Cyber Security for Protection Related Data Files

Report to the PSRC Main Committee from
WG H-18

Working Group Members

Amir Makki, *Chair*
Stephen Thompson, *Vice Chair*
Mark Taylor, *Secretary*

Tony Giuliante, *Advisor*
Stan Klein, *Subject Expert*
Abu Zahid, *Editor*

Arvind Chaudhary
Charles Sufana
Herb Falk
Joseph Hughes
Mark Peterson
Markus Braendle
Mike Childers
Neil Saia
Rick Cornelison
Vajira Pathirana

Sponsored by the
Power System Relaying Committee of the
IEEE Power & Energy Society

Table of Contents

Table of Contents

Cyber Security for Protection Related Data Files

(H18 Working Group Report, PSRC)

1. Assignment Statement

Develop a report on security for data files used for configuration, management, and analysis of protective relaying systems.

2. Background

Twenty years ago, cyber security was not a big concern for protection related data files because protection systems were mostly electromechanical and because dial-up and internet technologies were young and restrictive. Today, and after incredible advances in communication and embedded systems, protection systems are computer based and internet technologies are making their way into the substation. Cyber security is now a big concern. Utilities and various standards development bodies have heeded the call and are actively developing, refining and implementing standards for cyber security. Here is a list of examples:

- NERC CIP-002 through CIP-011
- NIST Cyber Security for Smart Grid
- IEEE P1711 Cryptography for SCADA
- IEEE 1686 Cyber Security for IEDs
- IEC 61850 Security Impact on Automation
- IEC 62351 Data and Communication Security

There are other standard development activities that are not directly related to cyber security but aid in security such as IEEE 1588 (Precision Time Protocol) which helps provide protection against replay attacks (repeating a previous command message, that without precision time stamping would be treated as a new message by the recipient). The collective efforts so far have mainly focused on managing physical and electronic access to protection equipment (data in motion issues) but have not specifically addressed access security for protection related data files (data at rest issues). Such files may contain critical information including passwords, phone numbers, IP addresses, settings, and load and fault records. The need to secure such files is clear and especially so because the files are transmitted between protection, control, and monitoring equipment (SCADA, HMIs, Master Stations, laptops) and exchanged between humans for analysis and maintenance purposes.

3. Security versus Functionality

A house without doors and windows is a secure environment but the problem with such a house is that you can never enter or leave. The same is true with securing protection related data

files. We can encrypt and protect each and every type of file but this will hinder configuration, management, and analysis procedures. The more security we add the less access we get. Accordingly, we need to strike a balance between security and access, a balance that does not hinder the business but one that provides a sufficient level of security.

4. Purpose of Report

The main subject of this report is to address access security for protection related data files: "data at rest issues". The working group members began with discussions on the need for developing this report. The discussions covered a wide range of comments starting with "there is no need for such security" and ending with "it is critical to have tight security". Excerpts of these discussions are listed in Annex-C as letters to the Chair. In the end, the members agreed on the need to develop this report.

5. Protection Related Data File Types

The working group members identified the following list of commonly used types of protection related files (i.e. files that are used for analysis, configuration, and management of protection related equipment):

File Type	Contents	Description
Manuals	Includes drawings, operation guides, and other types of documentation including inventory/spare equipment lists	Annex A.1
Ratings	Includes equipment, environmental, and seasonal ratings	Annex A.2
Settings	Includes operate levels and logic and zones of protection	Annex A.3
Measurements	Includes events (fault, disturbance, sequence of events) and load records (peaks, forecasting, and planning)	Annex A.3
Access	Includes phone numbers, IP addresses, passwords, keys	Annex A.4
Testing	Includes calculations for settings, coordination, simulation, and modeling	Annex A.5
Generator Dispatch Orders	Includes electricity pricing, arrangement of the transmission network, generation constraints	Annex A.6
Maintenance Schedules	Includes major substation equipment and those that are at greatest risk of failure	Annex A.7
Programs	Includes upgrades/updates of firmware and/or executable program code	Annex A.8

6. Report Summary

The working group members addressed each type of file individually, in the form of assignments. Each submitted assignment is composed of four sections: type definition, risk assessment, comments, and security recommendations. The results are listed in Annex-A as matrices that relate file types against risks/consequences and mitigations. Risk assessments are categorized based on confidentiality (risk of disclosure) and integrity (risk of compromise).

