PERA USER GUIDE

Preparing an
IACS / OT Project Master Plan
for a Process Industry Owner / Operator

August 25, 2024

Master Planning Guide
1-1-1

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

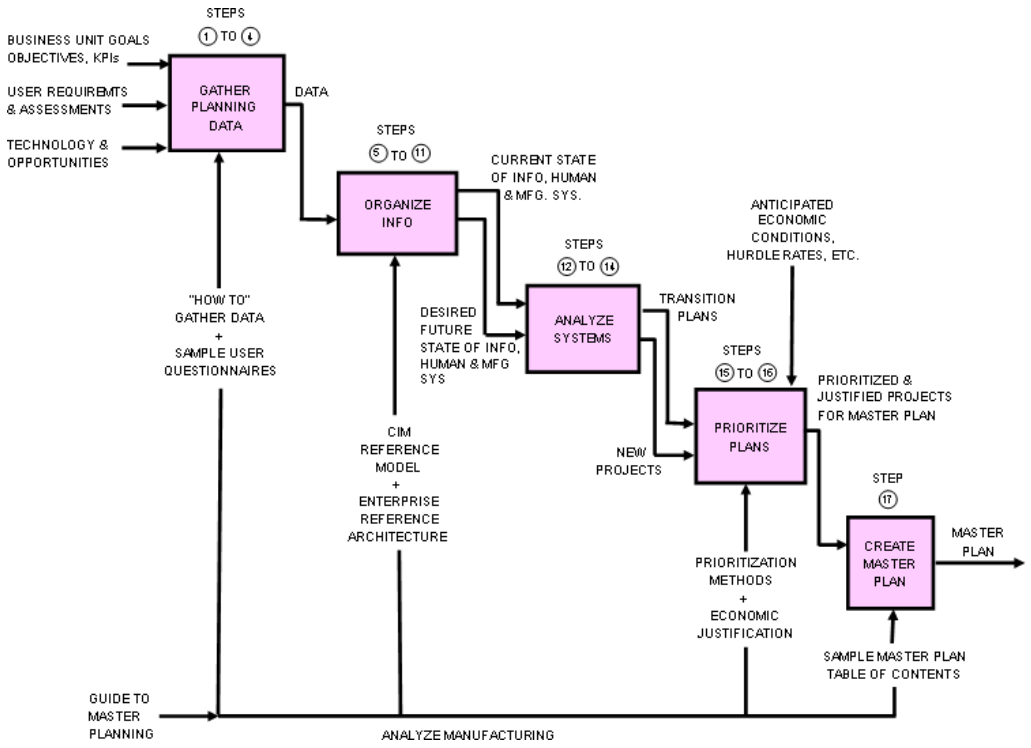
PERA Master Planning Guide
Generic Process Enterprise Planning

Overview of Planning Process

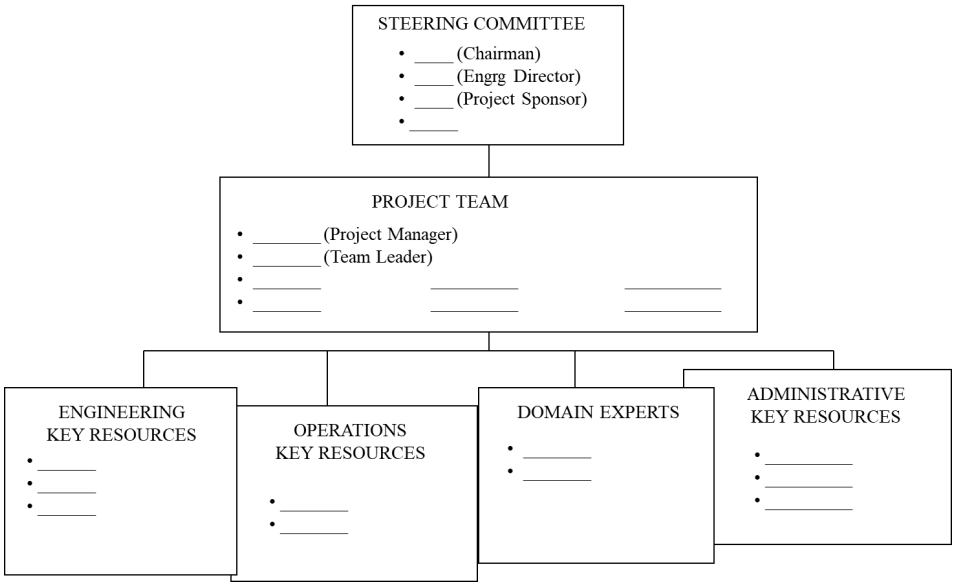
The PERA master planning process is comprised of 17 clearly defined steps. Each step produces a set of deliverables (e.g. reports or drawings) which are reviewed and approved by management before proceeding to the next step.

This document provides a "Guide" for each step in the Master Planning Process. For additional detail, see the "Handbook of Master Planning" on the PERA website (www.pera.net). The numbers in the above diagram refer to Chapters in this Handbook.

