmart grid systems, this refers to all the IT elements of theplant, likecontrol systems,safetysystems, operator work-stations,engineeringworkstations,manufacturingexecution systems, as well as the communication systems between theseelementsandtotheoutsideworld.
Maliciousattackstargetingavailabilitycanbeconsideredas denial-of-service (DoS) attacks, which attempt to delay,block or even corrupt information transmission in order tomake network resources unavailable to communicating nodesthat need information exchange in the smart grid. Since it iswidely expected that at least, if not all, part of the smart gridwill use IP-based protocols (e.g., IEC 61580 [35] has alreadyadopted TCP/IP as a part of its protocol stacks) and TCP/IP isvulnerable to DoS attacks. DoS attacks against TCP/IP havebeen well studied in the literature regarding attacking types,preventionandresponse[36]–[38].
However, a major difference between a smart grid commu-nication network and the Internet is that the smart grid is moreconcerned with themessage delay thanthe datathroughputdue to the timing constraint of messages transmitted over thepower networks. Indeed, network traffic in smart grid commu-nication networks is in general time-critical. For instance, thedelay constraint of generic object oriented substation events(GOOSE)messagesis4msinIEC61850.
Intruders only need to connect to communication channelsrather than authenticated networks in the smart grid, it is veryeasy for them to launch DoS attacks against the smart gridcommunicationnetworks,especiallyforthewireless-basedcommunicationnetworksthataresusceptibletojammingattacks [39]–[41]. Hence, it is of critical importance to evaluatethe impact of DoS attacks on the smart grid and to designeffectivecountermeasurestosuchattacks.

*D.* Integrity

Integrity referstopreventing undetected modification ofinformation by unauthorized persons or systems. For smartgrid communication systems, this applies to information suchas product recipes, sensor values, or control commands. Thisobjective includes defense against information

modificationvia message injection, message replay, and message delay onthe network. Violation of integrity may cause safety issues,thatis,equipmentorpeoplemaybeharmed.
Different from attacks targeting availability, attacks target-ing data integrity can be regarded as less brute-force yet moresophisticatedattacks.Thetargetoftheintegrity attacksiseither customer's information (e.g., pricing information andcustomer account balance) or network operation information(e.g., voltage readings, device running status). In other words,suchattacksattempttodeliberatelymodifytheoriginalinfor-mation in the smart grid communication system in order tocorruptcriticaldataexchangeinthesmartgrid.
The risk of attacks targeting data integrity in the powernetworksisindeedreal.Anotableexampleistherecentwork [42], which proposed a new type of attacks, called falsedata injection attacks, against the state estimation in the powergrid. It assumed that an attacker has already compromised oneor several meters and pointed out that the attacker can takeadvantage of the configuration of a power system to launchattacks by injecting false data to the monitoring center, whichcan legitimately pass the data integrity check used in currentpowersystems.

*E.* Authentication

Authentication is concerned with determination of the trueidentity of a communication system participator and mappingofthisidentitytoasystem-internalprincipal(e.g.,validuseraccount) by which thisuserisknown tothe system.Mostother security objectives, most notably authorization,distinguish between legitimate and illegitimate users based onauthentication.

*F.* Authorization

Authorization, also known as access control, is concernedwith preventing access to the system by persons or systemswithout permission to do so. In the wider sense, authorizationrefers to the mechanism that distinguishes between legitimateand illegitimate users for all other security objectives, e.g.,confidentiality, integrity, etc. In the narrower sense of accesscontrol, it refers to restricting the ability to issue commands tothe plant control system. Violation of authorization may causesafetyissues.

*G.* Auditability

Auditabilityisconcernedwithbeingabletoreconstructthe complete history of the system behavior from historicalrecords of all (relevant) actions executed on it. This securityobjective is mostly relevant to discover and find reasons formalfunctions in the system after the fact, and to establish thescope of the malfunction or the consequences of a securityincident.Notethatauditabilitywithoutauthenticationmayservediagnosticpurposes,butdoesnotprovideaccountability.

*H.* Nonrepudiability

Nonrepudiability refers to being able to provide irrefutableproof to a third party of who initiated a certain action in thesystem, even if this actor is not cooperating. This securityobjective is relevant to establishaccountability and liability.In the context of smart grid systems, this is most importantregarding to regulatory requirements, violation of this securityrequirementhastypicallylegal/commercialconsequences.

*I.* Third-partyProtection

Third-party protection refers to averting damage done tothird parties via the communication systems, that is, damagethatdoesnotinvolvesafetyhazardsofthecontrolledplant itself.Thesuccessfullyattackedandsubvertedautomationsystem could be used for various attacks on the communi-cation systems or data or users of external third parties, e.g.,via Distributed DoS (DDoS) or worm attacks. Consequencescould reach from a damaged reputation of a smart grid systemowneruptolegalliabilityforthedamagesofthethirdparty. The risk to third parties through possible safety-relevantfailures of the plant arising out of attacks against the plantautomation systemiscovered byother security objectives,mostnotablyauthorization/accesscontrol.

*J.* Trust

The new designs of future smart grid communication sys-tems form a multi-layered architecture. The growth of smartgridsystemsresultedinaplentifulnessofpowersystemrelatedsoftwareapplications,developedinmanydifferentprogramming languages and platforms. Extending old appli-cations or developing new ones usually involves integratinglegacy systems. Therefore approaching the security of futuresmart grid communication networks cannot be done with acompletenewstart.
In parallel to the development of smart grid communicationsystems, the complete and monolithic cyber security infras-tructure is not a viable option. Instead, multi-layer architec-ture,advancedcontrolmethodologiesanddependablesoftwareinfrastructure as well as device protection mechanisms andhardware monitoring anchors have

to be specified at the sametime. Advanced control approaches have to include predictiveand self-adaptive intelligence at higher level and cross-layermappingtothedifferenttechnicallayers.Thedependablesoftware infrastructures have to be designed to identify andisolatehigher-layerindependent applicationsaswellastosecure cross-layer communications. With such architecture, itshould have the flexibility of incorporating parts of existinginfrastructurewiththefrontiersandinterfacestoadjacentsystems.Furthermore, thearchitecture needstheflexibilitytointerchange or update thepart ofthesysteminasecureway at a later stage due to new laws and regulations or newdevelopmentsintheenergymarket[43].

## IV. CHALLENGES

Smart grid is a conglomeration of different legacy systemspaired with new technologies and architectural approaches,basedon different standards and regulations thatallneed tobe amalgamated into a communication network to support thechallenges of the future electricity network. To support thisobjective, the cyber security architecture for smart grid com-munications are being presented on the basis of cyber securityand architecture requirements, dependency on legacy installa-tions, and the regulations and industry standards. This sectionprovides anoverview ofclassifyingfunctions andsystemsinafuture smart grid communication network. Furthermore,it introduces methods for defining security controls and thusenablingthefurtherdevelopmentofacompliancep rocesswithregard to trusted connectivity in smart grid communications.Themajorchallengesinbuildingand operatingasecuresmartgridcommunication systemincludeinternetworking,securitypolicyandoperations,securityservices,efficiencyan scalability,andthedifferencesbetweenenterprisenetworkandsmartgridnetworksecurity.