In general, the members agree that integrity is usually a high priority but that confidentiality is sometimes a lower priority.

Additional discussions on security protection for data files and communication from a generic perspective along with a summary of current practices are provided in Annex-B.

Annex – A

Risks, Consequences, and Mitigations (File Types Matrix)

A.1 Manuals and Other Documentation:

Type definition	Risk assessment	Comments	Security recommendations
Drawings	Risk is high, especially if the prints show cable routing (i.e. tunnels) or physical layout. Integrity risk: high Confidentiality risk: high	Print types that could be compromised or used for terrorist activities include: Current/potential 3 wire schematics Current/potential/protection 1 line diagrams Relay tripping schematics Cable physical routing prints Cable identification tables Physical layout of transformers, circuit breakers, bus structures, generating station equipment (there could be even clues as to what type steel or concrete was used) Relay panel physical layout	The files should be password protect. Consider encryption of the file. Have a log that indicates who has copies of the prints.

Type definition	Risk assessment	Comments	Security recommendations
Equipment manuals	Risk is medium Integrity risk: low Confidentiality risk: medium	Many of the equipment manuals are available in the public domain; thus very little might be gained by having the actual station equipment manuals compromised unless the equipment is user specific and custom built.	If the equipment is custom for the utility then, consider the following: Provide password protection for the files. Consider encryption of the file. Have a log that indicates who has copies of the procedures.
Transmission and Distribution System Operation Procedures	Risk is high Integrity risk: high Confidentiality risk: high	Typically these types of operation procedures show what should be done for certain operating conditions. Many companies have entire system blackout restoration plans that need to be safeguarded. These plans might show vulnerable locations which could be compromised.	Provide password protection for the files. Consider encryption of the file. Have a log that indicates who has copies of the procedures.
Black Start Procedures	Risk is high Integrity risk: high Confidentiality risk: high	Should there be a major blackout requiring a black start, then the procedures might show vulnerable locations which could be compromised.	No company wide set of passwords, be station specific or even user specific. Consider encryption of the file.

Type definition	Risk assessment	Comments	Security recommendations
Post Disaster (storm, flood, snow, ice) recovery procedures	Risk is medium to high Integrity risk: high Confidentiality risk: medium to high	Should there be a major storm requiring a major restoration effort, then the procedures might show vulnerable locations which could be compromised.	No company wide set of passwords, be station specific or even user specific. Consider encryption of the file.
Nuclear station licensing and operation procedures	Rick is high Integrity risk: high Confidentiality risk: high	As the licensing and operation procedures identify every piece of the nuclear station, then the weak points of the station could be identified.	No company wide set of passwords, be station specific or even user specific. Consider encryption of the file.
Relay settings	Risk is high Integrity risk: high Confidentiality risk: high	Passwords: If the passwords were compromised, then the relays could be remotely accessed and lines could be tripped. I/O settings are often contained within the setting files and could identify the exact phone lines, fiber line, etc., any of which if interrupted could lead to widespread outages. Logic equations: If the logic equations were	No company wide set of passwords, be station specific or even user specific. Have a procedure in place wherein the load dispatchers or relay protection engineers can routinely and automatically check to see if the settings have been compromised. Consider encryption

Type definition	Risk assessment	Comments	Security recommendations
		changed, then the relay may not trip for a planted fault or trip in error for a non-fault condition. Settings: If the settings were compromised, then the relay may not trip for a planted fault or trip in error for a non-fault condition.	of the file.
Inventory and Spare Lists	Risk is medium Integrity risk: low Confidentiality risk: medium to high	The concept here is that knowledge of inventory and spare lists may help hackers focus on the weak links in the system (attack those equipment that are difficult/time consuming to replace especially where spare parts are not in inventory)	Have a process in place to store these files in a secure location (access by authorized personnel only) Consider encryption of these files.