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



MASTER PLAN ORG CHART



It is also true that the risks and costs associated with cyber-attacks on IACS are too high to simply assign technical project and operations personnel to “solve the cybersecurity problem”.
The IACS Cybersecurity program should therefore be created and managed by business and technical leadership, via a tiered IACS cybersecurity council. 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), and the Corporate Security Manager.

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 IACS control systems. The Champion will report progress on the IACS 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

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

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						

Step-by-Step Description

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). It may also be necessary to tour existing facilities, or study available technology (possibly including site visits). 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 organization.

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 PERA Workbench). Each form will contain either "assessments" for existing systems, or "anticipated value" for proposed new systems. See PERA Workbench for example survey forms.

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).

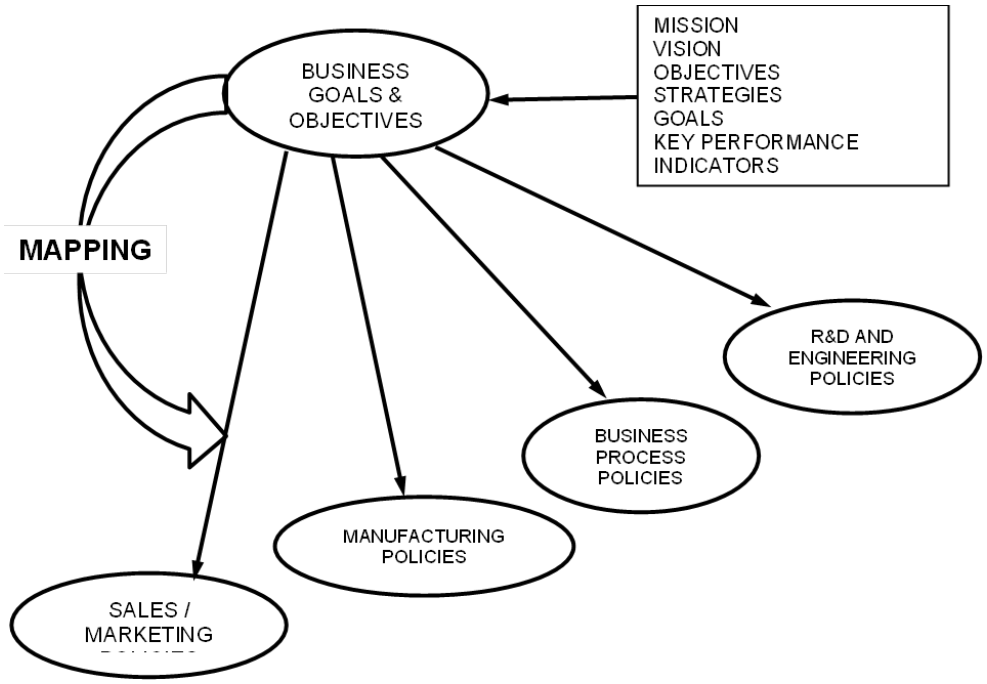
The **Business Plan** for each Enterprise Entity may also contain Goals that should be included, and these may be measured using Key Performance Indicators (KPIs).

These KPIs must be expressed in terms that are quantifiable 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.

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 all Enterprise Entities. 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 each 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 IACS Policies such as such as use of company-standard DCS, PLC and SCADA architectures and products. Such Industrial Automation and Control Systems (IACS) 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 IACS architectural policies.

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. These Opportunities may:

- Be drawn from successful implementations in similar industry
- Involve new technology, practices, or products
- Eliminate current obsolete technology, practices or products
- Improve existing Human and Organizational practices

Should any of these require changes to existing company Policies, this must be formally accepted before including the Opportunity in the proposed list.

