PERA USER GUIDE

Preparing a
Corporate Cybersecurity Master Plan
for a Process Industry Owner / Operator

January 2, 2024

Master Planning Guide
01-1-1

Industry	Process
Principal Role	Owner / Operator
Professional Role	All
Enterprise Phase	Master Planning

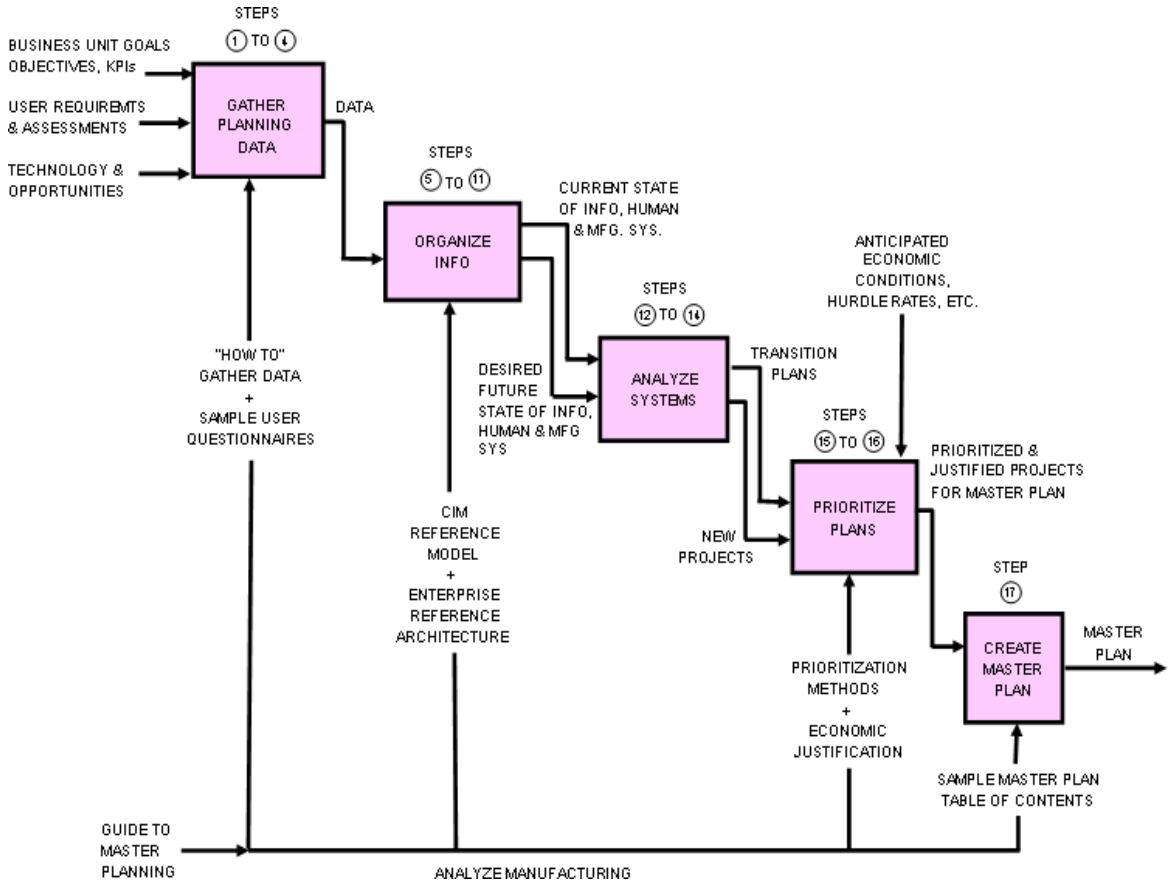
Overview of Master Planning Process

The PERA master planning process is comprised of 18 clearly defined steps plus two steps to be carried out after the plan is approved and issued. Each step produces a set of deliverables (e.g. reports or drawings) which are reviewed and approved by management before proceeding to the next step.

This document provides a "Guide" for each step in the Master Planning Process. For additional details, see the Handbook of Master Planning" on the PERA website (www.pera.net). The "Steps in this document exactly correspond to Chapters in this Handbook.

Master Planning Activities:

The following diagram indicates key information that should be assembled, reference materials, and a time sequence for assembling and analyzing this information.



In this User Guide, it is assumed that the Owner/Operator wishes to implement a Corporate Cybersecurity Program that includes:

- Automation and Control Systems (ACS),
- Operational Technology systems (OT), and
- IT systems, including Business Systems, Sales and Marketing, and Corporate support.

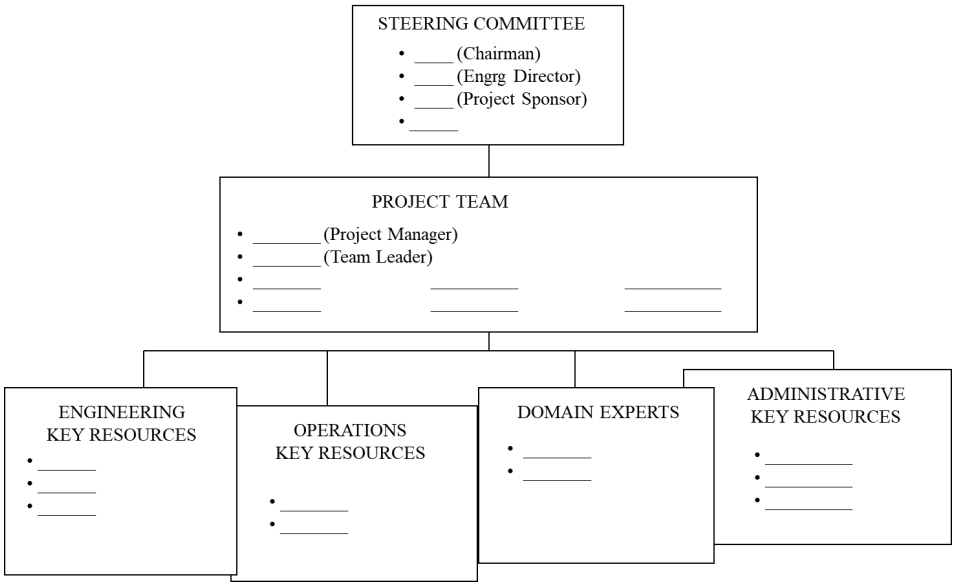
Although it is possible to complete a Master Plan for only ACS, or IT Cybersecurity, for the above scope, participation by both Engineering and IT management and staff in the Master Planning Study will be essential.

Master Planning Organization

The risks and costs associated with cyber-attacks are too high to simply assign technical project and operations personnel to “solve the cybersecurity problem”. It is therefore essential that “board-level” representatives oversee and guide the corporate cybersecurity program

The Cybersecurity program should be created and managed by business and technical leadership, via a tiered Cybersecurity Steering Committee. This may include at the first tier, CEO, CTO, COO, CFO, CIO and H/R, as well as at the second tier, senior staff in their organizations who are involved with cybersecurity standards and procedures, such as the CISO (Chief Information Security Officer), Engineering Management responsible for ACS (Automation and Control Systems, and the Corporate Security Manager.

MASTER PLAN ORG CHART



One of these executives should be given the role of “Program Champion”. The Chief Technical Officer is a logical choice, as the CTO is responsible for engineering staff who design major projects, and operations staff who operate ACS control systems. The Champion will report progress on the ACS Cybersecurity Program to a review board, that should include major stakeholders including representatives of:

- Plant Operations
- Capital Projects
- IT Operations
- Control and Automation Systems
- Physical Plant Security
- Corporate Risk Management
- Health, Safety and Environmental

Master Planning Schedule

Tasks						
Meeting with the Steering Committee						
Interview Key Players						
Confirm Goals, KPIs, Policies						
Plan Approach Develop Forms						
Set up the Review Schedule						
Finalize Policy Definitions						
Release Survey Forms & Interview Key Resources						
Research & Document 30 Opportunities, including Requirements, Costs & Benefits						
Steering Committee Review # 1						
Review requirements with Key Resources						
Steering Committee Review # 2						
Identify Standards including requirements						
Identify and Document 5 Projects including Scope, Schedule & Budgets						
Cost/Benefit Analysis of the overall program						
Document Staffing/Training/Transition Plan						
Steering Committee Review # 3						
Prepare Final Report						
Present Final Report and Master Plan						

Master Planning Budget:

Using ISA/IEC 62443 and PERA Master Planning, expenditures for initial phases of ACS Cybersecurity Program Planning are relatively modest, and can probably be funded from existing standards and training budgets. However, creation of the actual corporate program will likely require several months with a dedicated small team.

It should also be noted that the personnel required for an ACS Cybersecurity Program Plan should largely be drawn from existing enterprise resources. It is not possible to create an effective ACS Cybersecurity Program without engineers and technicians who have a deep understanding of the corporation's industrial facilities, ACS, industrial networks, hazards, and organization.
Thus, even if "cyber-certified" engineers and specialists were available, the cost to train these new hires or consultants would be excessive, and in any case, would delay implementation of an effective ACS cybersecurity program by many months or years.

The best approach is therefore to support and encourage professional development of current staff, including ACS cybersecurity training and certifications. This may be accomplished in parallel with creation of the ACS Cybersecurity Plan and implementation of the resulting Corporate ACS Cybersecurity Program.