Comment: Utility practices may have to be developed to manage the security issues for manuals.

A.2 Ratings:

Type definition	Risk assessment	Comments	Security recommendations
Equipment Ratings	Medium Risk	Knowing the current rating of a line or breaker and so forth would make it easier to find the weak link in the system or to set up a failure by opening or failing certain other lines.	Keep internal information about line ratings etc. secure by password
Environmental Ratings	Low Risk	If equipment is ordered with good margins of operation then knowing these ratings would have little effect and would be easy to find through the manuals.	
Seasonal Ratings	Low Risk	Anyone with a reasonable knowledge of the operation of electric systems could make a good guess about the temperature and season that the equipment is at the greatest risk of failure.	

A.3 Settings and Measurements:

Type definition	Risk assessment	Comments	Security recommendations
Settings	Risk is high Integrity risk: high Confidentiality risk: low	Settings files contain the parameters used to set relays. They include operate levels and logic and zones of protection. This does not include files containing passwords or other information on accessing relays. If a settings file is changed, the relay could be set either to operate too sensitively or to not operate at all. If settings are too sensitive, the relay may operate as soon as it is put in service - at which time, the difference in the intended (gotten from the secured database) and actual (gotten from the relay) settings could be determined. If the relay does not operate shortly after the corrupted settings are applied, then with the recommended feedback, the chances are good that the	Store permanent settings in limited access, password protected files. Compare settings in file to those in relay before applying to the relay. Any unexpected differences should be questioned. Limit exposure of the files that are to be uploaded to the relay. The time from generating the settings file to uploading to the relay should be kept at a minimum. While the integrity risk of settings files is high, with the exposure limited. There is a very tiny window of opportunity for contamination of these less secure files. Also, with limited exposure, very few settings files will exist at any one time. So even if a few files were compromised, the system would not necessarily suffer

Type definition	Risk assessment	Comments	Security recommendations
		differences would be discovered and corrected before the relay is called on to operate.	major problems. A feedback loop should be employed where the newly applied settings are downloaded from the relay and compared to the secured settings calculation database to insure that what was sent out was loaded into the relay. If remotely set, the relay should not be placed in service until confirmation is made.
Measurements	Risk is low to medium Integrity risk: Low to medium based on user decision Confidentiality risk: Medium	Measurement files are data files from IEDs. They include data on events (fault, disturbance, sequence of events) and load records (peaks, forecasting, and planning). There is no risk to the IED if its measurement files are contaminated. Utilities get corrupted files regularly and are not overly concerned because they have other means of conducting analysis. Moreover, data collection systems collect large numbers of measurement files (thousands per month) most of which end up	No extraordinary measures are needed to protect measurement files. Measurement data are invaluable in analyzing system problems, system operations, and planning for future enhancements to the system. While information from these files could provide an economic edge to power producers, and lack of or incorrect information could hamper operations and analysis, there is little information in these files that could aid

Type definition	Risk assessment	Comments	Security recommendations
		being deleting. To that extent, for those few measurement files that may be deemed critical then integrity risk can be stated as medium or high but that is a choice the user has to make.	cyber attackers. It could be argued that load and source centers could be identified with these data, but satellite images readily available on the internet could be used to determine load and source centers by tracking where many transmission lines come together.

Comment: Utility practices may have to be developed to provide a feedback loop that confirms that the new settings were sent from a secured settings database. The relay, if remotely set, should not be placed in service until this confirmation is made. This would prevent a hacker from trying to set all direct trip, zero sequence over-current elements in a substation to a low value that was just above the maximum system unbalance. Such changes in settings would result in the tripping of all substation circuit breakers for the first fault that occurs after a hacker resets the relay settings.

A.4 Access: File types for usernames, addressing, and security credentials

In analyzing this data at rest issue, this information would typically be presented or stored as a sub-field in some other file type. Therefore, the recommendations that follow apply only to the sub-fields and not the entire file.

The protection of the sub-fields must be recoverable and known by several individuals. This is due to the fact that if the information can not be recovered (e.g. shift or other) it could lead to operational problems. Therefore, when protection is suggested it would typically be grouped based protection and not individually oriented protection.