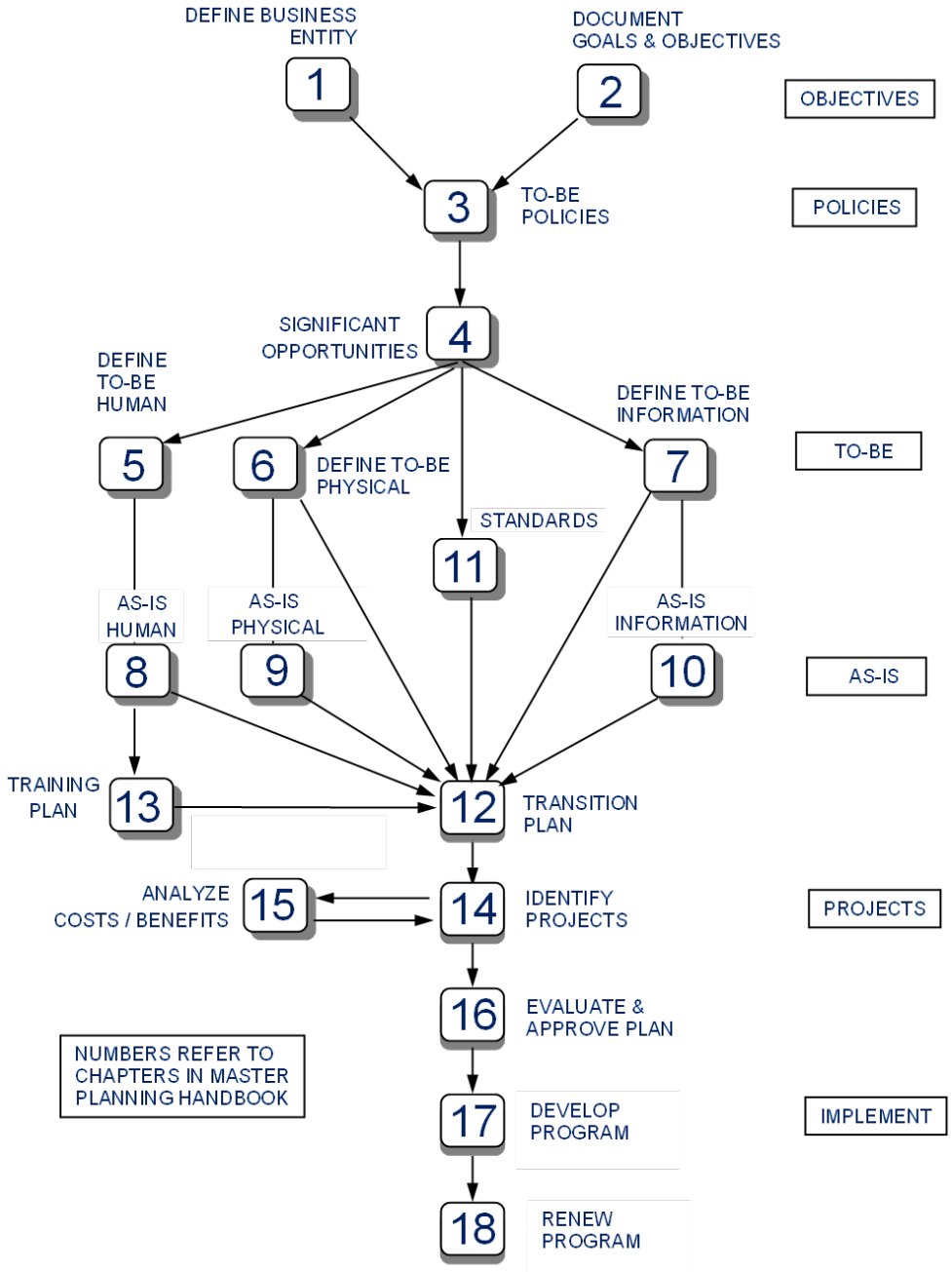
This list typically includes 20 to 30 Opportunities (dependent on the nature and size of the enterprise). The largest Master Plan that I have personally led involved 50 Opportunities, while the smallest had only 12.

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.

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.

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 PERA Master Planning Workflow diagram.

PERA MASTER PLANNING WORKFLOW



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, it would not be productive to assess the As-is situation in detail.

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).

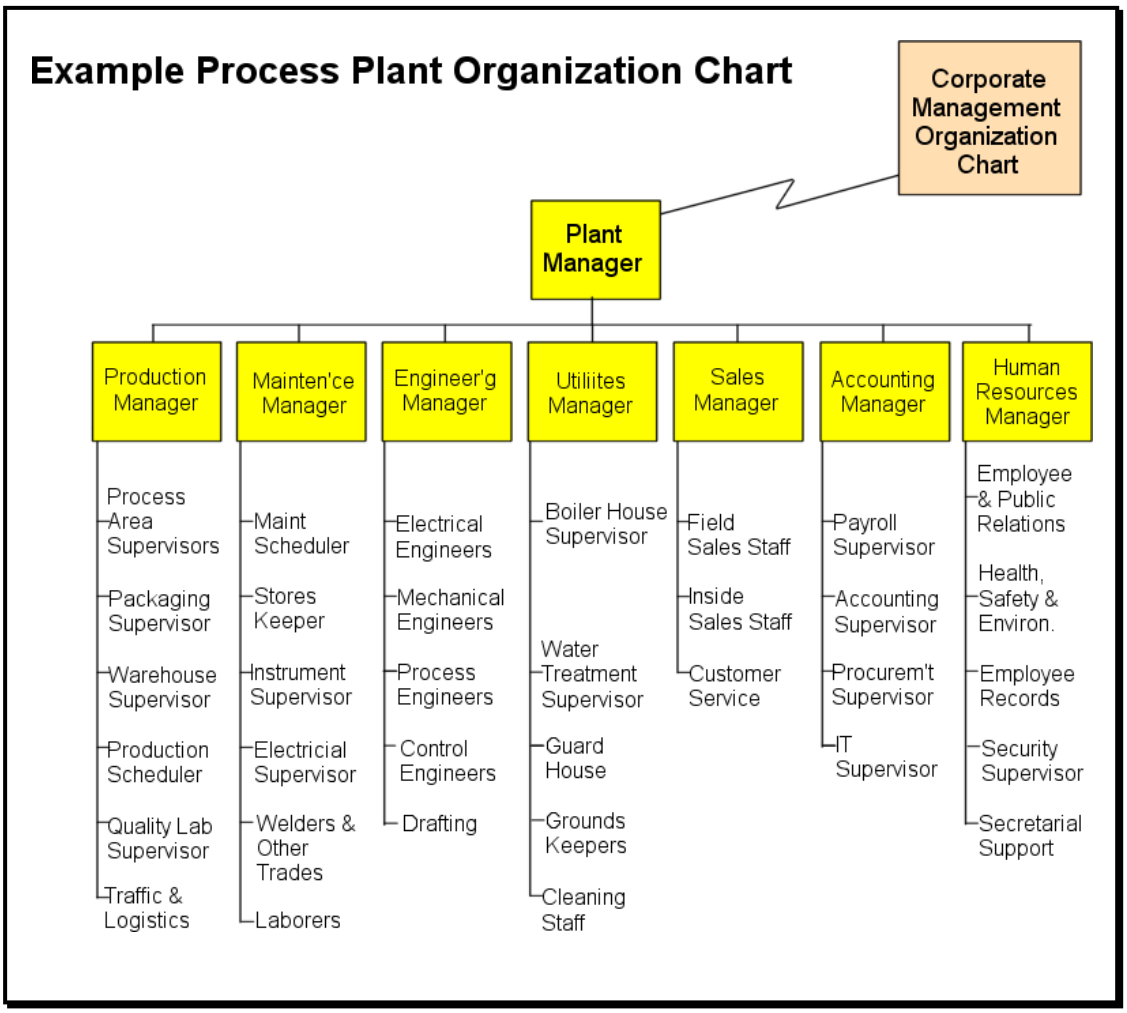
Training requirements (Step 13) are determined from As-is and To-be human and organizational requirements. These are added to the Transition Plan (Step 12).