Master Planning Resources

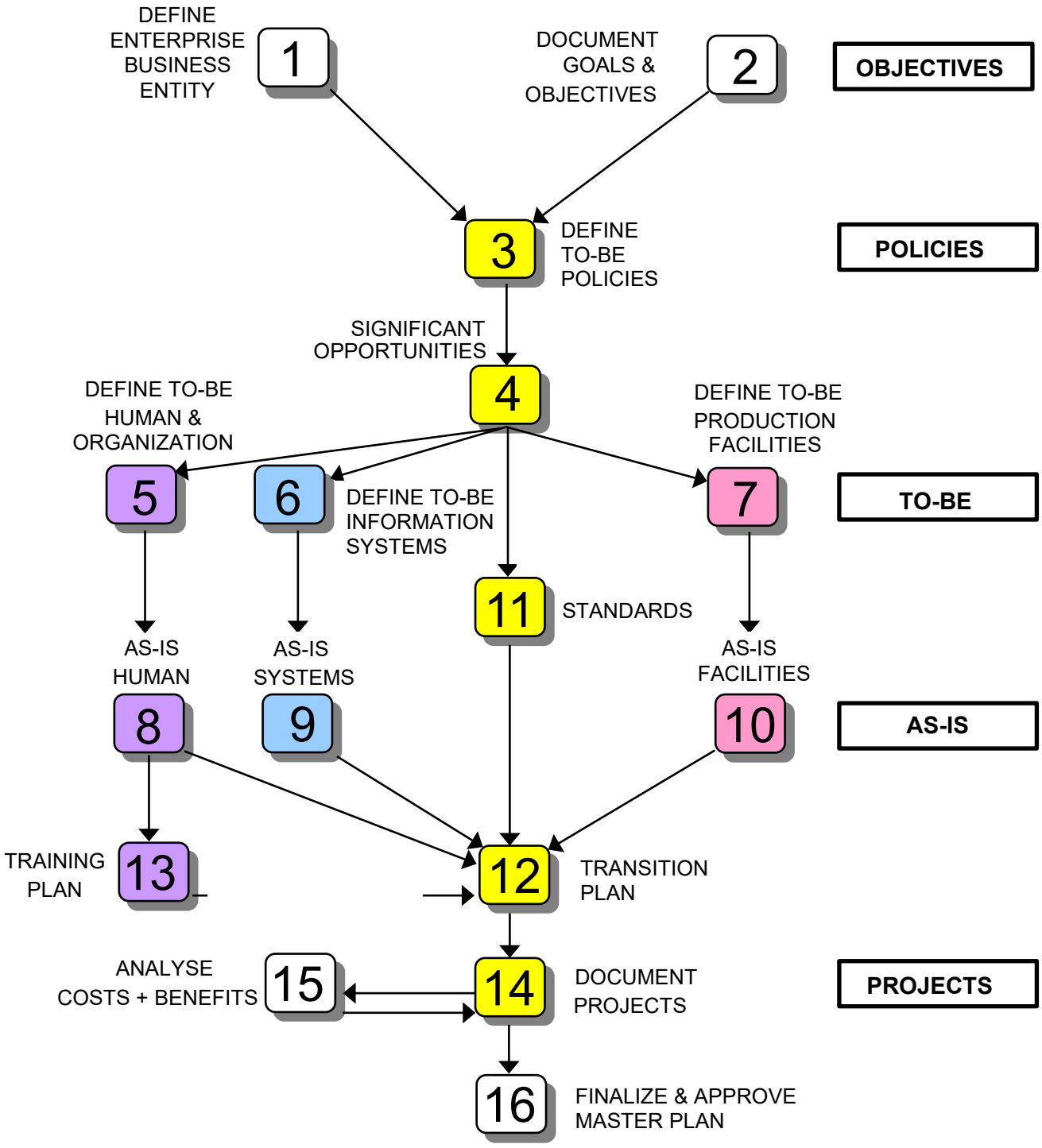
For more detailed information on Master Planning, you may view the *Introduction and Executive Summary* (61 pages) of the PERA Handbook on Master Planning for Enterprise Integration. Links to individual chapters of the Handbook are provided in the Resources section at the end of each Step below.

A Master Plan Report template may be downloaded here. This includes Introduction and Executive Summary sections as well as templates for Table of Contents and other materials to speed production of the Master Plan Report. The draft report contains 19 Sections that exactly correspond to the Steps described in this User Guide and in the PERA Handbook of Master Planning. Report Templates are provided for each Step (see below).

Step-by-Step Summary

The following diagram shows the steps involved in preparing, approving and implementing a Master Plan. Step numbers refer to Chapters in the PERA Master Planning Handbook.

PERA MASTER PLANNING WORKFLOW



Steps 1 and 2 - gather data from senior personnel and define their Objectives. Document input using carefully compiled forms and questions.

Steps 3 - document company Policies. These Policies will be followed without further investigation or consideration of alternatives. As such, they will save both time and money.

Step 4 – Identify Opportunities including approximate costs, Professional Roles, Phase when human and financial resources begin.

Steps 5 to 10 – Document the To-Be and As-Is People, Facilities, and Systems for each Opportunity. The next steps are built on the list of Opportunities that were defined in Step 4.
It is important to recognize that the human skills, experience, and certifications defined in Step 5 will be "generic skills" while the As-Is will be Positions in the organization. It may be necessary to convert Organizational Positions to the Generic Professional Roles they contain, in order to calculate differences in manpower, but for new Opportunities it is not.
Approximate costs and benefits are assessed for each "to-Be" Opportunity. Opportunities that are obviously not cost-effective or against company polices may be eliminated at this stage. However, those that remain will be analyzed more carefully in step 15.
Note that the To-Be condition is shown before the As-Is. This is recommended since many of the As-is aspects may be eliminated. In this case, assessing the As-is situation in detail would not be productive. That said, in real-world master plans, management often insists on an "As-is audit" as the first stage of the study, In practice then, for a given Opportunity, the As-is and To-be are often documented in parallel.

Step 11 – Standards are considered in parallel with the To-be and As-is assessments for People, Facilities and Systems. This is a two-step process. First the most relevant industry standards or government regulations are selected. Second the "requirements" from these standards are reviewed and either accepted or rejected. If accepted, these requirements will be included in the Company Policies and Practices. These will in turn influence the Opportunities that are included in the To-Be Human, Facilities, and Systems.

Step 12 – A Transition Plan.is developed to transform the As-Is People, Facilities and Systems to the To-Be Conditions. Generic Professional Roles associated with the selected Opportunities are assigned to the To-Be Org. Chart Positions. Each Opportunity includes earliest dates for resources including people, systems and facilities. Each Opportunity includes any training requirements.

Step 13 - Training plans are determined from As-is and To-be human requirements. These are added to the Transition Plan (Step 12) in terms of the To-Be Organization Chart..

Step 14 – Opportunities are usually combined into a set of Implementation Projects. A project to upgrade communication networks may not be cost-effective in itself; however it may make possible implementation of several other Opportunities. Similarly, a training program may be needed to upgrade skills in order to maintain several other Opportunities.

Step 15 – Once the set of Implementation Projects is identified, it is possible to do a much more useful economic analysis of costs and benefits than was possible with individual Opportunities.

Step 16 – Finalize and approve the Master Plan.

The following sections describe Steps 1 through 16 in more detail. It should be noted that each of these steps may vary with the industry involved. Terminology, drawings, documentation, practices, standards, and other aspects will be expressed in terms that practitioners in that industry will recognize.

Resources

For additional detailed information on creating the Executive Summary of the Cybersecurity Master Plan, view the Executive Summary section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A Master Plan template may be downloaded that includes Introduction and Executive Summary section as well as templates for Table of Contents, title page, Appendices, etc. Examples of Executive summaries from similar past Master Planning Reports may be available on request.

Step 1 - Define Enterprise Business Entity

In this first step, the **Enterprise Entities** involved are documented (e.g. the organizational and geographic entities where business will be done).

Then the business leaders of the enterprise are interviewed. For new enterprises this may be the project's Program Directors and/or the Corporate Sponsor if these are identified at that point in time. If the enterprise is existing, interviews may include the CEO, CIO, CTO, and Directors of Production, Finance, HR and Sales/Marketing.

After the senior management are interviewed, interviews will be continued with key Enterprise staff. For existing enterprises it is particularly important to include those with actual operations responsibility. A series of interview forms are provided (see the PERA Workbench) which address key aspects of the Enterprise (including facilities, people and systems). Touring existing facilities or studying available technology (possibly including site visits) may also be necessary. There may also be a value to holding "Town Hall" meetings, computerized surveys, and other mechanisms for getting input on the As-Is and To-Be facilities, systems, and human organizations.

Forms may be completed in hard copy, or as computerized surveys (which are easier to analyze). Survey forms will be completed by people who have "Roles" which correspond to specific Functions and Sub-Functions (see "Professional Roles" listing, and assignment of Roles to organizational "Positions" on the PERA website. Each form will contain either "assessments" for existing systems, or "anticipated value" for proposed new systems. See PERA Workbench for example survey forms.

Resources

For additional detailed information on defining the Business Entity, view the Step 1 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this Step 1 section. This may be added to the Table of Contents, Introduction, and Executive Summary Template (see above) to speed creation of a draft report.

Step 2 – Define Objectives, Strategies, Goals, Business Plan & KPIs

After approval of the information developed in the previous step, the high-level **objectives**, and the **Strategies** to achieve those objectives are identified. This may take the form of a hierarchy of key components such as the following:

Mission - (why the organization exists and what it contributes to the world)
| **Vision** - (What an organization aspires to in the future)
| **Values** - (Beliefs and principles that guide the organization's behavior)
| **Objectives** - (that are measurable, achievable, relevant, & timely)
| **Strategies** - (high-level plans to achieve these objectives)
| **Goals** - (specific targets that contribute to these objectives)
| **KPI's** - (Key Performance Indicators that are regularly measured)

Different enterprises may have very different mission, vision, values, and objectives. However, most will have basic objectives such as "minimum rate of return on investments (ROI), or acceptable risk (usually expressed in measures such as $ of loss per year).

The business Plan for each Enterprise Entity may also contain Goals that should be included, and these may be measured using Key Performance Indicators (KPIs).

These KPIs must be expressed in quantifiable terms and will be used as ongoing measures of whether the Enterprise is achieving the stated Objectives. In many cases, these KPIs form the basis for rewarding personnel at multiple levels and may even be reported in the company's annual report.

Objectives

The number of ACS cyber-attacks, and the financial impact of these attacks, are increasing rapidly. Average losses associated with each attack are reaching tens and even hundreds of millions of dollars, particularly in "infrastructure industries" like power generation and distribution, oil and gas processing, petrochemicals, and pipelines. This is increasing the urgency for corporations to establish ACS Cybersecurity Programs to address these risks.

Using ISA/IEC 62443 and the ACS Cybersecurity planning process, companies can apply their existing Control and Automation expertise, rather than hiring new staff, or training consultants on the operation of their facilities. This is increasingly important, as studies have indicated that over 1.5 million cybersecurity jobs remain unfilled in 2021, and that this is likely to increase in 2022.