Type definition	**Risk assessment**	**Comments**	**Security recommendations**
Addressing Information	Risk, in general is medium. However, may be high depending upon the protocol and deployment architecture. For private networks, medium risk would be assumed. However, for protocols/IED implementations that do not support user credentials, the risk would be considered high.		No protection for medium risk, just limit access to the entire file. Symmetric sub-field, group key, encryption for high risk

Type definition	Risk assessment	Comments	Security recommendations
Username	The risk in general is low if there are additional security credentials used by the IED/implementation to allow access and role determination. The risk is high if no additional security credentials are used.	Usernames, within our domain may be group based (e.g. a group of users make use of the same user name) or individual based.	Limit access to the entire file or low risk, group based, usernames. For low risk, individual usernames, it is recommended that this information be stored within a file that can only be accessed by the specified individual. For high risk, individual usernames, it is recommended this information be stored within a file that can only be accessed by the specified individual. It would also be recommended that the sub-field be encrypted using asymmetric encryption as a minimum. If sub-field encryption is not possible, it is recommended that each high risk username be contained in a file that is appropriately encrypted. For such situations, only one username per file should be stored.

Type definition	Risk assessment	Comments	Security recommendations
Authentication Credentials Within this scope, authentication credentials refer to passwords, security tokens, digital certificates, and encryption keys.	The risk for this information is dependent upon the type of credential: Password = High risk Security Tokens = Low risk. Public digital certificates = Low risk. Private digital certificates= High risk Encryption keys can be categorized as public, private, and group. Public keys = low risk Private keys = high risk Group keys = high risk The overall risk, for these credentials, is partially determined by policy and if the username is shared or individual. Typically, similar credentials may		For low risk, limit access to the file. For high risk, encryption of the sub-fields is recommended. If sub-field encryption is not possible, it is recommended that each high risk credential be contained in a file that is appropriately encrypted. For such situations, only one credential per file should be stored.

Type definition	Risk assessment	Comments	Security recommendations
	be used to authenticate to multiple endpoints. If this is done, this represents a high risk scenario except for public certificates and keys.		

Comment: Limiting access is suggested. Authentication credentials are recommended to have encryption if risk is high.

A.5 Relay Testing:

The overall security risk associated with relay test information is relativity low. The information that can be deducted from the relay test results and test plans information is as follows: The trip setting magnitudes for the protective elements, the protection scheme being used to protect the line, and the reclosing scheme being used.

In some modern relay test software applications the relay settings and control logic are stored as part of the relay test plan. The relay test program can log into the relay and change protective logic settings to perform automated testing. To log into the relay and make changes the test program needs to know the passwords for the relay and in some cases the communication paths and IP addresses for the relay. The passwords can be stored as part of the relay test plan or the relay test program can prompt the user to enter the password data as the program needs to eliminate the need to have the password information in the relay test file. Having the passwords and IP addresses stored as part of the relay test file would elevate the security risk of the information.

The relay settings and modeling information is also a low security risk to power system security. The only stretch on a security issue would be if enough relay and modeling information on the power system could be put together where under a certain system loading conditions a fault could be placed on the power system to make the system to go unstable.

Comment: Relay testing as a general comment is low risk. Repair should also be considered. For example if a relay is sent in for repair then the information within the relay should to be wiped.

A.6 Generator Dispatch Order:

The generator dispatch order can be considered one of the highly sensitive information, especially in a deregulated market environment. The knowledge of the generator dispatch order can be used for manipulating the electricity price in the market. The generator dispatch order is arranged so that energy is always dispatched in merit order based on the marginal cost of a generator unit, also considering the arrangement of the transmission network. Marginal costs, however, are confidential pieces of information that energy producers treat as corporate secrets. Therefore it is important that dispatch order information is kept confidential.

The generator dispatch order may not be highly sensitive information in a "non-deregulated" environment. However, knowing the transmission and generation constraints, it could become easier to find the weak link in the system and for example set up a failure by opening the weak link in the system.