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).

This Master Planning Guide is intended for a Process Industry Master Planning study, so the example diagrams, terminology, and proposed standards are ones that will be familiar to experienced practitioners in these industries.

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 are relevant to this study. These Professional Roles may be assigned specific Opportunities or Projects.

770	**Control and Information Systems**
771	Instrumentation Design
772	Metrology
773	SCADA Systems
774	Analyzers & Sampling Systems
775	Tele-mechanization
776	Process Fire Protection
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

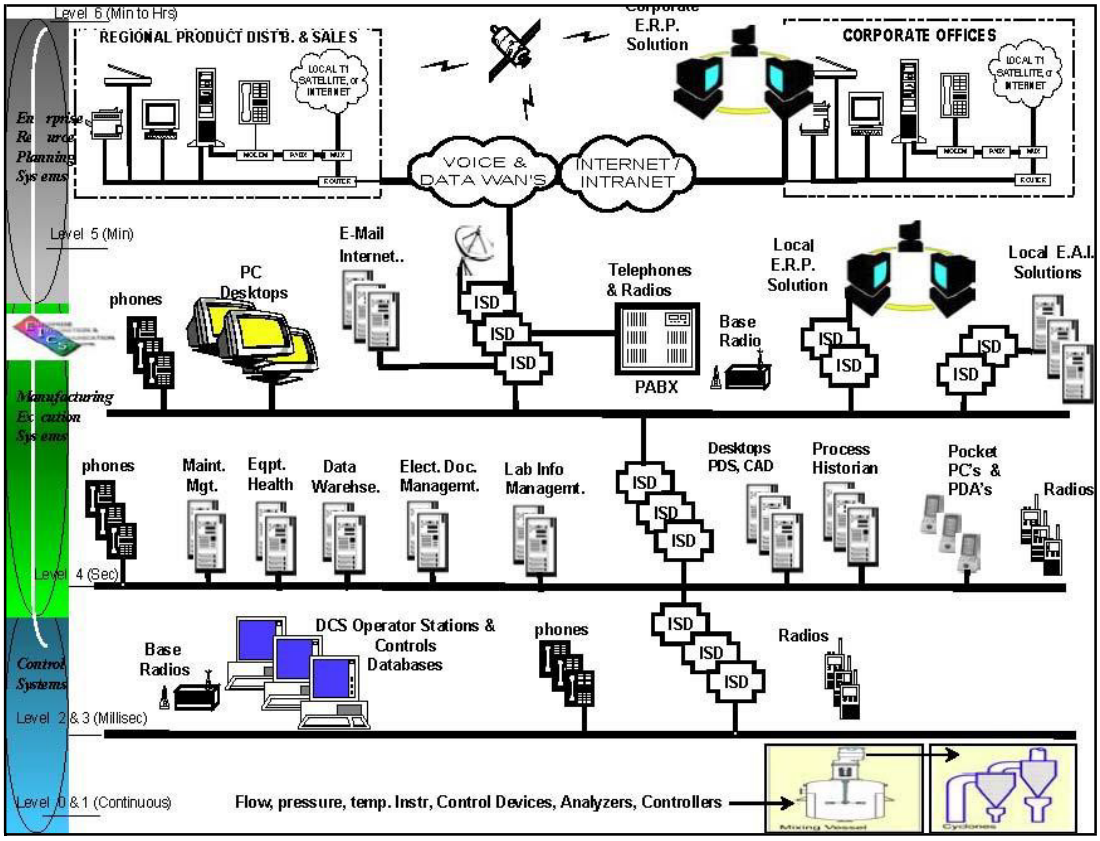
Step 6 - Define "To-Be" Control & Information Systems Architecture

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.