### *A.* Internetworking

The interconnected smart grid communication systems areriddled with vulnerabilities that vary across the networks duetothelackofbuilt-insecurityinmanyapplicationsanddevices.Thisshouldnotbethemodelforanetworkasimportant as the smart grid. Layers of cyber security defenseof smartgrid should bebuiltinto thesolution tominimizethe threats from interruption, interception, modification, andfabrication.

Keeping the network private, i.e. where all transport facili-tiesare wholly owned bya utility, would greatly minimizethethreatsfromintruders,astherewouldbeno potentialforaccessfromintrudersovertheInternet.But havingacompletely separate network is not feasible in today's highlyconnectedworld.Itmakesgoodbusinesssensetoreusecommunication facilities, such as the Internet. A minimallysecuredsmartgridconnectedwithInternetascommonlyfoundwithcommercial networks,opensthegridtothreats frommultiple types of attacks. These include cyber attacks fromhostile groups looking to cause an interruption to the powersupply[33],[44].

Oneofthesecyberattacksisworminfestationswhichhaveproventonegativelyimpactcriticalnetworkinfrastructures.Suchthreatshavelargelybeentheresultofleavinganetworkvulnerabletothreatsfromthe Internet.Forexample,therehavebeenDoSattacksonasinglenetwork thatdisruptedalldirectorynameservers,thusprohibitingusersfromconnectingtoanyoftheresources.Itdemonstratesthefragilityofaninterconnectedsmartgridcommunicationinfrastructure[45].Allconnections totheInternet fromasmartgridnetworkneedtobehighlysecure.Intrusiondetectionisneedednotonlyatthepointswhereasmartgridnetworkconnectstothe Internet,butalsocritical pointswithinthenetworkaswellas vulnerablewirelessinterfaces[46].

Thecomponents,systems,networks,andarchitectureareallimportant to the security design and reliability of the smartgrid communication solutions. But its inevitable that an inci-dent will occur at some point and one must be prepared withtheproperincidentresponseplan.Thiscanvarybetweencom-mercialprovidersandprivateutilitynetworks.Aprivate utilitynetwork is likely to provide better consistency of the incidentresponseplanintheeventofasecurityincident, assumingthe private network is built upon a standardized framework ofhardware and software. The speed of the response decreasesexponentially asthenumberofpartiesinvolvedincreases.Conversely , a private network would ideally depend on fewerparties, therefore a more efficient incident response processwould provide for more rapid response and resolution. Therapidityoftheresponseiscriticalduringsituationsthatinvolveablackout[47].

Criticalness of a device or a system also determines howprone it will be to attacks. History has shown that privatenetworks by their inherent nature are less prone to attacks. Asa result, it is recommended as the best approach in situationswheresecurityisparamount[48].

### *B.* SecurityPolicyandOperations

Thereliabilityofasmartgriddependsontheproperoperations of many components and the proper

connectivitybetween them [49]. To disrupt a smart grid system, an attackermight attempt to gain electronic access to a component andconfigureittoimpersonateasanothercomponentan d/orreporta false condition or alarm. One of the simplest types of attacksthat an adversary might attempt is the DoS attack, where theadversarypreventsauthorizeddevicesfromcommu nicatingbyconsuming excessiveresources onone device. Forexample,it is a well-known issue that if a node, such as a server or anaccesscontrol device, uses anauthentication protocol whichis prior to authentication and authorization, then the node maybe subject to DoS attacks. Smart grid protocol designers mustensure that proper care and attention is given to this threatduringprotocoldevelopment.
Manyorganizations willbeinvolved intheoperations ofasmartgrid.Asmoredistributedintelligenceentities areadded to the smart grid communication network, it will beessentialthatthoseentities(peopleordevices)canaut henticateanddeterminetheauthorizationstatusofother entitiesfromaremoteorganization.
Thisissueiscommonlyreferredtoas federated identity management. There are many possibletechnical solutions to this issue based on different securitypolicies, such as those offered by Security Assertion MarkupLanguage (SAML) [50], Web Services Trust (WS-Trust) [51],andPKI[52]. Notonly willvendors needtooffer consis-tent technical solutions, but organizations will further needconsistentsecuritypolicies.Greatcaremustbetak enbyorganizations to ensure their security policies and practices arenot in conflict with those of other organizations with whichthey willneed interoperability. At leastaminimum setofoperational securitypoliciesfortheorganizations operatinga smart grid is formally adopted and documented in industrystandards[53].

*C.* SecurityServices

Managingandmaintainingasecuresmartgrid willbeas equally vital as developing, deploying and integrating asecure smart grid solution. Security services will help networkoperators toidentify, control andmanage securityrisks insmartgridcommunications.

AccordingtoEPRI,everyaspectofasmartgri dmustbesecure[19]. Cyber securitytechnologies arenot enoughto achieve secure operations without policies, on-going riskassessment, and training. The development of these humanfocusedprocedurestakestimeandneedstotaket imetoensurethattheyaredonecorrectly.
Asmartgridrequiresaccesstocost-effective,high-performance security services, including expertise in
mobility,security,andsystemintegration.Thesesecuri tyservicescanbetailored per utility to best fit their needs and help them achievetheirorganizationalobjectives.Fig.2illustrate satypicalsetofsecurityservicesinsmartgridcommunic ations[54].It describes a framework that operationalizes cyber securityacross the people, process, policy and technology foundationsofeachorganization.

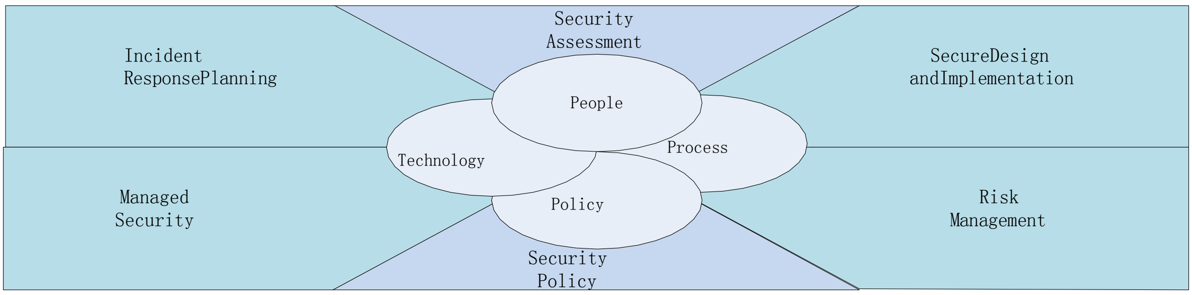


Fig.2.SmartGridSecurityServices[54]

*D.* EfficiencyandScalability

Ensuring system availability is a high priority in criticalsystems like the smart grid which requires that several keyissuesbeaddressed.First,thesystemmustbeefficie ntinits use of computation and communication resources so thatresources do not get overwhelmed and all requests can behandled. Second, the system must have good error manage-mentbuiltintoensureproperhandlingoffailures(e.g.,th ose resulting from bad messages). Furthermore, the errormanagement functions must be fail-safe in nature so they donot lead to resource exhaustion even in the face of adversarialaction. Third, the system must have adequate redundancy builtinto it sothat,if sub-systems fail orare compromised, thenthe entire system does not collapse. Fourth, the system shouldsupport auxiliary security functions that may be deployed inthe smart grid communication system to detect to and respondtocyberattacks[49].