Type Definition	**Risk Assessment**	**Comments**	**Security Recommendations**
Generator Dispatch Orders	Risk is medium to high Integrity risk: Medium Confidentiality risk: High	Transmission constraints may cause deviations from what would otherwise be minimum cost dispatch in order to maintain system security. If someone could get in and tamper with the generation dispatch order file, they could compromise system economics.	Provide password protection for the files. Consider encryption of the file.

A.7 Maintenance Schedules:

The maintenance schedule may not be considered highly sensitive information in a utility. However, someone with a reasonable knowledge of the maintenance schedule could make a fair guess about the equipment that is at the greatest risk of failure since certain equipment could be operating under N-1 or N-2 contingency situation due to some of the equipment being taken out of service for maintenance. Therefore with the knowledge of the maintenance schedule, someone could find a weak link in the system at a given time.

Type Definition	**Risk Assessment**	**Comments**	**Security Recommendations**
Maintenance schedule	Risk is medium Integrity risk: Medium Confidentiality risk: Medium	The maintenance of equipment at one station could also affect a larger area surrounding it. Maintenance could involve a lot of staff in a utility. Therefore it could become difficult to keep the maintenance schedule in a utility confidential. If someone could tamper with the maintenance schedule files, they could cause equipment to be taken out of service for maintenance when it might be needed most.	The files should be password protected. Consider encryption of the file.

A.8 Programs:

Type definition	Risk Assessment	Comments	Security recommendations
Installation of software (configuration programs, diagnostic tools, etc.) or IED firmware	Risk is low to high Confidentiality Risk: Low Integrity Risk: Low probability of occurrence but high potential of severe damage if compromised	The main risks posed by a cyber criminal to such software and firmware would be to corrupt it so as to make it unusable, or to modify it so as to cause unexpected or undesired results or operation of an end device. Modification of the installation files so as to cause the program to appear to the user to operate properly while it generates improper results, would be extremely difficult and would require lengthy reverse engineering by the criminal. However, integrity is absolutely critical to proper operation of equipment. Tampered software/firmware may not be evident to the user, and could include a wide variety of injected functionality that is very dangerous (sophisticated). For example, imagine firmware that works as designed except during certain date and time windows or until a bad guy signals it to stop working.	Limit access to the installation files or media. Due to the inherit risk associated with thumb drives, only approved company-issued protected thumb drives should be used to transfer and/or install such software and firmware. The use of personal thumb drives should not be permitted.

Annex – B

Security Protection for Files and Communications (Discussions and Current Practices)

B.1 Protection Goals

The general goals of security protection include:

- Confidentiality: Preventing unauthorized disclosure.
- Integrity: Preventing unauthorized modification. Non-repudiation is integrity for digital agreements.
- Availability: Ensuring authorized users have timely access.

Security issues include when and where protection is provided. Different considerations apply if security is an issue only during communications exchange or at all times. Most protection is provided by security controls outside the scope of the specific application or data format specification. In particular protections are provided by the platform operating system and the communication system.

The platform operating system provides access control protection that addresses the goals as follows:

- Confidentiality is protected by controls on file reading and possibly on execution of applications that access and interpret the file.
- Integrity is protected by controls on file writing and possibly on execution of applications that access and create or modify the file.
- Availability is protected by controls on file deletion and possibly by other measures that prevent exhaustion of platform resources needed for file access.

The communication system provides protection that addresses the goals as follows:

- Confidentiality is protected by file encryption during transmission.
- Integrity is protected by file authentication during transmission.
- Availability is protected by controls that counter denial-of-service attacks.

Certain other controls can be applied at the level of the file or application. The controls depend on the nature of the file format. For general file formats, there are controls that can be

applied to the entire file. For XML files, there are controls that can be applied to sub-parts of the file, generally at the level of XML elements.

For a comprehensive catalog of security controls and details on their application to electric power systems, see NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.