See the PERA Workbench for documentation standards for these drawings.

Physical Network Architecture Diagram



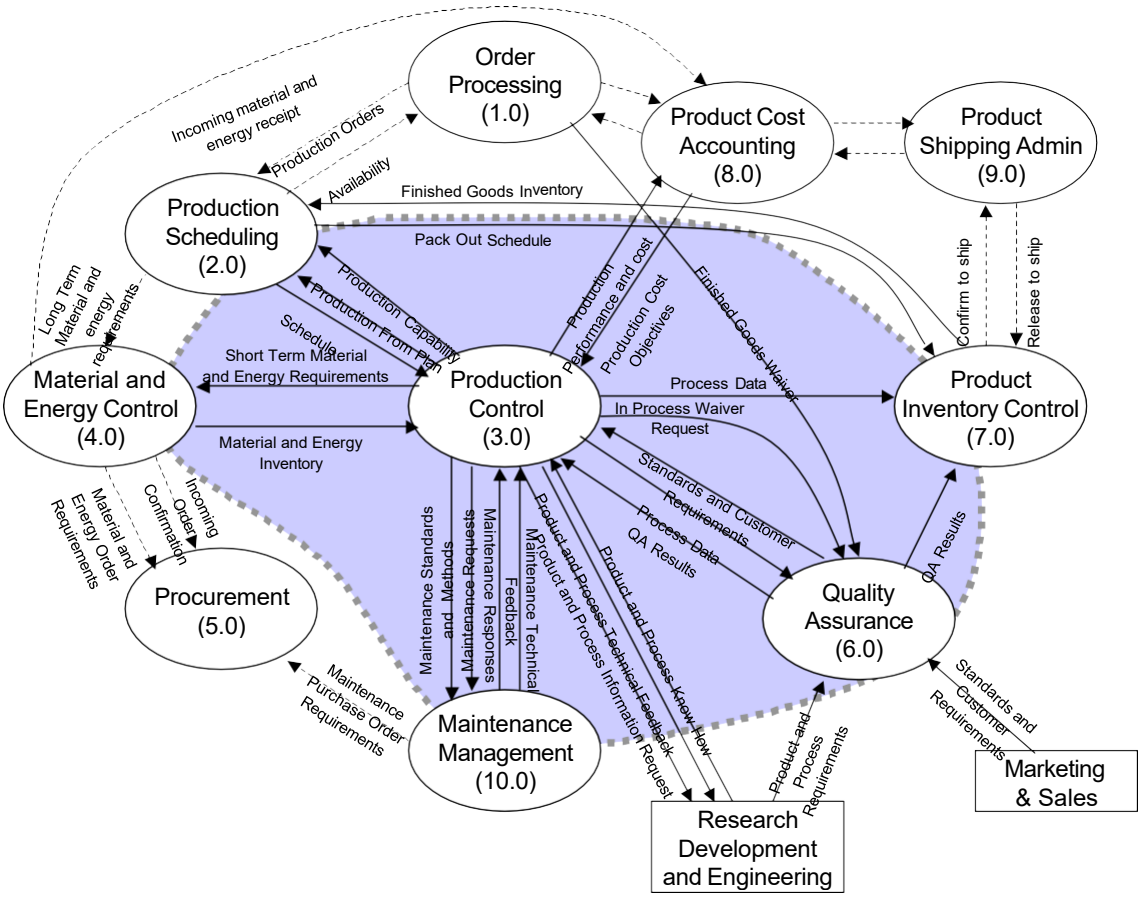
Source: Fluor Daniel EICS Group

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 the networks at the appropriate "Level" in the physical architecture. All connections between levels are "controlled" by a gateway, router, firewall or other "managed" device.

The rules for 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 Systems Architecture Diagram



Source: Purdue Reference Model (ISA-95)

The ISA-95 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.

Step 7 - Define “To-Be” Facilities

The “To-Be” Enterprise Facilities describe the Physical Production Facilities required to deliver the products and services produced by the Enterprise. Depending on the industry involved, these facilities may be documented with Process Flow Diagrams, Mechanical Flow Diagrams, Facility Layouts, Block Diagrams, and other standardized documents.

The physical layout of the production equipment and the control and information system devices are fundamental to risk management (e.g. in the event of explosion or fire) and of security (e.g. cybersecurity or plant perimeter security).