Sincemany existing cyber securityscheme suchaskeymanagement schemes are not suitable for deployment in smartgrid, in [55] the authors proposed a novel key managementscheme which combines symmetric key technique and ellipticcurve public key technique. The symmetric key scheme isbased on the Needham-Schroeder authentication protocol. Theknown threats including the man-in-the-middle attack and thereplay attack can be effectively eliminated under the proposedscheme. The advantages of the key management scheme forsmart grid communication include strong security, scalability,fault-toleranceandefficiency.

*E.* Differences between Enterprise Network and Smart GridNetworkSecurity

Duringthelastdecade,theITindustryhaswitnessedthe development of many cyber security solutions to protectenterprise networks and to reduce the vulnerabilities to cyberattacks. From firewalls to intrusion detection systems (IDS)andVirtualPrivateNetworks(VPN),thesesolutionshavebeenquiteeffective insecuring theITinfrastructure atbusinessand office automation levels. However, the enterprise networkbased cyber security solutions come short of providing thesame level of security at the control and automation levels.There are three major differences between enterprise networkandsmartgridnetworksecurity.

*1)* Different Security Objectives:In enterprise networks,the main security objective is to protect data. The followingmajor concerns exist: 1) data integrity; 2) data confidentiality;and3)dataavailability.Preservingdata integrityrefersto protecting data against modification by unauthorized personsor entities. Data confidentiality refers to the prevention of dataaccess by unauthorized persons or entities. Maintaining dataavailability involves ensuring that no person or entity coulddeny access to those authorized users and systems. In smartgrid, the first priority is always human safety. The secondpriorityistoensurethesystemreliability.Forinstance,acyberattack could create a blackout (system outage), a brownout(degraded power quality) or shift the power grid system fromits economically optimal running condition. The third priorityistheprotectionofequipmentandpowerlines[53].

*2)* Different Security Architecture: In enterprise networks,thedataserverresidesatthecenterofthenetworkandrequiresmore protection than the edge nodes, which are used as accesspointsbyendusers.Insmartgridnetworks,EMS sitsatthecenter(inthecontrol center)whereas RTU/PLCssitattheedge.Usually,onlydevices(suchas re-closer,circuitbreaker),whicharecontrolleddirectlyby RTU/PLCs,cando harm to human life, operation, or damage equipment andpower lines.EMS/SCADAand datalog servers cannot doany damage directly. Therefore, in smart grid communicationsystems,edgenodesneedthesamelevelofprotection ascentraldevices[56].

*3)* Different Technology Base: In enterprise networks, Win-dows, Unix and Linux are widely used as operating systems,whereasEthernetisusedtoconnectalldevices withIP-basedprotocols.Therefore, commonsecuritysolutionsaredesigned based on these common architectures. However, incurrent smart grid communication systems, besides the com-mon operating systems above, many utilities use proprietaryoperating systems and networks facilities, and many differentcommunication protocols (IEC61850, DNP3.0,ICCP,etc.)areinuseratherthanordinaryTCP/IPsuits.Thus,itisverydifficulttodevelopcommonhost-basedornetwork-basedsecuritysolutionsforsmartgridapplications[57].

## V. CURRENTSOLUTIONS

Inthissection,wesurveyseveralexistingsolutionsoncybersecurity for smart grid communications. We focus on the tech-nologies being deployed, the key smart grid communicationapplicationsbeingimplementedandtheoutlinesofpowerindustry trials that have recently been announced in privacy,integrity,authenticationandtrustedcomputing.

*A.* Privacy

Privacy of smart grid communication systems is importantto the eventual acceptance by the public. Smart grid commu-nications must assure that the communication data preservesprivacyanywhereatanytime.

In [44], the authors proposed a method for compressed me-ter reading for smart metering in smart grid communications.The distinguishing feature of the compressed meter reading isthat the active smart meters are allowed to transmit simulta-neously and the access point (AP) is able to distinguish thereports from different smart meters. The simultaneous accessresultsinuniformdelays,incontrasttothepossiblelargedelayincarriersensing multipleaccess(CSMA)technique.The random sequence used inthe compressed sensing enhancestheprivacyofthemeterreading.

In[58],theauthorsdescribedamethodforsecurelyanonymizing frequent (for example, every few minutes) elec-trical metering data sent by a smart meter. Although suchfrequentmeteringdatamayberequiredbyautilityorelectrical energy distribution network for operational reasons,thedatamaynotnecessarilybeattributabletoaspecificsmart meter or consumer. However, it needs to be securelyattributable to a specific location (e.g. a group of houses orapartments) within the electricity distribution network. Theproposed method provides a 3rd party escrow mechanism forauthenticated anonymous meterreadingswhich aredifficultto associate with a particular smart meter or customer. Thismethod does not preclude the provision of attributable meter-ing data that is required for other purposes such as billing,accountmanagementormarketingresearchpurposes.

In[59],theauthorspresentedahomeelectricalpowerrouting scheme that can be used to moderate the home's loadsignatureinordertohideapplianceusageinformation.Apowermanagementmodelusingarechargeablebatterywitha power mixing algorithm is proposed. Then, the protectionlevelisevaluatedbyproposingthreedifferentprivacymetrics:an information theoretic (relative entropy), a clustering classi-fication, and a correlation/regression one. This paper sets theground for further research on the subject of optimizing homeenergymanagementhidingloadsignatures.

Insmartgridcommunicationsystems,anystoreddatashould beencrypted using storage keys shieldedsimilartothe mechanisms proposed in [60]–[62]. While a Storage RootKey (SRK) can be used to develop a key chain by encryptingindividual storage keys whose private part will not be exposedto the host system. The storage keys then may seal potentiallyunlimiteddataonanymedium[63].