B.2 File Security Protection

B.2.1 Format independent

Format-independent file security protection applies protections to the overall file. The protections can include encryption or file authentication (integrity protection): Encryption involves selection of an algorithm, a key length, and a mode of applying the algorithm. Encryption protects confidentiality and may protect integrity if a proper mode is selected for the encryption algorithm. An example of a mode that does not protect integrity would be one in which the algorithm were used to create a sequence of bits and the bits were just serially exclusive-ORed to the sequence of data bits. Changing one of the encrypted bits would preserve confidentiality but modify the data.

The file authentication can be of two kinds:

- Un-keyed hashing: This applies a general hashing algorithm, such as one of the SHA series, to the file. The algorithm will produce a result for the file. The result can be incorporated into a file or message format or can be supplied separately. To check the file integrity the same algorithm is applied to the file and the results should agree.

- Keyed hashing: This also applies a hashing algorithm, such as one in the HMAC or AES-GMAC series. The algorithm uses a key. The key will need to be managed so it is available when the integrity hash is calculated and when it is checked. Just as with un-keyed hashing, the result can be incorporated into a file or message format or can be supplied separately. To check the file integrity the same algorithm is applied to the file using the same key and the results should agree.

Availability protection of a file can only be provided by the local operating system of the platform on which the file resides. The protection is provided by the access controls of the operating system. Protection against deletion is the most critical for maintaining availability. However, knowledge of the file existence (as obtained by viewing the relevant directory) may also be important. In addition, procedures such as backing up files provide protection against erasure due to hardware/software failure or inadvertent error by authorized users.

B.2.2 Format-specific for XML files

XML files can be protected by format-independent means. However, there are format-specific protections that can also be applied. XML-specific protections can address

confidentiality and integrity. They can protect either the entire file or specific parts, generally at the level of XML elements. These protections generally use the same technologies that are used for format-independent protection but apply the protections only to part of the file and use the markup capabilities of XML to identify which parts are protected and which parts remain unprotected.

The relevant XML standard for confidentiality is XML Encryption Syntax and Processing. For both integrity and non-repudiation the relevant standard is XML Signature Syntax and Processing.

There is a special issue that affects XML files to which cryptographic technology has been applied. In XML, white space (spaces, tabs, new lines) affects readability but not document content. Two XML documents with different white spaces are identical from an XML viewpoint. However, when they are encrypted or integrity-protected, the two resulting files will be completely different. The approach for resolving this issue is to standardize the white space using a standard called Canonical XML. As with format-independent protection, availability can be protected only by the local operating system.

B.3 File Communications Protection

B.3.1 Format independent

Communications protection can be provided at several layers in the communications stack. Protection at the physical layer is sometimes called “bump-in-the-wire” because it is invisible to the communicating systems. The only truly format-dependent protection is at the application layer. All other layers provide format-independent but protocol dependent protection.

At each layer confidentiality is provided by encryption and integrity by authentication. The major difference is that the encryption or authentication is on the basis of communication data units rather than files. Availability is provided by the ability of the communications system to avoid denial-of-service. Also, if protection is provided in a particular layer, its characteristics depend on the protocol at that layer and are generally independent of what is happening at the layers above.

B.3.2 Format dependent

XML has format-dependent, XML-specific communications protocols called Web Services. Messages sent by web services can be protected on the same basis as XML files using variants of the same protection methods. Users of web services communications have a choice between application layer protection and lower layer protection. As an example of lower layer protection, the most popular communications technology for web services messaging is http, the hypertext transfer protocol. Web services messages can be protected using transport layer security (TLS) which is ordinarily used to secure http.

Web services communication can also be protected at the application layer using the same XML encryption and authentication technology used for XML file protection. This is the approach taken in the Web Services Security standards. The web services standards also support application layer message switching that uses XML-aware technology above the network layers at which switching normally takes place. This has implications for overall system security design.

B.4 Other Issues

B.4.1 Key management

Any system of encryption or keyed authentication requires keys. Such keys must be managed, and key management is historically the weakest point of such systems. For a detailed discussion see NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Chapter 4, Cryptography and Key Management.

B.4.2 Switching

Switching can be performed at the network or application layers. A critical factor in communications protection is the trustworthiness of the switches and the extent to which details of the communications are exposed during switching.