Step 8 - Define ‘As-Is’ Human & Organizational Architecture

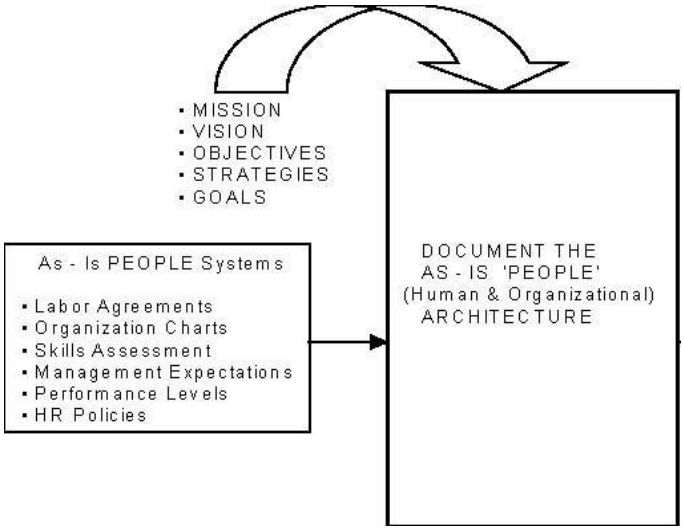
For an existing enterprise, the organization charts and position descriptions are assembled to establish an As-is “baseline”.

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).

Step 9 - 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.

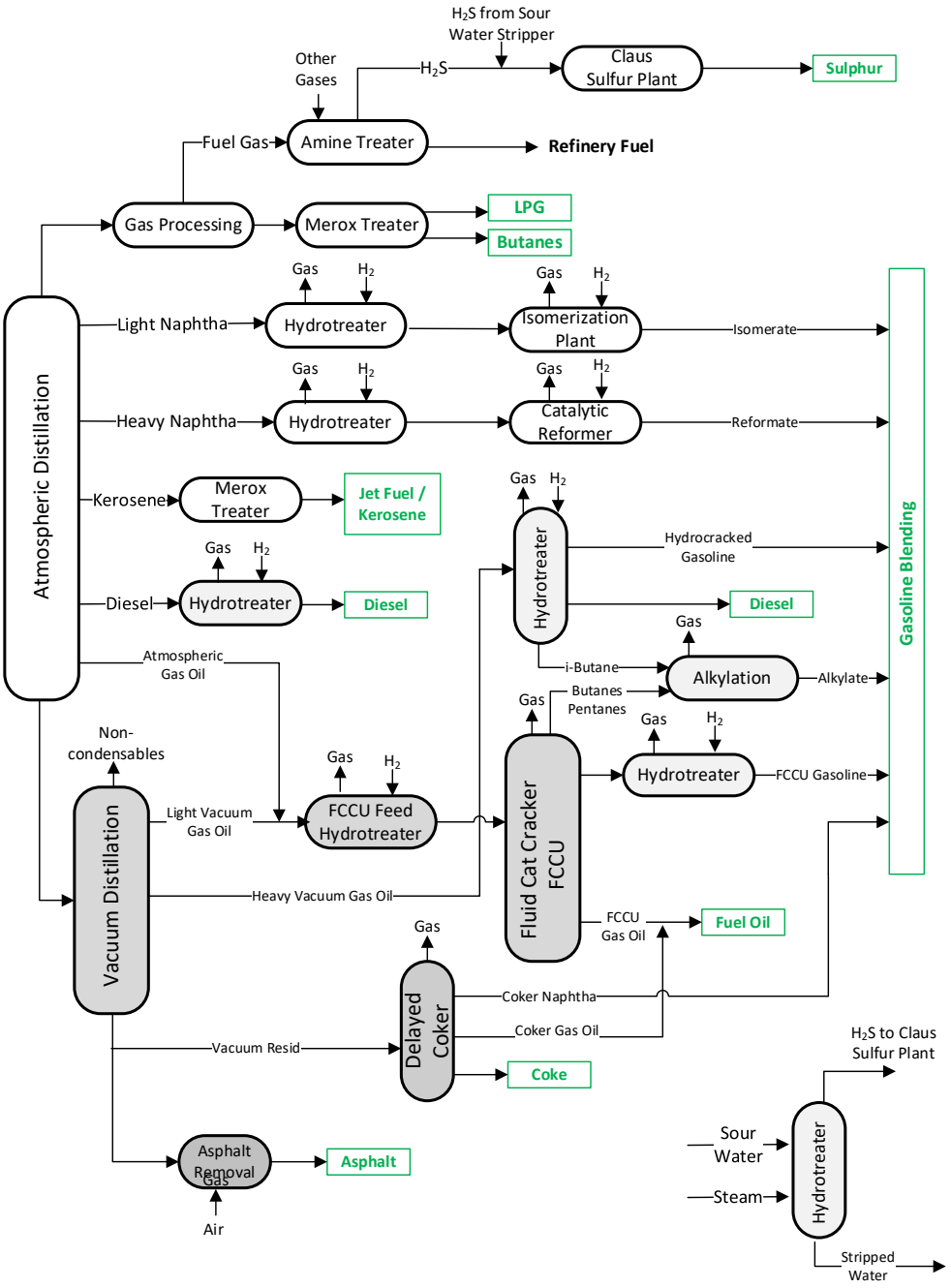
User Survey Forms including most of the common Enterprise Systems, MES, and Control Systems is provided on the PERA Workbench. This assessment will later be compared (in Step 12, Transition Plan) with the "To-Be" state, and will be used to assess the benefits of the proposed To-Be Systems.