*B.* Integrity

Several integrity policy models (e.g., Biba [64], LOMAC[65], and Clark-Wilson [66]) have been developed to governintegritylevelsofasystem.TheBibamodelensuresthatprocesses can not corrupt data in higher levels and are notcorruptedbydatafromlowerlevelprocesses[64].TheLOMACmodeldynamicallysetstheintegritylevelofaprocesstotheminimum integritylevelofdataitinteractswith [65]. Similarly, the Clark-Wilson model allows a processtodiscardorupgradetheintegritylevelofdatathusallowingit to interact with lower integrity level data [66]. In smart gridcommunications, however, it might leave the policy decisionstoauserbutfocusonmechanismstoprovidesecurityservices.In the following, system integrity, process integrity, and dataintegrityarediscussed:

*1)* System integrity:System integrity is a binary propertythat indicates whether the systemhas a trustworthy execu-tionenvironment.Usingtrustedcomputingfunctionalities,itperformsbinaryattestationtoverifytheintegrityofasystem and its enforcement capabilities. Particularly, all partiesin blind processing will challenge peers to ensure that theremote system conforms to Trusted Computing Group (TCG)specificationswith(1)aTrustedPlatformModule(TPM) providing rootoftrust,(2)asecuritykernelprovidinganisolated execution environment for trusted processes whosecomputationsandmemoryaresafefromtampering,(3)acryp-tographically protected storage for sensitive data decipherableonlybythededicatedprocess,and(4)shieldedcommunicationchannelswithremoteprocesses.

*2)* Process integrity: The integrity of a process essentiallydependsonthegenuinenessofitscode.Itisimportantnotonlyto detect changes in software but also to ensure that newly de-veloped code is trustworthy. A modified code may yield mali-ciousbehaviorthatwouldcompromisethedata.Wecan ensurethe integrity of a process using fingerprints, i.e., cryptographicdigestor hash functions of its code. When communicatingwithanallyor competitor process both parties willassurethe integrity of each other by comparing stored fingerprintswith reported Platform Configuration Registers (PCR) valuesbefore transmitting any data. To enforce process integrity, itapplies software engineering techniques that enhance softwaresecurity, including safe software architecture and compilationtechniques for intrusion prevention [67], security specificationand management[68], software quality assurance throughoutsoftwarelifecycle,andsecuritytesting[69].

*3)* Data integrity:Verifying the genuineness of data de-pends on whether the data is collected or generated. Collecteddata is primitive data given to a process and its integrity isapplication specific. Some techniques to ensure integrity ofcollecteddata aresemanticcheck(i.e., integration oflogicintotheprocesstoverifydatasemantics),certificate(i.e.,signatures from trusted central authorities), and trusted path(i.e.,ensuring that thedata come from anauthenticated userorsensingdevice)[70]. Generateddataintegritydependsongenuinenessoftheprocessandcollecteddata.Overall,dataintegrityrequiresachainoftrust.Ensuringtheintegrityofgenerateddat arequires ensuring the integrity of the generating process aswell as the integrity of input data to the process. Ensuring theintegrityofinputdata requires ensuringthegenuineness ofthecommunicatingprocessortheinputdevice.

Integrity evaluation involves verifying the source, its in-tegrity,andfreshnessofthemeasurementsandrequires knowl-edge of fingerprints (i.e., SHA-1 hashes) of the code involvedin blind processing. Secure root processes of the TPM areutilizedtodevelopauthenticatorsthatensureintegrityofprocessesusingtheCoreRootofTrustforMeasurement(CRTM) [71]–[73]. Moreover, as CRTM performs integritymeasurementatload-time,run-timevulnerabilitieswillbedetected using run-time attestation [70] and verifiable codeexecution[74]. Integritymeasurementofacompleteinteractivesystem isachallengingtask,asthousandsofmeasurementsand knowledge of their fingerprints may be required for varioussoftware [75], [76]. In [77] the authors investigated the in-tegrity of a known set of processes loaded in a deterministicorderandrunninginanisolatedenvironmentfromtherestof the processes. Using a security kernel, a system needs toensure integrity of the TPM, the BIOS, the security kernel andawell-knownsetofprocessesprovidingblindprocessing.

YANetal.:ASURVEYONCYBERSECURITYFOR SMARTGRIDCOMMUNICATIONS 9

$M_{Comm}|T|Sign[H(M_{Comm}|T)_{PR}$ ]

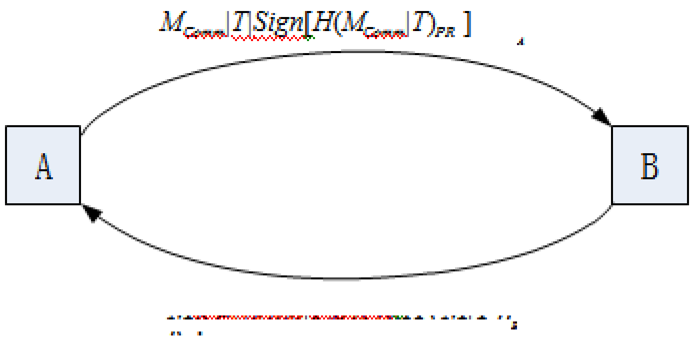


Fig.3.Digitalsignatureapproachforauthenticationandintegrity[81].

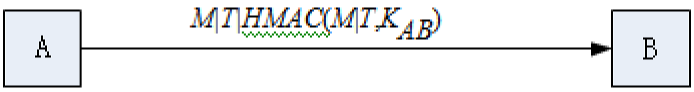


Fig.4.HMACapproachforauthenticationandintegrity[81].

thatwasknowntoAbeforeencryptedit,computesitsown

hash $H'(M'|T')$, and compares $H'$ with H. If they

$M_{Respone}|T|Sign[H(M|T)_{PR}$ ]

*C.* Authentication

Smartgridcommunicationsmustbeauthenticatedbyadding to the information flow transmission to verify whethera communication entity is the one that is claimed and thetransmitted data has integrity [78]. The mechanisms that pro-vide authentication usually alsoprovide integrity, the abilityto verify that a message has arrived unaltered from its originalstate. Authentication and integrity can help smart grid systemto protect against the most common cyber attacks, includingman-in-the-middle, forgery, impersonation, and message mod-ification. Numerous tools exist for providing authenticationandintegrity,includinghashesandkeyedhashessuchasSHA-1 or HMAC-SHA-1 and digital signatures such as RSA orECCsignatures[79].

One of the sophisticated attacks that authentication proto-cols must address is the replay attack, in which an adversarycaptures messages and replays them to the devices later. Amessage may have dramatically different effects dependingupon when it is received. For example, a message to increasereactive power output by 10 MVAr is appropriate to deal with alowvoltagesituation.However,ifthesamemessageis delayedand resent during a time when the system is experiencing highvoltages, the result of the same message willbe the oppositeof what was intended. There are two popular ways for helpingensure that a message is fresh and not a replay. If the systemcansupportthenotionoftimeandatleastlooseclocksynchro-nization, then timestamps can provide freshness. Therefore,timestamps have their own constraint on synchronization [80].Otheroptionsincludetheuseofnonces(randomnumbers)andsequence numbers. Nonces usually involve an extra messageexchange while sequence numbers, which identify the order ofindividual TCP packets, need reliable communication channelstoensuresynchronization.Anyauthenticationeffortmustprovide some waytoensure that amessage iscurrent andnottherebroadcastofapreviouslysentcommunication.