Resources

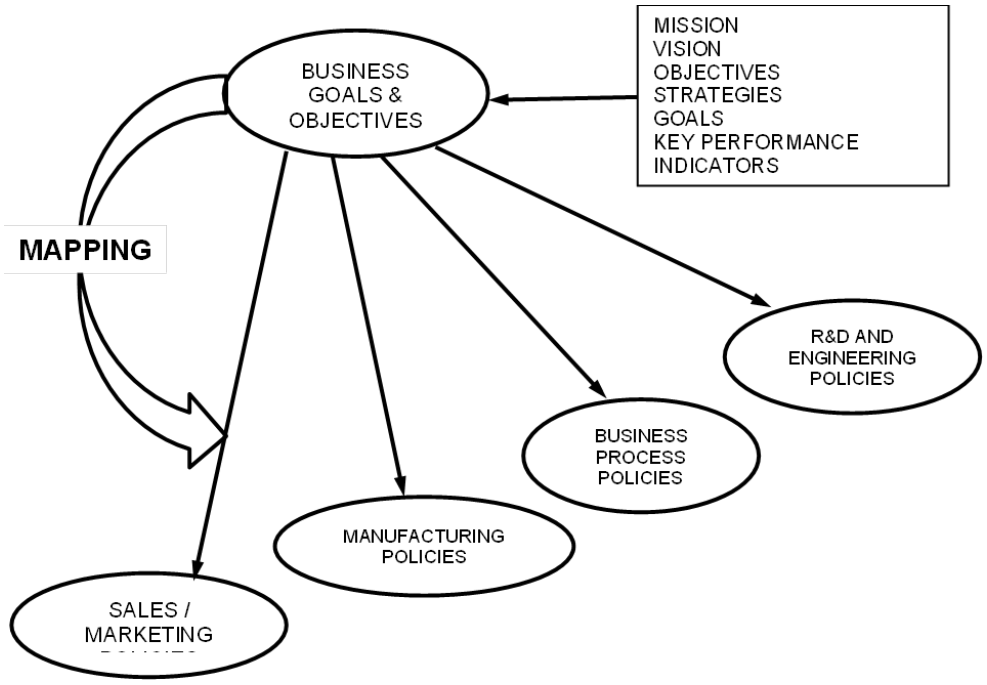
For additional detailed information on defining the Business Objectives, view the Step 2 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, Introduction, and Executive Summary Template (see above) to speed creation of a draft report.

Step 3 - Define "To–Be" Policies

After approval of the information gathered in the previous two Steps, relevant **Policies** of the Enterprise are established. Policies are enduring decisions made by management that must be followed by the Enterprise. These may be relevant existing Policies, or new ones developed as part of the Enterprise Master Plan. These Policies will be applied without further examination. As such, they focus the study and avoid evaluation of alternatives that are not acceptable.

Policies are typically implemented by area, such as Manufacturing, Sales/Marketing, IT, Business Processes, Engineering Policies, and others. A single set of Business Objectives and Goals may result in several sets of Policies, as shown below.



These policies may impact facilities, control & information systems, and human aspects of the enterprise. For example, a corporate IT policy such as use of a standard accounting system, will have consequences for computer hardware and networks, training and even corporate organization. It may also influence facilities such as backup power supplies, air conditioning, badge readers, fire and flood protection, etc. The degree of centralization and, thereby, communications that the selected system uses will also influence physical and cyber security requirements.

This is also true of ACS Policies, such as using company-standard DCS, PLC, and SCADA architectures and products. Such Automation and Control Systems (ACS) and cybersecurity policies can dramatically simplify integration, maintenance, and training.

Thus, it is particularly important for the Master Plan to establish compatible IT, OT, and ACS architectural policies

Resources

For additional detailed information on defining To-Be Policies, view the Step 3 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

s.

Step 4 - Define & Document Significant Opportunities

Selection of Opportunities begins with the current Enterprise "scope" for new Enterprises, or existing scope for current ones. It then identifies ways to improve this Enterprise.

This list typically includes 20 to 30 Opportunities (dependent on the nature and size of the enterprise). The largest Master Plan I know of involved 81 Opportunities (see below), while the smallest had only 12. This large Oil Pipeline Master Planning Study required many man-months, while the smallest was completed in 1 month by 3 people.

No.	Opportunity	Costs KUS$	Benefits KUS$	Phase (in which to start)
7	Secure Industrial and IT Network Standards, including design, procurement, & maintenance	20	30	Conceptual Engineering
8	Facility Physical Security Equipment & Systems	100	100	Detail Design
12	Cybersecurity Project Control & Change Management	10	20	Pre-Filing
14	Cybersecurity Tabletop Studies	20	50	Detail Design
18	PLC and Smart Instrument Programming Standards and Configuration System	500	3000	Detail Design + Operations
27	Plant ACS and IT Network Monitoring	200	500	Detail Design Phase
28	Secure Engineering Network	100	400	Detail Design Phase
30	Emergency Response System (including Cyber)	500	500	Detail Design Phase
67	Standardize Enterprise Systems Interfaces, including ACS, OT, IT, IoT and IIoT	2500	2500	Preliminary Engineering
70	Security Monitoring for Construction Phase	500	1000	Preliminary Engineering
71	Asset Inventory Import from EPCs	200	400	Preliminary Engineering
82	Learning Management System, including training modules for selected devices and systems	100	200	Operations Phase
83	Training manhours for selected devices and systems	100	400	Operations Phase
84	Annual KPI & Cybersecurity Program Evaluation	10	20	Operations Phase
85	Secure remote maintenance & technical support facility	50	100	Operations Phase

Each Opportunity will relate to one or more of the 3 PERA components (Facilities, People and Systems) and these will first be documented as part of each Opportunity, and then combined into an overall view of Enterprise Facilities, People and Systems in the final Master Plan.

At this stage in the study, the costs and benefits of each Opportunity are limited to "factored estimates" such as dollars per installed user, or operating costs per year. A more detailed evaluation of each of the Opportunities identified is done in Step 15 when additional "As-Is" and "To- Be" information is available.

The end of Step 4 marks the completion of the "first pass" of information gathering. Until this point, Facilities, Systems and Human and organizational factors are treated together. However, in Steps 5 through 10 the additional detail considered makes it necessary to separately document "To-Be" and "As-Is" for Facilities, Systems and Human Factors as shown in the following diagram.

It should be noted, that in Steps 5 to 10, the To-be condition is defined first, and the As-is

second. This is recommended since many of the As-is aspects may eventually be eliminated. In this case, assessing the As-is situation in detail would not be productive.

That said, it should also be noted, that in real-world master plans, management often insists on an "As-is audit" as the first stage of the study. It is also true that some assessment of As-is is required for Step 12 (the Transition Plan). In practice then, for a given Opportunity, the As-is and To-be are often documented in parallel, perhaps also including part of the Transition plan.

As shown above, the selection and application of Standards (Step 11), is also done in parallel with the To-be and As-is assessments. It is important to recognize that the human skills, experience ,and certifications required by Standards (Step 11) or Control and Information Systems (Step 7) will be "generic skills". These will only be assigned to Organization Chart positions later as part of the Transition Plan (Step 12).

The following sections describe Steps 5 through 18 in more detail. It should be noted that the description of each of these steps will vary with the industry involved. Terminology, drawings, documentation, practices, standards, and many other aspects have been expressed in terms that practitioners in that industry will recognize. These "industry-specific Master Planning Guides are intended to provide a "Go-by" that other enterprises in that industry may use (and further develop).

Resources

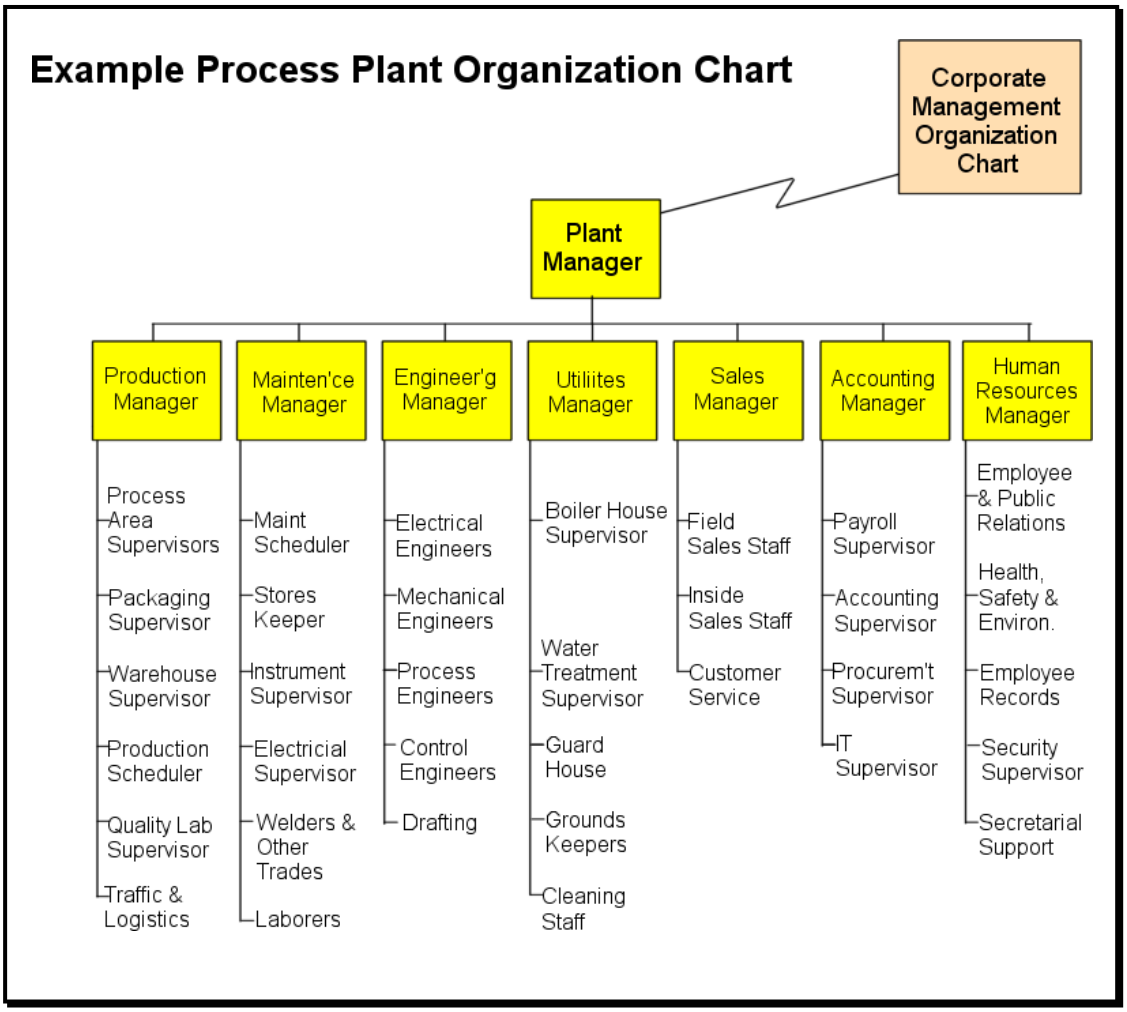
For additional detailed information on defining To-Be Policies, view the Step 4 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

.

Step 5 – Define "To-Be" Human and Organizational Architecture

The "To-Be" Human Architecture will typically include conceptual-level organization charts for each phase of the Enterprise (beginning with Conceptual Engineering and progressing through each PERA enterprise phase to Operations). These organization charts may be linked to provide an "Organizational Architecture for the Enterprise.



Generic Professional Roles are then assigned to "positions" in each Organization Chart. Note that standards or educational bodies can only define requirements for generic professional roles, however part of the Master Plan is to assign these generic roles to positions in the Enterprise Organization charts. Any position (shown above) may be assigned one or more generic professional role.

For this Cybersecurity Master Plan, the following subset of Professional Roles were considered relevant. Generic Professional Roles may be assigned to specific Opportunities.