Step 10 - Define "AS-IS" Facility 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



Step 11 - Standards Selection

Definition of As-Is and To-Be Control and Information systems has been greatly facilitated by new standards such as ISO ISA95, SIS/SIL, ISA99, and MESA standards which standardize enterprise systems functions, nomenclature, architectures, and interfaces. Some of the major areas covered by these user input forms include the following. The source of the standard definitions for major systems, subsystems, sub-subsystems, etc. is also indicated

System or Subsystem	ISA95	MESA	ISO 27000	ISA99 Cyber-security	ISA84 SIS/SIL
Order Entry	1.0				
Production Scheduling	2.0	2.			
Production Control	3.0				
Process Support Engineering	3.1	8.			
Operations Control	3.2	3.		1.	1.
Operations Planning	3.3	1.			
Material and Energy Control	4.0	10			
Product Procurement	5.0				
Quality Assurance & Management	6.0	7.			
Product Inventory Control	7.0				
Product Cost Accounting	8.0	11.			
Product Shipping Administration	9.0				
Maintenance Management	10.0	9.			1.
Document Control		4.			
Data Collection / Acquisition		5.			
Labor Management		6.			
Process & Human Safety					1.
Control & Information Systems Security				1.	

All of the above systems have standardized Functions, data elements, and data interface flows. Typically, the Functions and Information Flows of one level deeper in the hierarchy are included in the questionnaire. Thus the survey is composed of approximately 100 Functions (note the number of functions that are necessary are strongly influenced by the industry involved, whether operations are continuous, batch, semi-batch, manufacture to inventory, manufacture to order, or custom-engineered to order. See PERA Workbench for Industry Type Codes and lists of Opportunities by Industry.

In many cases, standards for Physical Facilities vary by country, and many even have the force of law. Thus these standards will have a major impact on the design and documentation of Facilities, and should be identified at the earliest possible stage in the Enterprise planning process.

See the PERA Workbench Standards library for descriptions of selected individual standards from groups such as:

- ANSI - American National Standards Institute
- API - American Petroleum Institute.
- ASME - American Society of Mechanical Engineers
- IEEE - Institute of Electrical and Electronic Engineers
- ISO - International Standards Organization
- BS - British Standards Institute
- DIN - German Institute for Standardization.
- EIA - Electronic Industries Alliance
- GOST - State standards of Russian Federation
- PIP - Process Industry Practices

Particularly important for Enterprise Integration projects are standards such as:

- ANSI / ISA 95 (IEC/ISO 62264-1) which deals with how to design open architectures that allow integration of Manufacturing Execution Systems with upper level Enterprise Resource Planning Systems and with lower level Production Control Systems.
    - Part 1: Models and Terminology (July 2000)
    - Part 2: Object Model Attributes (October 2001)
    - Part 3: Models of Manufacturing Operations (Draft)
    - Part 4: Object Models & Attributes of Manufacturing Operations Management
    - Part 5: Business to Manufacturing Transactions

- ANSI /ISA 99 and IEC 62443 that describes how Control and MES networks are designed, implemented and maintained in a secure, consistent manner. ISA S99 provides guidance documents and standards for IT security for existing industrial control and automation Systems.
    - Part 1 – defines terms and models used in automation security, and
    - Part 2 – establishing Cyber Security Management Systems. IEC 62443 – mainly addresses technical aspects of system security architecture.

Step 12 -Document Transition Plan From “AS-IS” To “TO-BE” Architectures

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.

Step 13 -Training and Documentation Plans

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

Step 14 – Document Proposed Projects

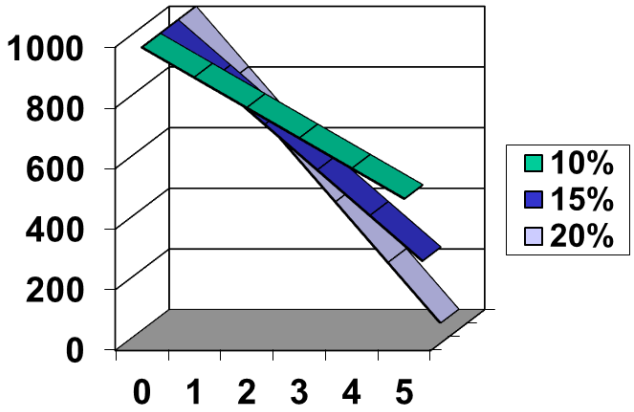
We now combine the Opportunities developed in Step 4 (and their resulting “To-Be” architectures of Steps 5 to 7) with the Transition Plan defined in Step 12. The “To-Be” opportunities and the Transition from “As-Is” systems are organized into “Projects” so that the work can be planned, developed and implemented most efficiently. Where possible, projects are organized into modular groupings where the interfaces are minimized in order to improve project execution effectiveness and reduce interfaces.

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

Step 15 -Analyze Costs, Benefits and Risks

A cost/benefits analysis is prepared for each of the selected projects. The process is a cooperative iteration with Step 14 to agree 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 is input for each Opportunity at each Facility as shown on the right.

Step 16 –Finalize and Document Enterprise Systems Project Evaluations

The proposed projects and implementation plan are now reviewed by all Master Planning Team participants. As a group, they agree all of the opportunities and projects to be taken forward as well as all supporting documentation (e.g. cost and benefits assessments).