In [81], the authors proposed an authentication and integrityapproach that used digital signatures and timestamps. Fig. 3 il-lustrates this approach. Parties A and B reside within the samecommunication realm. A transmits to B the message $M_{Comm}$and a timestamp T in plaintext, along with the digital signatureofthemessageandtimestampcombination, $M_{Comm}|T$.Itcomputesthedigitalsignaturebyhashing $M_{Comm}|T$andthenencrypting itwithitsprivatekey $PR_A$. TherecipientB receives the plaintext message $M_{Comm}$and timestamp T,alongwiththedigitalsignature.Itdecryptsthesignatureusing A'spublickeytounwrapthehash$H(M_{Comm}|T)$ identical. Therefore, B can conclude that the message musthavebeensentbyA,sinceA'spublickeycanfaithfullydecrypt something encrypted by A's private key only; and thatthecombinationofmessageandtimestampwerenotalteredin transit. To guard against replay, when B confirms that thetimestamp it received matches what A tried to send, it willrecord the timestamp in its own log. If it receives anothermessage with the same timestamp later, it knows that the latermessagemustbeareplay,andcandiscardthat.

The digital signature approach might introduce more com-putational overhead than is necessary. Since confidentialitydoes not merit as much concern as authentication and integrityforreal-timecontrolinsmartgrid,anapproachthatdoesnot require an encryption step, HMAC [82], might be moreappropriate.Fig.4showsAsendsamessageMtoB attimeTusingHMACtoprovideauthenticationandintegrity.AandBsharesomesecret,$K_{AB}$.AlongwithMandT,AcomputesandsendstoBtheHMACofthecombinationM T . When this message arrives at B, B computes its ownHMAC of the combination M Tit received. If the HMAC Bcomputes matches the HMAC value received from A, then Bcan conclude, assuming no other entities have knowledge ofthe secret key $K_{AB}$it shares with A, that A must have sent themessageandthatnothirdpartyalteredthecombinationMTin transit. Therefore, B has authenticated the sender of themessage and verified the integrity of the contents. Verificationof message freshness works as that B will maintain a log ofreceived timestamps and reject later messages that have anidentical timestamp toone thatappears in thelog already.The reduced computational expense of HMAC makes it thepreferred authentication and integrity approach for situationswhereconfidentialityisnotaprimaryconcern.

*D.* TrustedComputing

Considering the incredible size of the cyber security threatand severe consequences from cyber attacks, the smart gridcyber security protection must be extremely tight to the cybersecurity requirements. Smart grid communication requires acomprehensive securityplanthat encompasses virtuallyallaspectsofsmartgridoperations.Onecomponentofsuchaplanincludestrustedcomputing.Fig.5showsabasictrusted computing model [83]. Such platforms and associatedmechanisms are used to ensure that malware is not introducedinto software processing devices. The main design goal is therealization of a minimal and therefore manageable, stable andevaluablesecuritykernelforconventionalhardwareplatforms,servers,embeddedsystems,andmobiledeviceslikePDAsandsmartphones. All requirements are fulfilled by extracting onlysecurity-criticaloperationsanddatatothesecuritykernel.

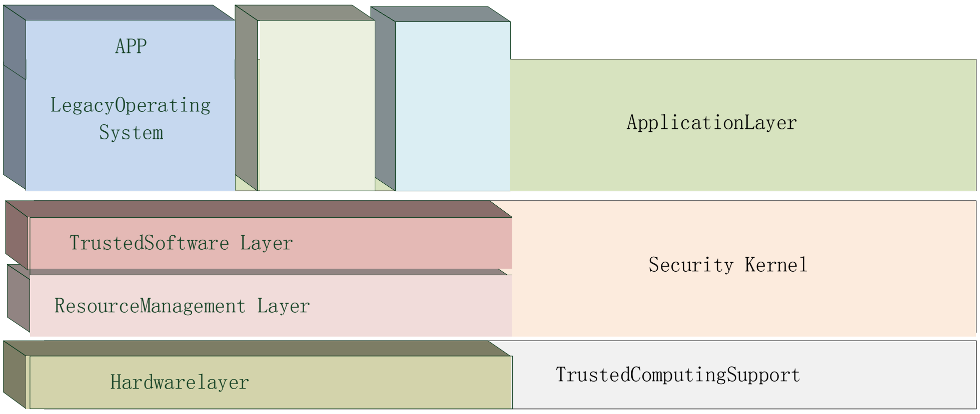


Fig.5.TrustedComputingmodel[83]

Therearetwocategoriesofdevicesforwhicht hemal-in the widespread deployment of a number of mobile codetechnologies. Mobile code is the code which is downloadedandrunonyourPC,typicallybyyourbrowser,withoutthe users' knowledge. Examples of mobile code include Ac-tiveX, Flash animation, Java, JavaScript, PDF, Postscript, andShockwave. TheDepartment of Homeland Security (DHS)Control System Security Program recommends tight controlson mobile code in critical control systems for the nation'scriticalinfrastructureandkeyresources(CIKR wareprotectionproblemsshouldbeconsidered:embedded computersystemsandgeneralpurposecomputersystems.Embeddedsystemsarecomputersystemsthataredesignedtoperformaspecifictaskorsetoftasks.Theyareintendedtorunonly software that is supplied by the manufacture. By contrast,generalpurposesystemsareintendedtosupportthirdpartysoftwarepurchasedbythespecificconsumerwhopurchasedthe system. A PC is an excellent example of a general purposesystem.Amicrowaveoven,orcabletelevision set-topbox,areexamplesofembeddedsystems.Theproblemofmalwareprotectionshouldbeconsideredseparatelyforeachcategory.For embedded systems the problem of protecting the systemagainsttheinstallationofmalwarecanbesolved withhighdegreesofassurance. Firstandforemostthemanufacturermust implement secure software development processes. Manystandardmodelsforsuchprocessesaredefined[84].Second,ifthedeviceisintendedtobefieldupgradable,theman-ufacturermustprovideasecuresoftwareupgradesolution.Thepredominantmethodofdoingthisistomanufacturetheembeddedsystemhardwarewithsecurestoragecontainingkeyingmaterialforasoftwarevalidation.Typ

)[86]. Toaddressthisconcern,theadoptionof,andadherencet o,strictcodesigningstandardsbysmartgridsuppliersand operators are proposed. Mechanisms for enforcing suchstandards on general purpose computers, such as PCs, havebeenputforthbytheTrustedComputingGroupan darewell documented [87]. Such standards should cover all criticaldevices including field deployed units, such as RTU and IED,networkdevices,suchasrouters,switches,andfirewalls,and

icallythehard-wareisconfiguredwiththepublickeyofasecuresigning serveroperated bythemanufacturer.Withthiskey,thedevicecanvalidateanynewlydownloadedsoftwarepriortorunningit.Suchaproactiveapproachcanprovidehigherlevelsofassurancethancanbeobtainedwithareactiveapproachsuch asaviruschecker.