770	**Control and Information Systems**
771	Instrumentation Design
772	Metrology
773	SCADA Systems
774	Analyzers and Sampling Systems
775	Tele-mechanization
776	Process Fire Protection
779	Industrial Telecom Engineering
780	**Industrial Computer Systems**
781	Production Management Systems
782	Maintenance Management Systems
783	Production Quality Management Systems
784	Health Safety & Environment Systems
789	Industrial Telecom Engineering

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 5 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 6 - Define "To-Be" Physical Facilities

ISA/IEC 62443 provides a powerful tool to reduce the risk of financial, reputational, human, and environmental impact from cyber-attacks on Automation and Control Systems (ACS). However, since it is a "horizontal standard", 62443 is meant to address a wide range of industries, and any specific company is likely to find that while most of the standard applies to their ACS, parts of it may not. For example, some "normative requirements" that are appropriate for an interstate pipeline, may not be relevant to a chemical plant or a discrete manufacturing facility. There are also obvious differences between a large-scale corporation with many sites and thousands of employees, and a small company with a few dozen staff. It is therefore recommended that each company establishes their own Automation and Control Systems (ACS) Cybersecurity Program to manage these cybersecurity risks. ISA/IEC 62443 2-1 provides guidance on how to establish a Security Program for ACS asset owners. This process might look like the following.

The "To-Be" Enterprise Facilities describe the Physical Production Facilities required to deliver the enterprise's products and services. Depending on the industry involved, these facilities may be documented with various standard documents such as the following.

DOCUMENT TYPE	DOCUMENT NAME	PHASE FIRST PRODUCED
Corporate Standard Block Diagrams	such as Process Flow Diagrams showing main equipment and piping, or Mechanical Flow Diagrams showing main areas and equipment.	Corporate Master Planning
Schematic Diagrams	such as Site Plans, Electrical Hazardous Area Classifications, Radio signal propagation maps, Major cableways, power distribution, and switch yards	Corporate Master Planning
3D Models and Diagrams	such as Facility Layouts, and initial 3D models	Corporate Master Planning

The physical layout of the production equipment and the control and information system centers are fundamental to risk management including:

i. area protection (e.g. blast radius separation)
ii. fire protection
iii. hazardous gas detection
iv. physical perimeter security
v. cybersecurity (equipment and communications physical access).

Resources

For additional detailed information on defining the To-Be Physical Architecture, view the Step 6 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

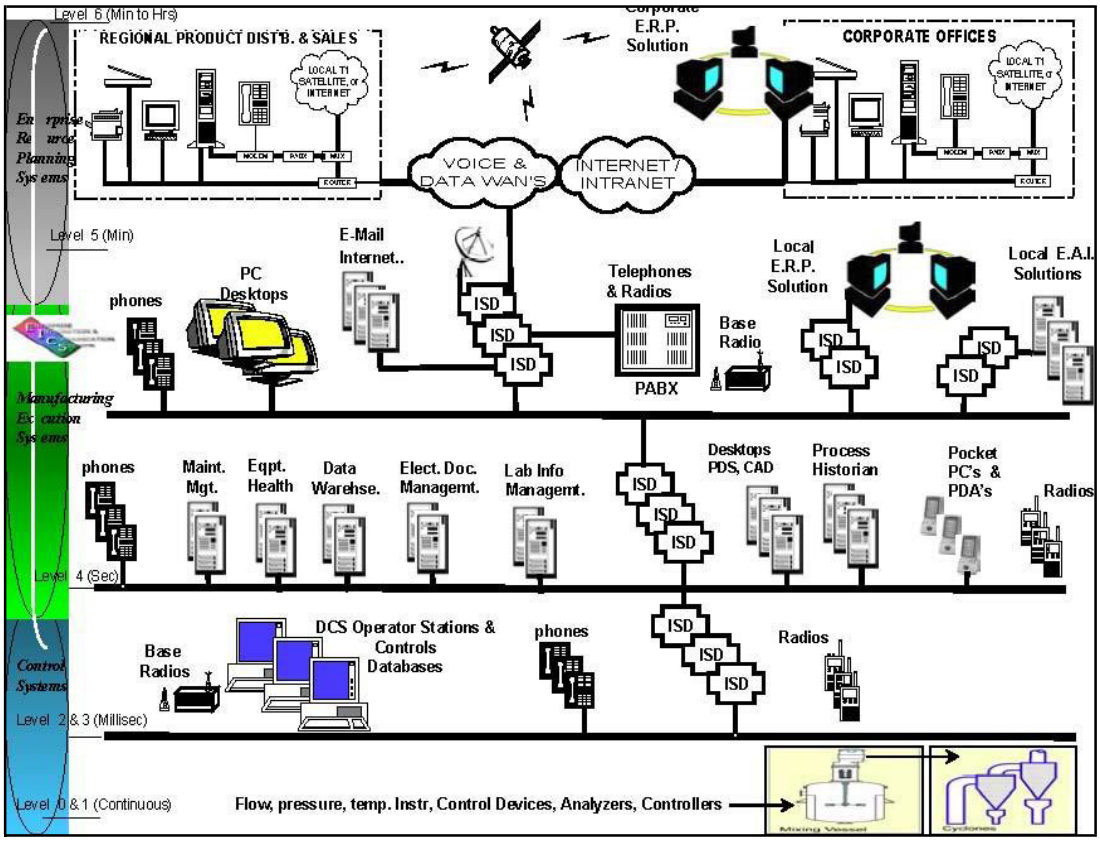
A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 7 - Define "To-Be" Control & Information Systems Architecture

At this stage, overview diagrams of the Control and Information Systems are prepared, including;

- A **Physical Network Architecture Diagram** showing the principal LANs, WANs, Servers, and groups of end-user computers.
- A **Logical Systems Architecture Diagram** showing Major Systems and information flows between systems.

Physical Network Architecture Diagram



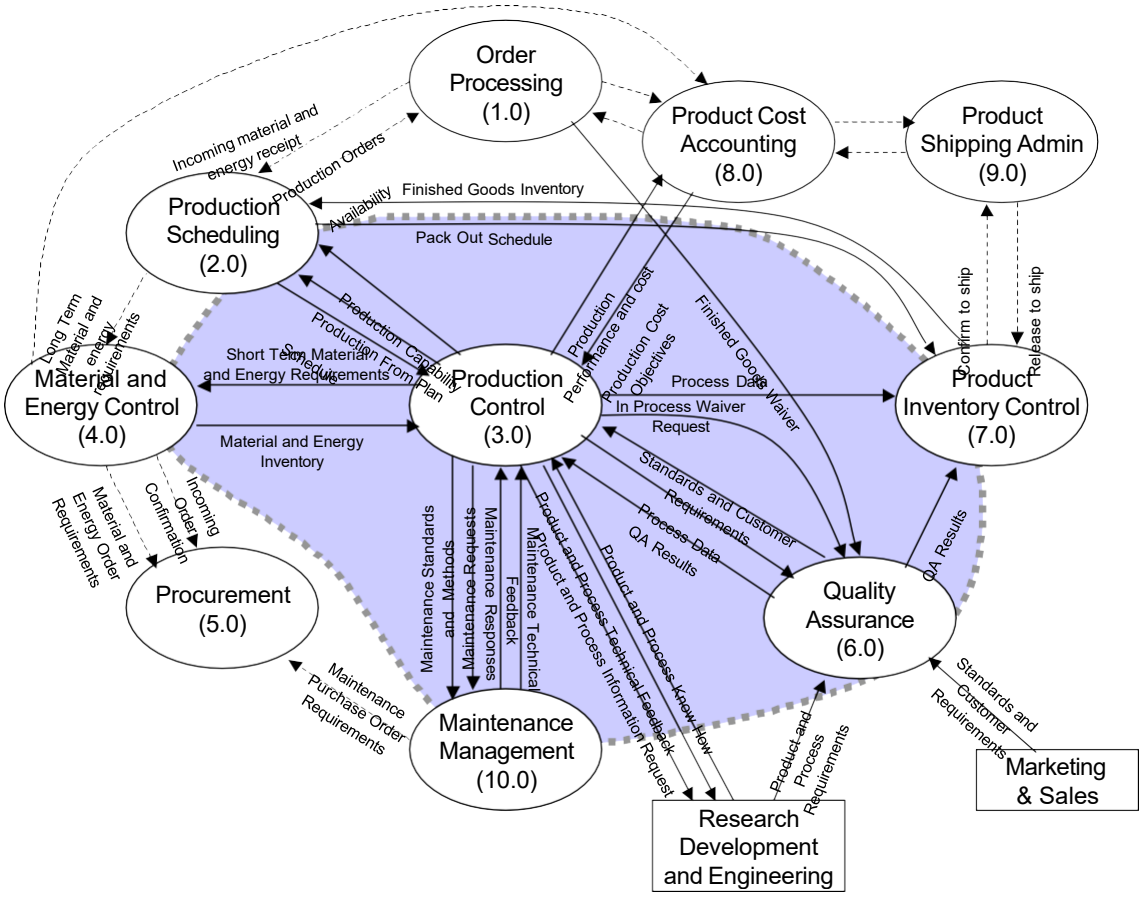
Source: Fluor Daniel EICS Group

This Physical Network Architecture Diagram shows the sensing, actuators, computing, and network devices and how they are connected. By convention, networks are shown as horizontal buses, and devices are connected to them at the appropriate "Level" in the physical architecture. All connections between levels are "controlled" by a gateway, router, firewall, or other "managed" device.

Rules for the design of the Physical Architecture are determined during the Enterprise Master Plan. PERA suggests this by done according to the "4Rs" (Response, Resolution, Reliability, and Reparability) that is required of that equipment.

This example is of a process industry enterprise with 4 network levels. However, as the "PERA Reference Model for CIM" describes, different industries may have different network levels and design rules. What is important is that these levels and rules are established for the enterprise as "Policies" that are consistently applied across the enterprise.

Logical Network Architecture Diagram



Source: Purdue Reference Model (see also ISA-95)

The ISA95 Logical System Model identifies 12 main enterprise functions between which information is exchanged (see the arrows above). The colored area represents the Manufacturing Execution Systems area (MES).

By splitting each function into sub-functions (with associated information flows) and even sub-sub functions, all activities within the enterprise can be described. According to the Opportunity being considered, the Logical Architecture may be represented with more or less detail.