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

Step 17 -Author Enterprise Master Plan

Finally, the Enterprise Master Plan is documented and formally presented to the steering committee.

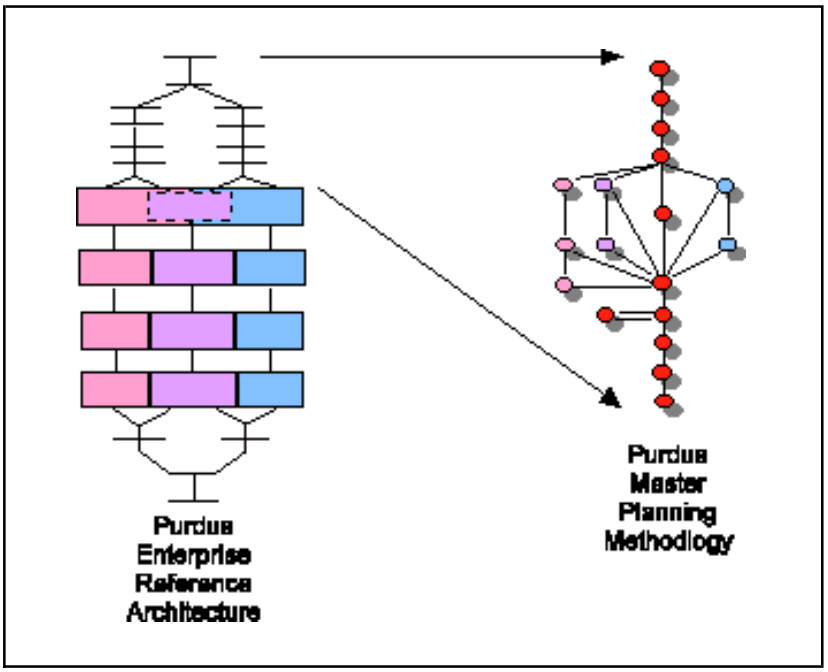
The completed Master Plan will typically contain the following items:

- Executive Summary
- Enterprise Business Entities
- Goals / Objectives, KPIs
- “To-Be” Enterprise Policies
- Opportunities Conceptual Description
- “To-Be” Human and Organizational Systems
- “To-Be” Control & Information Systems
- “To-Be” Physical Facilities
- “As-Is” Human and Organizational Systems
- “As-Is” Control & Information Systems
- “As-Is” Physical Facilities
- Standards Selected (and Requirements identified from each)
- Transition Plan
- Training Plan
- Project Conceptual Descriptions
- Approximate Costs & Benefits Summary
- Final Project Disposition
- Approvals for Projects

Step 18 – Project Implementation and Operations

With completion of the Master Plan and approval of proposed projects, a more formal engineering design process begins. PERA provides an overall framework for all parts of the subsequent engineering and design process, as well as construction and eventual operation of the completed facilities. This relates to the PERA Master Planning process as follows:

The PERA Master Planning process directly corresponds to the Study Phase and Conceptual Engineering Phase of the Purdue Enterprise Reference Architecture (and most other Phased Engineering methods). After Master Planning, the next phase is Preliminary Engineering, where (among many other things) formal purchase specifications are prepared for bid by vendors or for custom programming by in-house or outsourced groups.



Client Approvals Process

In addition to the technical design of facilities, people, and systems there are parallel activities involving management and approvals by the owner (sometimes described as “Stage-Gate Processes), International Finance organizations (who have their own special documentation requirements), and Regulatory groups (whose documentation and approval processes vary widely by country). See PERA Workbench for additional information on Stage Gate methodology.

Note:

Under the classical PERA definition, Facilities are associated with delivery of the Goods and Services that are provided by the Enterprise. Thus, Control Cabling, Computers, and Networks are part of the Control and Information Systems of an Enterprise; the logic being that in an enterprise with no automation, the Humans would directly interact with the Facilities (e.g. read gauges and directly manipulate valves), and the cabling, computers, etc., would be eliminated. The interface between Physical Facilities and Control and Information Systems is thus typically defined as “the first connection point above the plant sensor or valve actuator”

However, for some enterprises (e.g. a telecommunications company or an Internet web services company), the goods and services they provide are largely contained in these computers and networks. Also, for Enterprise Integration Master Plans the plan is largely focused on the Control and Information Systems, and on the Human components of the Enterprise, with little impact on the Physical Facilities which deliver goods and services. In both of the above cases, it has been the practice to define the Physical Networks and computers as part of the Enterprise Facilities. In practice, this means that the Physical Network Architecture Diagram (and associated documentation) is included in the Physical Facilities component of the Enterprise. In this case, the interface between the Physical Facilities and the Control and Information Systems is defined as “where Logical Systems and Networks interface with Physical Networks and Systems.

For a description of a Master Planning process for “Information Services” or Enterprise Integration projects see “PERA Master Planning Process – Enterprise Integration”.

Either definition may be used, but once made for a given Enterprise, it should be used consistently.