For devices which are intended to run for long periods oftime(e.g.,years)withoutbooting,itisusefultohavea methodofperformingsecuresoftwarevalidationonrunningcode.Itispossibletohavebackground tasksthatcanperiodicallyperform suchfunctions without disrupting theoperations ofthe device. It is further possible to couple such backgroundvalidation steps with other operational aspects of the device,such that if the device is found to be compromised, securehardware on the device (needed to bring up and maintain se-curity associations with remote entities) will prevent the localdevice from establishing and maintaining security associationswith the remote entities. In [85], the authors described somemethodstoprovideremotedeviceattestation. Tomakemattersworse,therapidadoptionofcloudcomput-ingandsophisticatedInternetbasedapplicationshasres ulted control center equipment, such as servers and user consoles.The standards should cover embedded systems,as wellasgeneral purpose computers, their operating systems, drivers,andapplications,aswellasallmobilecodes.Th atis,nomobile code should beallowed torun on acriticalPCorserverthathasnotbeensignedbyanautho ritythatisabletodeterminethetrustworthinessoftheco de.Consideringthatitiscertainthathardwareandsoftw areelementsforcritical components of the grid will come from many differentproviders, it is likely that a trust management framework willhave to be established for smart grid. This framework willlikelyrequire theestablishment ofasetofcriteriathataretobemetbyvendorswhowishto sellcriticalcomponentsto smart grid operators. Additionally it is likely that one ormore accreditation organizations will need to be established toauditsupplierstodeterminethattheyaremeetingthes pecifiedcriteria[87].

## VI. CONCLUSION

As a critical infrastructure, smart grid requires comprehen-sive solutions for cyber security. A comprehensive communi-cation architecture with security built in from the very begin-ning is necessary. A smart grid communication security solu-tion requires a holistic approach including traditional schemessuch as PKI technology, trusted computing elements, authen-ticationmechanismsbasedonindustrystandards.Clearly,securingthesmartgridcommunicationinfrastructurewillrequiretheuseofstandards-basedstate-of-the-artsecurityprotocols.Toachievethevisionputforth,therearemanystepswhichneedtobetaken.Primaryamong themistheneedfora cohesive set of requirements and standards for smart gridsecurity. Industry and other participants should continue theworkthathasbegununderthedirectionofNISTtoaccomplishthese foundational steps quickly. However, the proper attentionmust be paid to creating the requirements and standards, asthey will be utilized for many years, given the lifecycle ofutility components. In this paper, we present the backgroundandrequirementsforsmartgridcommunicationsecurity.Afterdiscussingthechallengeofsmartgridcommunicationsecurity,the current research and solutions are surveyed. This papergivesaninsighttosmartgridcommunicationsecurityin architecturefeatures,systemdesignsaswellastechnicaldevelopment.

## REFERENCES

[1] C. W. Gellings, M. Samotyj, B. Howe, “The future’s smart deliverysystem (electric power supply),” IEEE Power and Energy Mag., vol.2,no.5,pp.40-48,Sept.-Oct.2004.

[2] H. Farhangi, “The path of the smart grid,” IEEE Power and EnergyMag.,vol.8,pp.18-28,2010.

[3] S. M. Amin, B. F. Wollenberg,“Toward a smart grid:power deliveryfor the 21st century,” IEEE Power and Energy Mag., vol.3, no.5, pp.34-41,Sept.-Oct.2005.

[4] Litos Strategic Communication “The Smart Grid: An Introduction ,” 31May2009[Online].Available:http://www.oe.energy.gov/DocumentsandMedia/DOESGBookSinglePages.pdf

[5] H.Khurana,M.Hadley,L.Ning,andD.A.Frincke,“Smart-gridsecurityissues,”IEEESecurityandPrivacy,vol.8,pp.81-85,2010.

[6] S. Clements, H. Kirkham, “Cyber-security considerations for the smartgrid,” in IEEE Power and Energy Society General Meeting 2010, pp.1-5,2010.

[7] C. H. Hauser, D. E. Bakken, A. Bose, “A Failure to Communicate,”IEEEPowerandEnergyMag., pp.47-55,Mar-Apr,2005.

[8] J. Fan, S. Borlase, “The evolution of distribution,” IEEE Power andEnergyMag.,vol.7,pp.63-68,2009.

[9] T. Baumeister, “Literature Review on Smart Grid Cyber Security,” TechReport,2010.

[10] C.LoandN.Ansari,“TheProgressiveSmartGridSystemfromBothPowerandCommunicationsAspects,”IEEE Commun. Surveys&Tutorials,pp.1-23,2011.

[11] S. Hong, and M. Lee, “Challenges and Direction toward Secure Com-munication in the SCADA System,” in Eighth Annual CommunicationNetworksandServicesResearchConference(CNSR2010),pp.381-386,2010.

[12] V.C.GungorandF.C.Lambert,“Asurveyoncommunicationnetworksfor electric system automation,” Computer Networks, vol. 50, pp. 877-897,2006.

[13] L. Wenpeng, D. Sharp, and S. Lancashire, “Smart grid communicationnetwork capacity planning for power utilities,” in IEEE TransmissionandDistributionConferenceand Exposition,pp.1-4,2010.

[14] E.Liu,M.L.Chan,C.W.Huang,N.C.Wang,and C.N.Lu,“Electricity grid operation and planning related benefits of advancedmeteringinfrastructure,”in 5th InternationalConferenceon CriticalInfrastructure(CRIS2010),pp.1-5,2010.

[15] P.P.Parikh,M.G.Kanabar,andT.S.Sidhu,“Op

portunitiesandchallenges of wireless communication technologies for smart grid appli-cations," in IEEE Power and Energy Society General Meeting,pp. 1-7,2010.

[16] A.R.Metke;R.L.Ekl,"SecurityTechnologyfor SmartGridNetworks,"IEEETrans.SmartGrid, vol.1,pp.99-107,2010.

[17] C.H.Wells,A.Moore,K.Tjader,andW.Isaacs," Cybersecuresynchrophasor platform," in IEEE/PES Power Systems Conference andExposition(PSCE2011),pp.1-4,2011.

[18] D. Dzung,M. Naedele,T. P. VonHoff, andM. Crevatin,"Securityfor Industrial Communication Systems," Proc. IEEE, vol. 93, pp. 1152-1177,2005.

[19] Reportto NISTon SmartGrid InteroperabilityStandardsRoadmapEPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf

[20] M.Zafirovic-Vukotic,R.Moore,M.Leslie,R.Midence,and M.Pozzuoli,"Secure SCADA network supportingNERC CIP," in Power& Energy SocietyGeneral Meeting,2009. PES '09. IEEE, 2009, pp.1-8.