For in-depth analysis of high-value Opportunities, additional Business Process Modeling (BPM) may be done using Work Process Modeling tools such as ARIS, NetWeaver, etc. These tools can be used to clarify the functions and information flows for major systems, particularly as many now incorporate the ISA-95 Reference Model as part of their packages.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 7 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

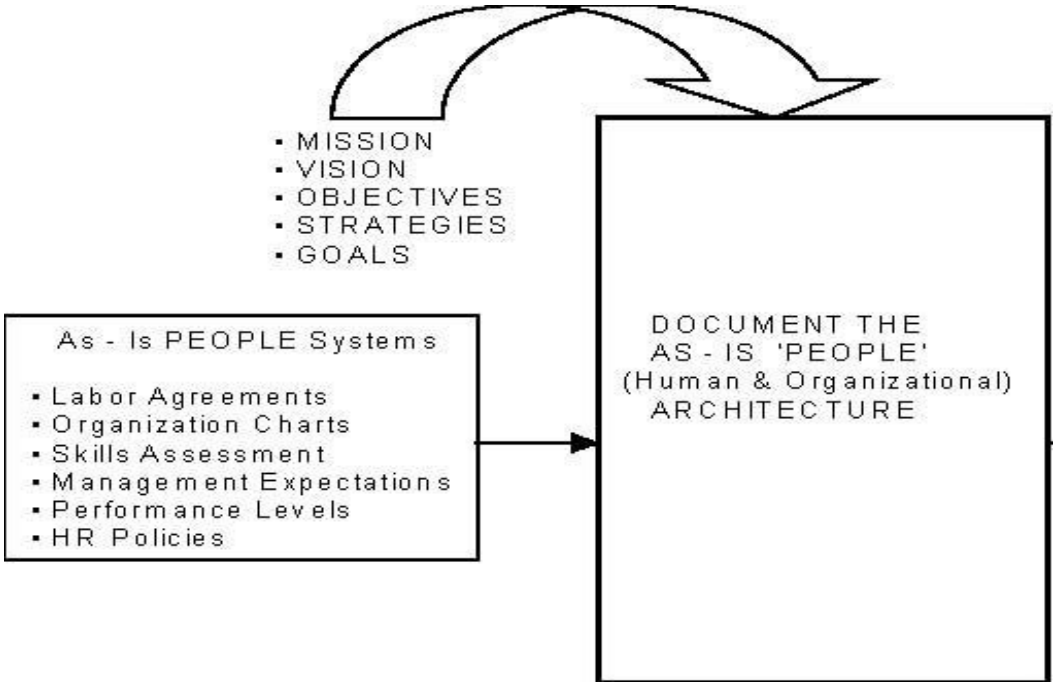
A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 8 - Define 'As-Is' Human & Organizational Architecture

For an existing enterprise, the organization charts and position descriptions are assembled to establish an As-is "baseline".

For new organizations, the Organization Chart will be assumed to transition from the Project Organization. Position descriptions for the Operating Phase may be created "from scratch" or based on similar facilities.

From this baseline, analysis of staff and training costs required to implement To-Be systems, benefits, and other factors can be estimated. The transition costs and schedule can then be determined later in Step 12 (Transition).



Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 8 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

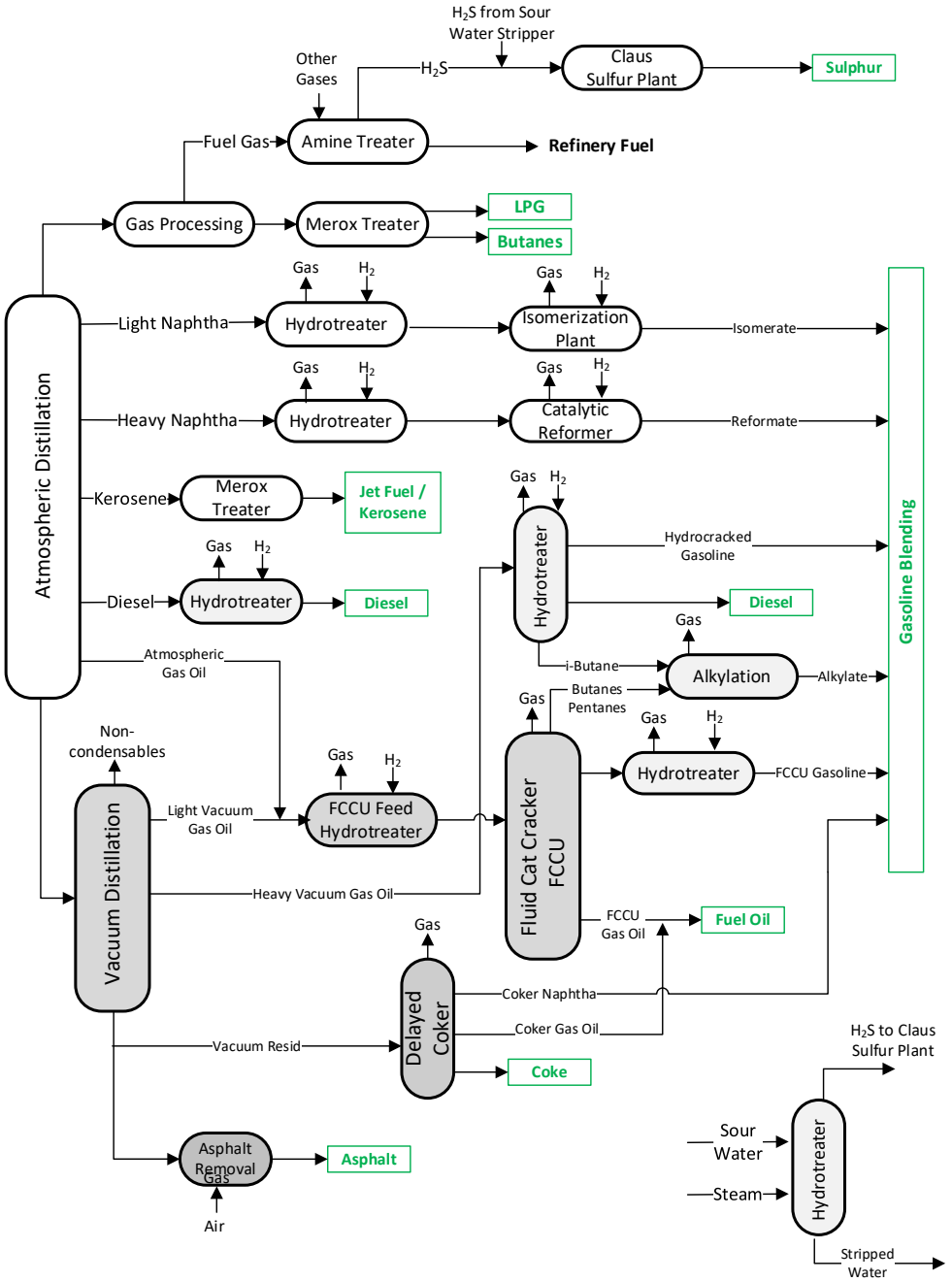
A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 9 - Define "AS-IS" Facilities Architecture

As in Step 9, what is desired is an "AS-IS" snapshot of the existing Enterprise Facilities and their effectiveness in serving the objectives of the Enterprise. To the extent feasible, this should be documented in a manner which is consistent with the "To-Be" Facilities to facilitate comparison and assessment of the Transition Plan.

Some Enterprises are compact and exist primarily on a single physical site. Others, like a pipeline or a mining and metallurgical enterprise, may have physical locations separated by hundreds of miles. This has a profound effect on communications infrastructure, physical and cyber security and even human architecture.

REFINERY PHYSICAL FACILITIES ARCHITECTURE



Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 9 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 10 - Define “As-Is” Control & Information Systems Architecture

Almost all Industrial Enterprises and their Control and Information systems are under more or less continuous change. What is necessary therefore, is a “snapshot” of the existing systems. Ideally these should be converted to the same format as the To-Be Systems, however this may not always be practical.

It is also desirable to assess the effectiveness of the existing systems in serving the Objectives of the Enterprise, with particular
care to document perceived shortcomings.

User Survey Forms including most of the common Enterprise Systems, MES, and Control Systems is provided on the PERA Workbench. This assessment will later be compared (in Step 12, Transition Plan) with the “To-Be” state, and will be used to assess the benefits of the proposed To-Be Systems.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 10 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 11 - Standards Selection

The selection and use of standards in Enterprise Integration is a complex subject for at least the following reasons:

1) Enterprise Integration addresses all levels of the enterprise architecture, from plant control and data acquisition to corporate reporting systems. As a result, standards that may be relevant range from ACS (automation and control systems) standards like ISA 62443 at the plant level to IT standards like ISO 27001 at the corporate level.

2) National and industry standards such as NIST 800 (US standard) or the NAMUR set of standards (European process industry

3) Other technical standards may be relevant such as ISA 5.1 (Graphic Symbols) or 12.1 (Alarm Management)

ISA/IEC 62443 describes how cyber secure Control and MES networks should be designed, implemented, and maintained. It provides normative requirements and guidance documents for Automation and Control Systems.(ACS).

Series Part	Title	Description
62443-1-1	Security for industrial automation and control systems – Part 1-1: Terminology, concepts and models	Introduces the concepts and models used throughout the series.
62443-1-5	Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 security profiles	Specifies a scheme for defining (selecting, writing, drafting, creating) IEC 62443 security profiles.
62443-2-1	Security for industrial automation and control systems – Part 2-1: Security program requirements for asset owners	Defines the requirements and provides guidance to develop an automation and control system security program for asset owners.
62443-2-3	Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment	Describes a format for the exchange of information about the status of patches and their applicability and provides guidance on planning and building a patch management program within asset owner, service provider, and product supplier organizations.
62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers	Contains security requirements for providers of integration service including commissioning activities, and maintenance service for ACS.
62443-3-1	Security for industrial automation and control systems – Part 3-1: Part 3-1: Security Technologies for Industrial automation and control systems	Surveys and provides an evaluation and assessment of many current types of electronic- based cyber security technologies that may apply to protecting an ACS environment from detrimental cyber intrusions and attacks.
62443-3-2	Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design	Describes the activities required to perform security risk assessments on a new or existing ACS and the design activities required to mitigate the risk to tolerable levels.
62443-3-3	Security for industrial automation and control systems – Part 3-3: System security requirements and security levels	Describes the technical security requirements for systems related to the seven foundational requirements defined in ISA 62443-1-1 and assigns system security levels (SLs) to the equipment under control.

62443-4-1	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	Describes product development lifecycle requirements related to cyber security for products (i.e., components and systems) intended for use in the ACS and provides guidance on how to meet the requirements described for each element.
62443-4-2	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components	Describes the technical security requirements for the components that are used to build automation and control systems. These requirements are derived from the system requirements for ACS defined in ISA 62443-3-3, and as such, assigns component SLs based on the system security levels
62443-6-1	Security for industrial automation and control systems – Part 6-1: Security evaluation methodology for IEC 62443-2-4	Specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443 - 2-4 requirements.
62443-6-2	Security evaluation methodology for IEC 62443 - Part 4-2: Technical security requirements for IACS components	Specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443 - 4-2 requirements.