B.4.3 Selection of protections

Selecting the appropriate protections for any particular system should begin with a risk analysis. Factors to be considered in such an analysis include:

- The importance of the overall application,
- The sensitivity of the system and the data,
- The consequences of system or data becoming compromised,
- The threat landscape:
    - Who are the threat agents?
    - What are their capabilities?
    - What might they gain by compromising the system or its data?
    - Is the system is sufficiently important to assume that it will be attacked in any way feasible?
- The various system engineering tradeoffs and considerations involved in the system design.

The risk analysis will drive the selection of security protections including:

- What to protect,
- How it should be protected (confidentiality, integrity, availability), and
- How intensively to protect it (e.g., selection of encryption key lengths).

Annex – C

Letters to the Chair, Discussions on the Need to Report on Cyber Security for Protection Related Data Files

Letter I: The report is needed by many in the power industry because they do not have a clear understanding of what is required of them. Often times, the result of this ignorance is that drastic nonsensical "security" steps are taken that have a net effect that is detrimental to the operation of the power system.

Letter II: Part of the issue will be identifying which types of files need securing and why. Some files can just have simple password protection whereas others may need full-blown encryption. Some file types, especially XML (SCL) files may even be partially secured using techniques outlined by Stan in his presentation. Another point is data organization and process management. By that I mean that, as shown in the example you presented, having to have passwords embedded in a text file in order to allow some automated tool to access the system is a clear vulnerability, but it should be possible to re-organize the data requirements or process mechanism to avoid the problem.

Regarding file data encryption, key management is a big issue:

- If a file is partially or totally encrypted, how will the key be managed? Who manages the keys?
- If the file is not accessed for several months/years will the accessing s/w be able to find which key was used, or know which algorithm was used for encryption? The key and the algorithm type have to be stored (or known) somewhere.
- A shared key system may be OK providing that the key has not been compromised. If this happens then it necessitates the change of the key in both the encryptor and the decryptor, but what about files already encrypted using the old key? Would (or should) they need updating to be recrypted using the new shared key? (Is there even such a word as recrypted?)
- A PKI system may mean issues with certificate management/authority. How can this be done?

There probably are mechanisms for handling these issues but which are appropriate to our needs and environment?

Letter III: Security for file exchange is good for this group to work on since protection engineers are in the best position to understand what is at risk if a file is altered or hacked. Ideally security mitigation should be commensurate with what is at risk. Developing a report to capture these issues could be a good contribution to the industry.

Letter IV: My inputs are mostly about the need to first define the risk associated with data files as well as the goals of security before recommending any solutions. We first need to gain a better understanding of what the potential risks of disclosure, modification, deletion, etc. of data files are before we can start to discuss how to protect them. I have seen too many cyber security working groups that do not look at the risk first, but start by defining technical solutions! Also the work should look at this in context of overall end-to-end security and work with H13.

Letter V: I would say we have to first define what are the protection related data, are SLD, IED Configuration Files, Test Procedures, Test Results etc. protection related data? Then we need to document the current practices of storing and managing these data? Are they kept in secured DB server? What are the potential threats to these data? Then may be we can think of what tools are required or if manufacturer's relay software should provide security level to their relay software and may be server based software etc. We can think of the utility practice as well.

Letter VI: The chief need for security for configuration files is for the integrity of the data. There is very little information that can be obtained from these type files that could cause harm. If configuration files are corrupted just before uploading to the relay, then the system could suffer. The time from approval to uploading is fairly short.

Assuming management contains passwords or other such information to access relays, then the security for these type files is high. Much damage could be done by accessing the relays themselves.

Analysis data should be considered a low risk. Very little harmful information is available in these files. We are accustomed to sometimes receiving corrupted or no data due to machine or delivery problems, so corruption by some external entity is of little concern.

Letter VII: The working group should report on the need to secure protection related data files that originate from, or are downloaded to, protection related equipment. The report should include discussions on version control, non-repudiation, tamper proofing, confidentiality (encryption), safe storage, loss prevention, and on best practices for file manipulation and access to protection related data.