[21] J.M.Guerrero,J.C.Vasquez,J.Matas,L.G.deVicuna,andM.Castilla,"Hierarchical Control of Droop-Controlled AC and DC Microgrids: AGeneral Approach Toward Standardization," Industrial Electronics, IEEETransactionson,vol.58,pp.158-172,2011.

[22] IEEEGuideforElectricPowerSubstationPhysicalandElectronicSecurity,IEEEStd1402-2000,2000.

[23] D. Dumont, "Cyber security concerns of Supervisory Control and DataAcquisition (SCADA) systems," in IEEE International Conference onTechnologiesforHomelandSecurity(HST2010),pp.473-475,2010.

[24] T. Zhang, W. M. Lin, Y. F. Wang, S. Deng, C. C. Shi, and L. Chen,"The design of information security protection framework to supportSmart Grid," in International Conference on Power System Technology(POWERCON2010),pp.1-5,2010.

[25] Draft smart grid cyber security strategyand requirements,NIST IR7628, Sep. 2009 [Online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

[26] S. Widergren, A. Levinson, J. Mater, and R. Drummond, "Smart gridinteroperabilitymaturitymodel,"in2010IEEEPowerandEnergySocietyGeneralMeeting,,2010,pp.1-6.

[27] S. Rohjans, M. Uslar, R. Bleiker,J. Gonzalez, M. Specht, T. Suding,and T. Weidelt, "Survey of Smart Grid StandardizationStudies andRecommendations," in First IEEE International Conference on SmartGridCommunications(SmartGridComm2010),pp.583-588,2010.

[28] National Institute of Standards and Technology, "Announcing the Ad-vanced Encryption Standard (AES)," in Federal Information ProcessingStandardsPublication,Nov.26,2001.

[29] National institute of Standards and Technology, "Data Encryption Stan-dard," Federal Information Processing Standards (FIPS) Publication 46-7,USA,1999.

[30] IEEEStd802.11i,"IEEEStandardforInformationTechnology-Telecommunications and Information Exchange Between Systems-Lo-cal and Metropolitan Area Networks-Specific Requirements Part 11:WirelessLAN MediumAccessControl(MAC)andPhysicalLayer(PHY) Specifications Amendment 6: Medium Access Control (MAC)SecurityEnhancements,"pp.1-175,2004.

[31] IEEE Std 802.16e, "IEEE Standard for Local and Metropolitan AreaNetworksPart16:AirInterfaceforFixedandMobileBroadbandWireless Access Systems Amendment 2: Physical and Medium AccessControl Layers for Combined Fixed and Mobile Operation in LicensedBandsandCorrigendum1,"pp.1-822,2006.

[32] A. Bendahmane, M. Essaaidi, A. El Moussaoui, and A. Younes, "Gridcomputing security mechanisms: State-of-the-art," in International Con-ference on Multimedia Computing and Systems (ICMCS '09), pp. 535-540,2009.

[33] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges intheSmartGrid,"IEEESecurity&Privacy,vol.7,pp.75-77,2009.

[34] K. Allan, "Power to the people [power energy saving]," Engineering &Technology,vol.4,pp.46-49,2009.

[35] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance eval-uation of IEC61850-based substation communication systems," IEEETrans.PowerDel.,vol.22,no.3,pp.1482C1489,July2007.

[36] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H.

Spafford, A. Sundaram,and D. Zamboni, "Analysis of a denial of service attack on tcp," in Proc.IEEESymposiumonSecurityandPrivacy (S&P1997),May1997.

[37] A. Yaar, A. Perrig, and D. Song, "Pi: A path identificationmechanismto defend against DDoS attacks," in Proc. IEEE Symposium on SecurityandPrivacy(S&P2003),2003.

[38] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoSdefensemechanisms,"SIGCOMMComput.Commun.Rev.,vol.34,no.2,pp.39C53,2004.

[39] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistantkey establishment using uncoordinatedfrequency hopping," in Proc.IEEE Symposium on Security and Privacy (S&P 2008), May 2008, pp.64C78.

[40] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcastcommunication without shared keys," in Proc. 18th USENIX SecuritySymposium(Security09),Aug.2009.

[41] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS:Jamming-resistantwireless broadcastcommunication,"in Proc. 29thIEEE Conference on Computer Communications (INFOCOM 10), Mar.2010.

[42] Y. Liu, P. Ning, and M. Reiter, "False data injectionattacks againststate estimation in electric power grids," in Proc. ACM Conference onComputerandCommunicationsSecurity(CCS09),Sept.2009.

[43] N.Kuntze,C.Rudolph,M.Cupelli,J.Liu,andA. Monti,"Trustinfrastructures for future energy networks," in IEEE Power and EnergySocietyGeneralMeeting2010,pp.1-7,2010.

[44] L. Husheng, M. Rukun, L. Lifeng, and R. C. Qiu, "Compressed MeterReadingfor Delay-SensitiveandSecure Load Report inSmart Grid,"in First IEEE International Conference on Smart Grid Communications(SmartGridComm2010),pp.114-119,2010.

[45] G. Carl, G. Kesidis, R. R. Brooks, and R. Suresh, "Denial-of-serviceattack-detection techniques," IEEE Internet Computing, vol. 10, pp. 82-89,2006.

[46] S. Kent, "On the trail of intrusions into information systems," IEEESpectrum,vol.37,pp.52-56,2000.

[47] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for CriticalInfrastructures: Attack and Defense Modeling," IEEE Trans. Systems,ManandCybernetics,PartA:Systems andHumans,vol.40,no.4,pp.853-865,July2010.

[48] W. Dong, L. Yan, M. Jafari, P. Skare, and K. Rohde, "An integratedsecuritysystemofprotectingSmartGridagainstcyberattacks,"inInnovativeSmartGridTechnologies(ISGT2010),pp.1-7,2010.

[49] M. Jensen, C. Sel, U. Franke, H. Holm, and L. Nordstrom, "Availabilityof a SCADA/OMS/DMS system - A case study," in IEEE InnovativeSmartGridTechnologiesConferenceEurope(ISGTEurope2010),pp.1-8,2010.

[50] T. Komura, Y. Nagai, S. Hashimoto, M. Aoyagi, and K. Takahashi,"Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol," in Ninth Annual International Sym-posium on Applications and the Internet (SAINT '09), pp. 235-238,2009.

[51] C.YongkaiandT.Shaohua,"SecuritySchemeforCross-DomainGrid: Integrating WS-Trust and Grid Security Mechanism," in Interna-tional Conference on Computational Intelligence and Security(CIS '08),pp.453-457,2008.

[52] R. Perlman, "An overviewof PKI trust models," IEEE Network, vol.13,pp.38-43,1999.

[53] R.J.Thomas,"Puttinganactionplaninplace," IEEEPowerandEnergyMag.,vol.7,pp.26-31,2009.

[54] A. R. MetkeandR. L. Ekl, "SmartGridSecurityTechnology,"inInnovativeSmartGridTechnologies(ISGT2010),pp.1-7,2010.