Source: ISA-62443-1-1 Security for industrial automation and control systems – Part 1-1 Terminology, concepts and models.

- ISO 27000 series describes how cybersecure IT systems should be designed, implemented, and maintained. IT systems are defined as those that process information for presentation to humans but do not take independent actions on real-world equipment.
- NIST Special Publication (SP) 800 series presents information of interest to the computer security community. The series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities.to address and support the security and privacy needs of U.S. Federal Government information and information systems.

Comparison of NIST 800 vs 27001

https://www.linkedin.com/posts/lindatuckchapman_nist-iso-iso27001-activity-7308855581597962243-4y8O?utm_medium=ios_app&rcm=ACoAAAFOOYcBf-RbX8pnz-RrNGoXRfe_hh8iO2A&utm_source=social_share_send&utm_campaign=mail

The work process involved is:

a) Select appropriate standards

b) Organize Standards by Clause / Requirement

c) Edit or delete Requirements that do not apply for this Owner/Facility

d) Align Requirements and Recommendations from selected standards

Another example might be taken from a project to certify Vendor components to IEC/ISA 62443-4-1 where only part of the Requirements of this standard are required (those referring to components, but not those related to systems).

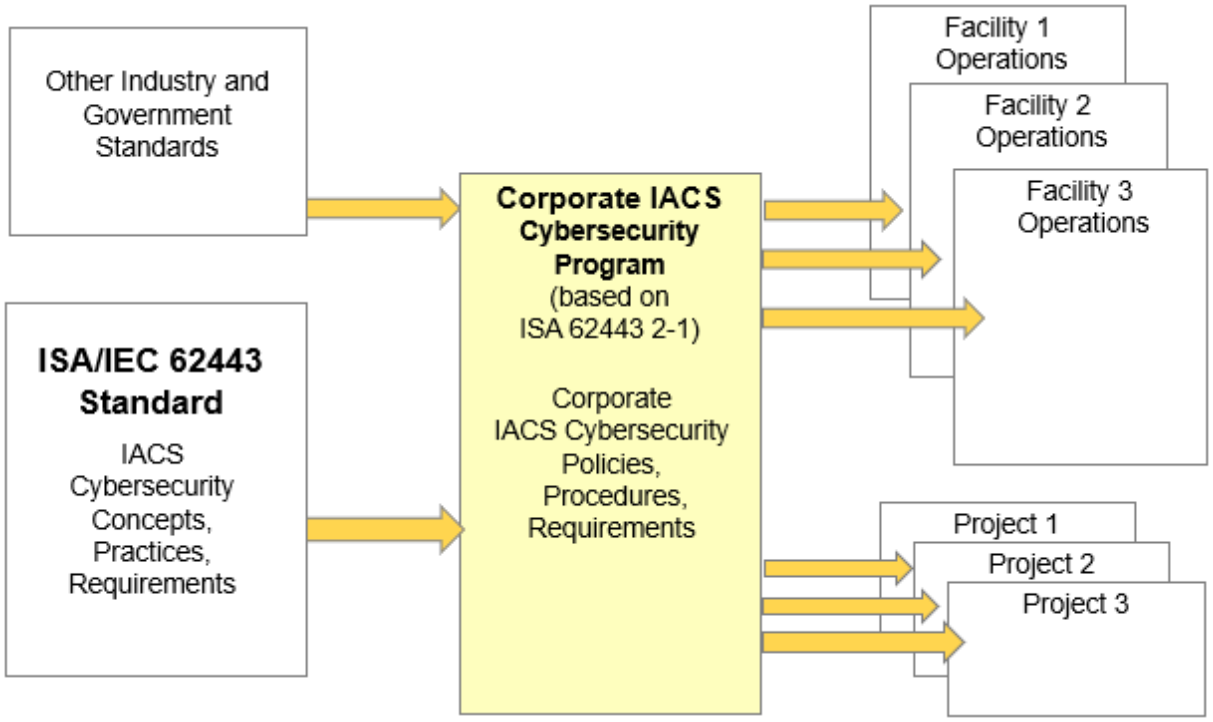


Figure 2 – ACS Cybersecurity Program Concept

As this diagram indicates, the ISA/IEC 62443 standard provides Concepts, Practices, and Requirements that may be included in a corporate ACS cybersecurity program. Note that a Corporate ACS Cybersecurity program is a necessary first step, however, the Policies, Procedures and Requirements defined in this program, must then be implemented within existing Corporate and Facility procedures if they are to be effective. This implementation should be undertaken as one or more projects, with stated schedules, scopes, and budgets; and must include training and management of change to address human and organizational aspects.

At present, the 62443 standard identifies hundreds of separate requirements that may be necessary for a given company's facilities. It is impractical to search through ISA/IEC 62443 to determine what is necessary for a given project or operating facility. A key objective of the ACS Cybersecurity Program is therefore to establish approved requirements that may then be incorporated in project or facility standards and procedures within the enterprise..

A corporate ACS cybersecurity program must select which ISA 62443 requirements to include for:

- A company's Existing Facilities
- New company projects that involve ACS

As shown in Figure 2, requirements and recommendations from other industry, national, and international standards, may also be considered for inclusion in the company's ACS Cybersecurity Program. Examples of these might include:

- ISA standards such as:
  - ISA84 (safety instrumented systems),
  - ISA95 (enterprise integration),
  - ISA100 (Industrial wireless networks), and
  - ISA108 (intelligent device configuration)

Note: Since ISA standards are internally "harmonized", use of these together with ISA/IEC 62443 may save considerable time and effort for the Owner/Operator.

- Additional cybersecurity standards and guidelines from NIST, NAMUR, ISO, IEC, and others
- Standards and guidelines for human factors, risk analysis and risk mitigation.

Many of the above have been aligned with ISA/IEC 62443, including cross-reference documents and other whitepapers.
Examples of government standards include regulations and legislation at national, state, and local levels. These must also be considered when creating the Corporate ACS Cybersecurity Program.
ISA is currently active at US Federal, State, and local government levels, to gain acceptance and standardization of regulations based on ISA/IEC 62443. ISA is also participating in programs to promote use of ISA/IEC 62443 in multiple countries around the world.

How does ACS Cybersecurity relate to IT Cybersecurity?

Many corporations already have a corporate position responsible for cybersecurity of information. This position typically resides in the corporate IT (Information Technology) department. The most widely used standards for IT cybersecurity are the ISO 27000 series and selected guidelines from NIST.
Although not yet as common, many corporations are establishing a corporate role that is responsible for OT (Operations Technology) cybersecurity. While IT Cybersecurity is responsible for Information Cybersecurity, OT Cybersecurity is responsible for cybersecurity of ACS. ISA/IEC 62443 is widely accepted as the leading standard for ACS cybersecurity, much as ISO 27000 series is for Information Cybersecurity.
Thus, ISA/IEC 62443 and ISO 27000 are, in effect, "parallel" standards, as shown in the diagram below.

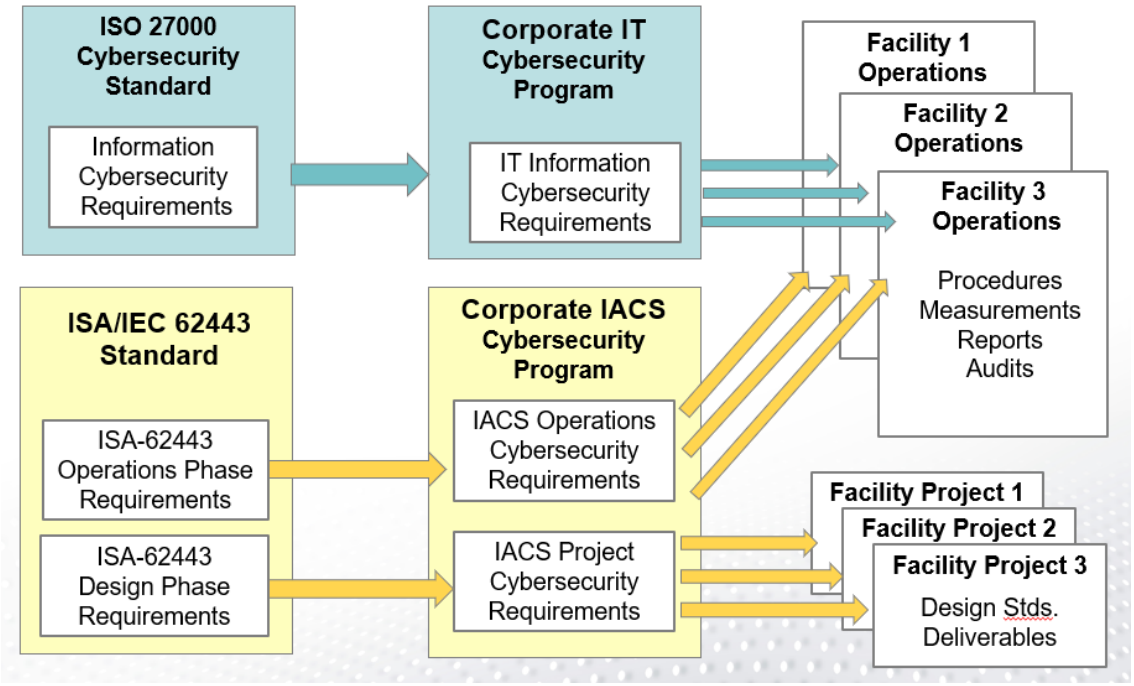


Figure 5 – Mapping of Cybersecurity Requirements

The distinction between where ISA/IEC 62443 and ISO 27000 are applied is indicated in this diagram.

A Corporate ACS Cybersecurity Program (yellow) will contain Requirements for all enterprise phases of corporate facilities including project design phase and operations

phase. These may include project deliverables such as design documentation and drawings (lower right in this diagram), or Operations deliverables such as Operations measurements (e.g., KPIs), incident reports, etc. (upper right in this diagram).

It should be noted that the security of IT information is focused on Operations phase at plants and corporate offices (blue arrows above). Although company information security objectives during project execution may be specified by the Owner, the actual security of information on projects is normally the responsibility of the Integrator, equipment supplier, or engineering contractor.

Typically, information security for ACS in plants (as an addition to equipment operating safety) should be managed by those responsible for the ACS Cybersecurity Program. However, company standards for security of this Information should be provided by the Corporate IT Information security program.
Once areas of responsibility for plant control and automation are agreed in the ACS Cybersecurity Program, the standards to be used for safety and security of ACS systems will be selected and documented (see Step 11 in the PERA Planning Diagram).
Finally, the corporate ACS cybersecurity program, and the corporate IT cybersecurity program, should be aligned, as they provide complementary parts of overall corporate cybersecurity.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 11 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 12 - Document Transition Plan From "AS-IS" To "TO-BE"

The transition plan identifies the best path to resolve the gaps between the "As-Is" condition and the "To-Be" state. This will involve the following activities:

Review the three "To-Be" architectures against the overall Enterprise plan.

- Determine the steps needed to migrate "As-Is" Facilities to the "To-Be" Facilities
    - Estimate the time and costs to accomplish this transition.
- Determine the steps needed to migrate "As-Is" Systems to the "To-Be" systems.
    - Estimate the time and costs to accomplish this transition.
- Determine the steps needed to migrate the "As-is" Human and Organizational to the "To-be" Human and Organization.
    - Estimate the time and cost to accomplish this transition

The "People" part of the transition plan is just as important as the systems or facilities transition plan. Unfortunately, the People aspects are often forgotten or left until too late, causing more failures than any other aspect.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 12 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 13 - Training Plan

Upgrading the technical capabilities, and skills needed to effectively use and maintain the To-Be" systems must be planned in parallel with the systems themselves. This includes developing the following:

- A list of required training programs, including conceptual content.
- Estimate of needed resources in space, equipment, personnel and capital.
- A conceptual level 'Skill Development' matrix relating the personnel and training programs.
- An overall Training Schedule

Training requirements are determined from As-is and To-be human and organizational requirements. These are added to the Transition Plan (Step 12).

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 13 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 14 – Document Proposed Projects

Opportunities (1 to 81) are organized into Projects (A to P) where organizational interfaces are minimized to improve project execution effectiveness and to simplify technical system interfaces. The Enterprise Phase where each Opportunity is started is also listed to help level manpower and transition plan and

Costs and Benefits of selected Opportunities are combined by Project.

Project List

No	Project	Phase in which to start this Project	Total Cost (K US$)	Costs (K US$)	Total Benefits (K US$)	Benefits (K US$)	Opportunity No.	Opportunity
A	**SCADA**	Preliminary Engineering	**12,000**	500	**37,000**	500	9	Custody Transfer System Automation
		Preliminary Engineering		9,000		25,000	24	Enhanced SCADA
		Preliminary Engineering		1,500		1,500	25	Leak Detection
		Detail Design		1,000		10,000	47	Pipeline Operator Training Simulator
B	**Pipeline Communications Backbone**	Operations & Maintenance	**181,150**	450	**181,700**	600	4	Share Backup with TAPS
		Preliminary Engineering		180,000		180,000	7	Pipeline Control Backbone
		Detail Design		300		300	48	Pipeline External Communications
		Operations & Maintenance		-		-	69	Sell Fiber Bandwidth
		Detail Design		400		800	75	Optimize Block Valve Building (120 to build)
C	**Pipeline Operating Systems**	Preliminary Engineering	**29,750**	1,000	**32,900**	2,000	5	Customer Management (Pipeline Scheduling) System
		Detail Design		1,050		3,000	11	Maintenance Management
		Detail Design		1,000		1,000	32	Corporate Management Information Interfaces
		Pre-Filing		1,500		1,500	55	Functional definition of production systems
		Preliminary Engineering		25,000		25,000	67	Enterprise Systems Interfaces
		Preliminary Engineering		200		400	71	Maintenance Data Imported From EPCs
D	**Engineering Support Systems**	Preliminary Engineering	**825**	100	**4,684**	1,000	1	Engineering Office Communications
		Pre-Filing		50		50	16	Client Deliverables Creation and Management
		Operations & Maintenance		500		3,000	18	PLC & Smart Instrument Standards
		Preliminary Engineering		100		400	28	Engineering Office Systems & Communication
		Pre-Filing		40		104	38	GIS Web Page
		Preliminary Engineering		35		130	46	Automated Alignment Sheet Generation
E	**Personal Productivity Infrastructure**	Construction	**556**	300	**1,594**	140	2	Standardize Personal Productivity Applications
		Pre-Filing		60		360	26	Remote Desktop Support
		Pre-Filing		40		80	29	Master Project Web Menu
		Preliminary Engineering		100		400	35	E-Mail Implementation
		Preliminary Engineering		11		110	50	Video Conferencing
		Preliminary Engineering		15		24	51	Manage Distribution & Contact Lists
		Preliminary Engineering		20		400	53	Scan and Store Admin Forms
		Preliminary Engineering		10		80	54	Instant Messaging
F	**Procurement and Logistics Support**	Preliminary Engineering	**3,947**	2,100	**26,303**	18,000	10	Warehousing and Material Control
		Detail Design		250		2,500	14	Logistics Modeling
		Detail Design		300		1,500	22	Material Tracking
		Preliminary Engineering		172		1,063	33	Procurement Document Management
		Preliminary Engineering		400		1,760	44	Vehicle Tracking
		Preliminary Engineering		700		1,400	66	Procurement Database and Work Process
		Preliminary Engineering		25		80	80	Local Contract Management
G	**Security, Safety, Health & Environment**	Detail Design	**2,380**	1,000	**3,616**	1,000	8	Pipeline Security Systems
		Detail Design		20		36	15	Waste Management Database
		Detail Design		140		580	23	Medivac and Remote Medical Support Services
		Detail Design		500		500	30	Emergency Response System
		Detail Design		220		500	43	Field Personnel Security Systems
		Preliminary Engineering		500		1,000	70	Security Monitoring for Construction Phase
H	**Project Controls Support**	Pre-Filing	**411**	11	**420**	20	12	Project Cost Control and Change Management
		Pre-Filing		100		100	60	Project Scheduling
		Pre-Filing		300		300	61	Project Cost Accounting
K	**Document Management**	Construction	**805**	580	**2,426**	1,556	3	Technical Document Management
		Pre-Filing		100		300	19	Quality Assurance Data Management
		Pre-Filing		40		400	34	Project Correspondence Management
		Pre-Filing		40		80	62	Commitment Management Database
		Pre-Filing		5		10	63	Provide repository for Codes & Standards
		Detail Design		40		80	81	Permit Management System
L	**Construction Support**	Detail Design	**982**	100	**1,852**	100	6	Construction Communications
		Detail Design		100		350	13	Provide Construction Contractor Communications
		Construction		100		380	17	Field Personnel System
		Pre-Filing		100		300	19	Quality Assurance Data Management
		Detail Design		42		42	31	Add Voice Channels to Data Links
		Detail Design		40		80	39	Construction Web Page
		Preliminary Engineering		-		100	72	Integration between Engineering & Construction
		Construction		500		500	78	Mobile SAT at Construction Spreads
P	**IT/Telecom Infrastructure**	Pre-Filing	**2,860**	60	**10,860**	360	26	Remote Desktop Support
		Detail Design		200		500	27	Network Monitoring
		Detail Design		2,600		10,000	76	Establish Hardware and System Software Standards
		Totals	**235,666**		**303,355**			
		Less Projects over	**(214,000)**		**(230,000)**			
		"Small Projects"	**21,666**		**73,355**			

We now combine the Opportunities developed in Step 4 (and their resulting "To-Be" architectures of Steps 5 to 7) with the Transition Plan defined in Step 12. The "To-Be" opportunities and the Transition from "As-Is" systems are organized into "Projects" so that the work can be planned, developed and implemented most efficiently.

The identification of the Projects is an iterative process with Step 15 (Analyze Costs, Benefits and Risks).

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 14 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 15 - Analyze Costs, Benefits and Risks

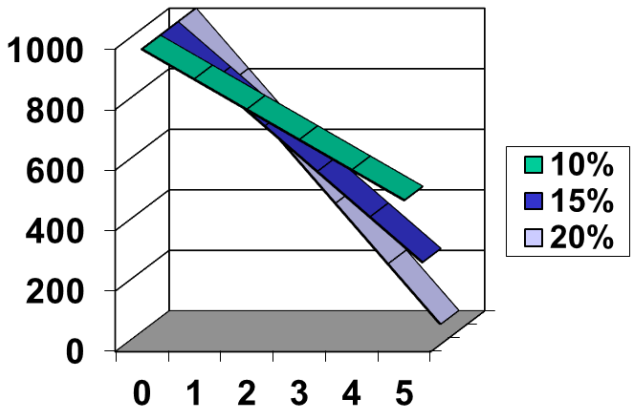
An ACS Cybersecurity Program should be assessed and budgeted like any other investment made by the corporation. Implementation of the proposed cybersecurity plan will be divided into a number of projects, each of which is individually justified, approved, and tracked (see Step 14 in the PERA Planning Diagram).

To facilitate this evaluation, cybersecurity risks will be assessed using accepted industry and company criteria. A series of measures will then be evaluated that may mitigate these risks, and the cost of these measures compared to the risk reduction benefits (see Step 15 in the PERA Planning Diagram).

As part of evaluation of the corporate ACS Cybersecurity Program, possible costs of ACS security breaches associated with the proposed ACS Cybersecurity Program will be assessed. Note that the likely cost of an ACS breach is typically much more than for an information breach, since in addition to the risk of data loss, actual physical plant operations may be impacted. Thus, loss of production, equipment damage, environmental damage, and injuries or death may result.

A cost/benefits analysis is prepared for each of the selected projects. The process is a cooperative iteration with Step 14 to agree on the benefits, cost-effectiveness, and priority levels of the projects. The projects are also evaluated in accordance with Enterprise Objectives, Strategies, Goals, and Critical Success Factors to ensure their implementation will support these criteria in an optimal way. Finally the technological impact and business risks for each project are assessed to further refine the priority for their implementation.

A Graph of payback vs cost of capital is typically generated for each project using a simple spreadsheet.



- "Simple Payback" is good enough for Cost/Benefit analysis at this Phase.
- "Straight Line" Benefits are counted for only 5 years since future value of benefits diminish rapidly.
- The project spreadsheet also shows the "Net Present Value" (NPV) of benefits received in Future Years.
- Annual maintenance cost is deducted from Benefits to get a "Net Benefit".
- Timing of Costs and Benefits may be examined for each Opportunity as shown here.

Case 1 - Investment all within 2004, Completed early during Year, so 80% of Benefits accrue during Year 1						
Item	**Start Year**	**Yr 1**	**Yr 2**	**Yr 3**	**Yr 4**	**Yr 5**
Costs, % of Total	2004	100%	0	0	0	0
Benefits, %/Year	2004	80%	100%	100%	100%	100%

These costs are in addition to the likely costs of information security breaches, including:

- Ransoms
- Lawsuits
- Penalties and fines
- Increased insurance premiums
- Loss of revenue do to reputational or brand damage.

Balanced against the risk of losses are the costs of mitigation measures, including staffing and training of Corporate and Plant Personnel.
Other benefits of the ACS Cybersecurity Program may be realized, including

- More efficient use of staff
- Insurance savings
- KPIs and employee awareness (eg., number of attacks vs penetrations, time from attack to detection)
- Benefits of improved asset tracking and ACS architecture documentation
- Improved IT/OT integration

The costs of a Cybersecurity Program must be assessed against the potential benefits, and this must be done using the same criteria as are used for other investments in the corporation.