[55] D. Wu and C. Zhou, "Fault-tolerant and scalable key management forsmartgrid,"IEEETrans.SmartGrid,vol.2,pp.375-381,2011.

[56] T. M. Overman,R. W. Sackman,"High assurancesmart grid: smartgrid control systems communications architecture," in First IEEE Inter-national Smart Grid Communications (SmartGridComm 2010), Confer-ence,pp.19-24,2010.

[57] E. Santacana, G. Rackliffe, L. Tang, X.M. Feng, "Getting smart," IEEEPowerandEnergyMag.,vol.8,pp.41-48,2010.

[58] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymiza-tionof Smart MeteringData," in First IEEE InternationalConferenceon Smart Grid Communications (SmartGridComm 2010), pp. 238-243,2010.

[59] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda,“PrivacyforSmartMeters:TowardsUndetectableApplianceLoadSignatures,”inFirstIEEEInternationalConferenceonSmartGridCommunications(SmartGridComm2010),pp.232-237,2010.

[60] E.Cesena,G.Ramunno,andD.Vernizzi,“Securestorageusingasealingproxy,” In Proc. 1st European Workshop on System Security, pages 27-34,NewYork,NY,USA,2008.

[61] U.Kühn,M.Selhorst,andC.Stüble,“Realizingproperty-basedattesta- tion and sealing with commonly available hard and software,” In Proc.2007 ACM workshop on Scalable trusted computing, pp. 50-57, NewYork,NY,USA,2007.

[62] U.KühnandC.Stüble,“User-friendlyandsecuretpm-basedharddisk key management,”In Proc. First InternationalConferenceFuture ofTrustinComputing,pp.171-177,Berlin,Germany,2009.

[63] H.S.Fhom,N.Kuntze,C.Rudolph,M.Cupelli,J.Liu,andA.Monti,“Auser-centricprivacymanagerforfutureenergysystems,”inInternationalConference on Power System Technology (POWERCON2010), pp. 1-7,2010.

[64] K.J.Biba,“Integrityconsiderationsforsecurecomputersystems,”Technicalreport,MITRECorp.,Apr,1977.

[65] T. Fraser, “Lomac: Low water-mark integrity protection for cots envi-ronments,” In IEEE Symposium on Security and Privacy, pp. 230C245,2000.

[66] D. D. Clark and D. R. Wilson, “A Comparison of Commercial andMilitary Computer Security Policies,” In IEEE Symposium on SecurityandPrivacy,pp.184-194,1987.

[67] D.Kirovski,M.Drinic,andM.Potkonjak,“Enablingtrustedsoft-wareintegrity,”In proceedingsof the10th internationalconferenceonArchitecturalsupportforprogramminglanguagesandoperatingsystems(ASPLOS-X),pp.108-120,NewYork,NY,USA,2002.

[68] I. Sommerville, “Software Engineering,” Addison-Wesley, 8th edition,2007.

[69] R.S. Pressman,“SoftwareEngineering:APractitionersApproach,”McGrawHill,7thedition,20010.

[70] E. Shi and A. Perrig, “Bind: A fine-grained attestation service for securedistributed systems,” In IEEE Symposium on Security and Privacy, pp.154-168,2005.

[71] M. Alam, X. Zhang, M. Nauman, T. Ali, and J.-P. Seifert, “Model-based behavioral attestation,” In Proc. 13th ACM symposium on Accesscontrolmodelsandtechnologies (SACMAT08),pp.175-184,NewYork,NY,USA,2008.

[72] R.Sailer,T.Jaeger,X.Zhang,andL.V.Doorn,“Attestation-basedpolicyenforcement for remote access,” In 11th ACM conference on ComputerandCommunicationsSecurity,pp.308-317,2004.

[73] F. C. Schweppe and J. Wildes, “Power system static-state estimation,”IEEETrans.PowerApp.Syst.,pp.120-125,Jan,1970.

[74] A.Seshadri,M.Luk,E.Shi,A.Perrig,L.vanDoorn,andP.Khosla,“Pi-oneer: Verifying integrity and guaranteeing execution of code on legacyplatforms,” In ACM Symposium on Operating Systems Principles, pp.1-15,Oct.2005.

[75] J.M.McCune,A.Perrig,A.Seshadri,andL.van Doorn,“Turtles allthewaydown:researchchallengesinuser-basedattestation,”Inproceedingsof the 2nd USENIX workshop on Hot topics in security (HOTSEC07),pp.1-5,Berkeley,CA,USA,2007.

[76] F. Stumpf, A. Fuchs, S. Katzenbeisser, and C. Eckert, “Improving thescalabilityof platform attestation,”In Proc. 3rd ACM workshop onScalable trusted computing (STC 08), pp. 1-10, New York, NY, USA,2008.

[77] M. H. Gunes and C. Y. Evrenosoglu, “Blind processing: Securing dataagainst system administrators,” in IEEE/IFIP Network Operations andManagement Symposium Workshops (NOMS Wksps 2010), pp. 304-311,2010.

[78] International Standards Organization and International ElectrotechnicalCommission, ISO/IEC 9798-1:1997 Information Technology-SecurityTechniques-EntityAuthenticationParts.

[79] W. Stallings, “Network security essentials : applications and standards.”Boston:PrenticeHall,2011.

[80] R.J. Anderson,R.M. Needham,“Robustnessprinciplesfor publickeyprotocols,”inProc.15thAnnu.Int.CryptologyConf.AdvancesinCryptology(CRYPTO95),pp.236-247,1995.

[81] K. M. Rogers, R. Klump, H. Khurana, A. A. Aquino-Lugo, and T. J.Overbye,“AnAuthenticatedControlFrameworkforDistributedVoltageSupport on the Smart Grid,” IEEE Trans. Smart Grid, vol. 1, pp. 40-47,2010.

[82] Q. Dang, “Recommendationfor ApplicationsUsing Approved HashAlgorithms” National Institute of Standards and Technology SpecialPublication,2009.
[83] European Multilaterally Secure Computing Base, “Towards trustworthysystemswithopenstandardsandtrustedcomputing,”2005[Online]Available:http://www.emscb.com/content/pages/49373.htm
[84] N. Davis, “Secure software development life cycle processes,” SoftwareEng.Inst.,CarnegieMellonUniv.,2009.
[85] M. Shaneck, K. Mahadevan, V. Kher, and Y. Kim, “Remote softwarebased attestation for wireless sensors,” Comput. Sci. Eng., Univ. Min-nesotałTwinCities,2005
[86] U. S. Department of Homeland Security “Catalog of Control SystemsSecurity:RecommendationsforStandardsDevelopers,”Sep.2009.
[87] D.Challener,K.Yoder,R.Catherman,D.Safford,andL.V.Doorn,“APractical Guide to Trusted Computing”, Upper Saddle River, NJ: IBMPress.