It must also be recognized that as more mitigation measures are added, the possibility of failure of these mitigation measures also represents a risk. Recent cyber events such as the "Cloud Strike" disaster introduced enormous costs that resulted because the mitigation measures were over-centralized and propagated through thousands of systems worldwide. In effect, mimicking the effect of viruses

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 15 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

.

Step 16 – Final Critical Evaluation

Master Planning Team performs a final critical review of the draft Master Plan and of each chapter in turn, including its thoroughness, accuracy, and credibility.

Identify issues raised previously that have not been resolved and requiring further work before finalizing the Master Plan. This includes identifying and addressing anything that might not be implementable in this company at the present time and what additional work might be required.

This review is also intended to improve the understandability of the work for communication to other internal and external organizations involved.

Verify that there is a broad-based understanding and support for the proposed program within the Enterprise Business Entity and in upper company management.

Deliverables include:

1. Identification of all issues requiring additional work
2. Plan of action including assignment of personnel
3. Completion and approval of all outstanding issues including deletions where appropriate.
4. Formal “sign-off” by the Steering Committee to allow completion of remaining tasks and authoring Master Plan.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 16 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 17 – Author Master Plan

The Cybersecurity Master Plan **Report** will typically contain the following sections:

0. Executive Summary
1. Enterprise Business Entities
2. Goals / Objectives, KPIs
3. “To-Be” Enterprise Policies
4. Define and Document Significant Opportunities
5. “To-Be” Human and Organizational Systems
6. “To-Be” Control & Information Systems
7. “To-Be” Physical Facilities
8. “As-Is” Human and Organizational Systems
9. “As-Is” Control & Information Systems
10. “As-Is” Physical Facilities
11. Standards Selection (and Requirements identified from each)
12. Document Transition Plan from As-Is to To-Be
13. Training Plan
14. Document Proposed Projects
15. Analyze Costs, Benefits, and Risks
16. Final Critical Evaluation
17. Author Master Plan
18. Renew the Master Plan

The Champion will submit the Master Plan to a review board, that should include major stakeholders including representatives of:

- Plant Operations including Chief Operations Officer (COO)
- Capital Projects including CTO Chief Technical Officer (CTO)
- IT Operations including Chief Financial Officer (CFO), CIO,
- Control and Information Systems including Chief Technology Officer (CTO), and Chief Information Officer (CIO) and Chief Information Security Officer (CISO)
- Physical Plant Security including Chief Security Officer (CSO)
- Corporate Risk Management including Chief Executive Officer (CEO)
- Health, Safety and Environmental including Chief Executive Officer (CEO)

This review board will also receive monthly KPI reports and project progress reports

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 17 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Step 18 – Renew Cybersecurity Master Plan

After the Master Plan has been approved and implemented, it is important to carry out a periodic review of:

- effectiveness of the program in preventing incidents,
- maturity of the organization and procedures
- cost of the program vs. benefits obtained
- Training of staff

Key Performance Indicators (KPIs) may be used to provide weekly or monthly feedback to Operations staff of performance of the cybersecurity program.

The Cybersecurity Review might include the following steps.

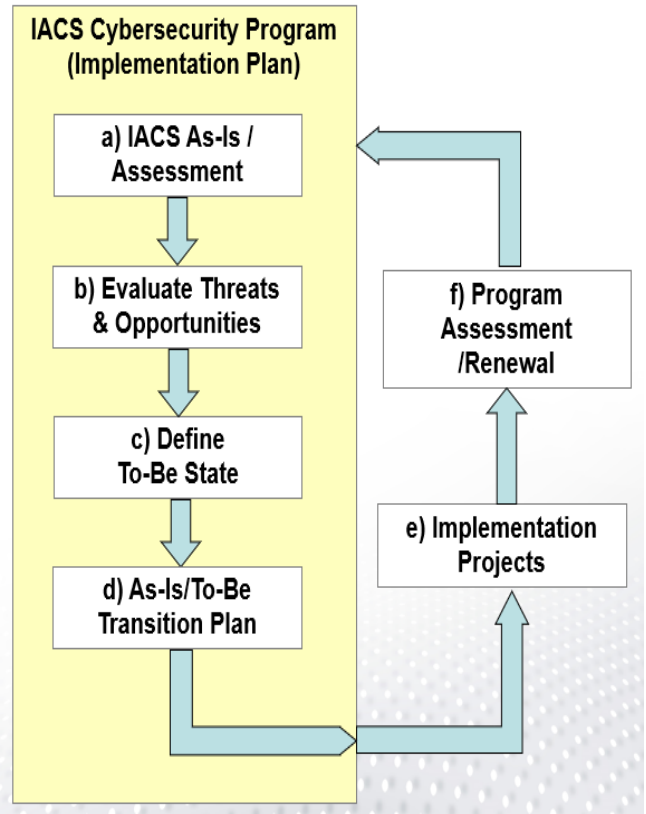


Figure 4 – ACS Cybersecurity Program Lifecycle

In addition, an, annual audit may be desirable. Synchronizing a cybersecurity audit with safety audits such as SIS/SIL (ISO 61511) or OSHA human safety might also be considered.

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 18 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.
.

Step 19 – Continuing Education and Training

The personnel who work with the enterprise integration system will change over time so it is important that those responsible for the operation, and maintenance of the system be well trained and capable.

The necessary training will be based on what was developed for the initial implementation. , there will be differences as noted below.

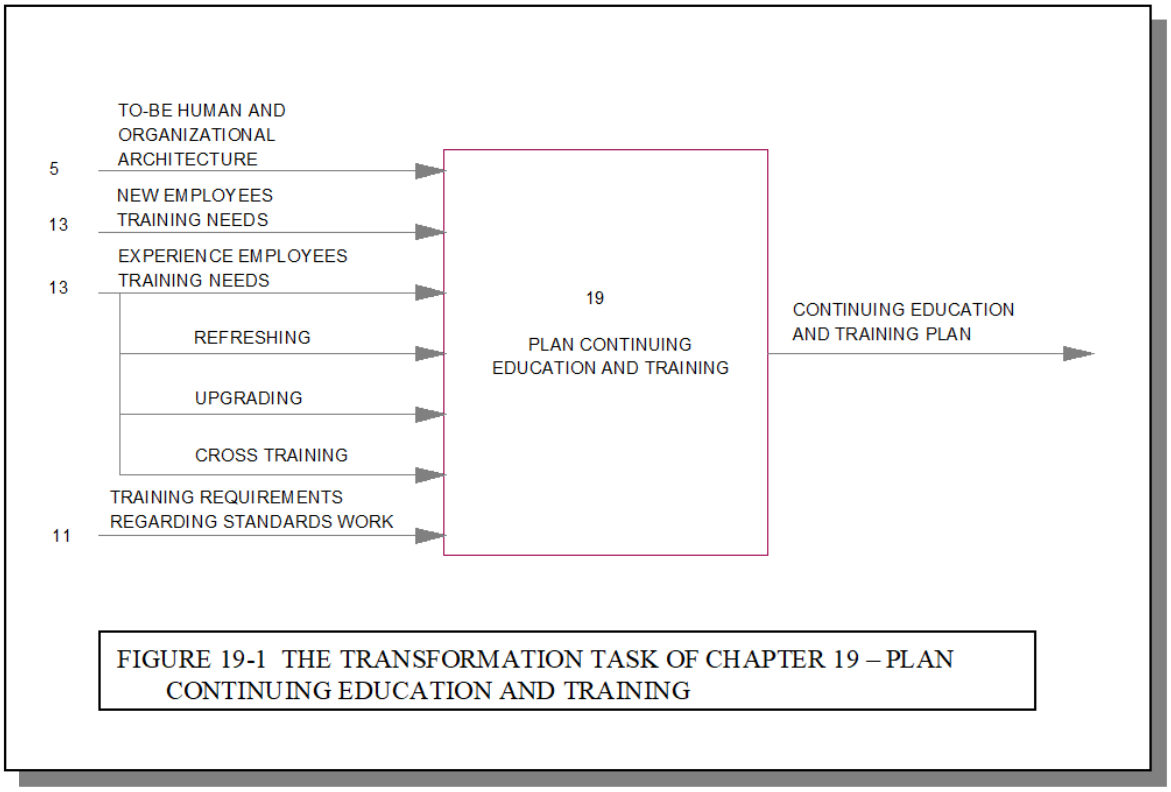


FIGURE 19-1 THE TRANSFORMATION TASK OF CHAPTER 19 – PLAN CONTINUING EDUCATION AND TRAINING

Training Requirements

Responsibility for training

Resources

For additional detailed information on defining the To-Be Human and Organizational Architecture, view the Step 19 section of the *PERA Handbook on Master Planning for Enterprise Integration.*

A template may be downloaded with chapter headings and formats for this report section. This may be added to the Table of Contents, and report sections described above to speed creation of a draft report.

Appendix I – Additional Reference Materials

- **Additional PERA Reference Materials**
- For additional detailed information on the PERA Master Planning Process, view the Appendices section of the *PERA Handbook on Master Planning for Enterprise Integration.*
- **Related MLMs**
  - MLM-072-A, Cybersecurity importance of Field Devices
  - MLM-074-A, ISA 62443 Applicability to Level 0, 1 SAIC Devices
- **PERA Articles**
  - PERA Master Planning and EPC to Permanent Facilities Migration, Shelby Laurents
  - Industrial Information and Control Network Architectures, Gary A. Rathwell
  - PERA and GERAM -- Enterprise Reference Architectures in Enterprise Integration, T.J. Williams and Hong Li
  - ISA GCA White Paper Implementing an ACS Cybersecurity Program Gary A. Rathwell

Appendix II – Author Background

Gary Rathwell

Process, Control, and Enterprise Integration Consultant

Gary has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for ethylene, polyethylene, ammonia and urea fertilizer plants, explosives manufacturing, hard rock and open pit mines, paint manufacture, plastics extrusion and packaging, pulp and paper, food and beverage plants.

For nearly a decade, Gary was the Functional Leader of Control and Systems Integration for Fluor Daniel. With over 50 offices, Fluor designed world-scale facilities using PERA Master Planning principles in oil refining and petrochemicals, onshore and offshore production, pipelines, chemicals, coal, gas, and oil-fired power plants, and pharmaceuticals. We also designed many infrastructure facilities, including Fire, Police, and Emergency Response systems for major US cities, and emissions reporting and trading systems for more than 100 US Power Plants.

As president of Enterprise Consultants International, Gary led Master Plans for many pipelines, including the world's largest crude oil pipeline network, oil and gas field production, transportation pipelines, refining, and marine loading facilities in several countries. We also did master planning for LNG facilities in Europe and Louisiana, a world-scale arctic LNG complex, and the Control systems and IT infrastructure for the largest oil production and refining facility in Kazakhstan.