SYSTEMS AND SOFTWARE ENGINEERING FOR THE MAX IV FACILITY

T. Friedrich, MAX-lab, Lund and KTH Stockholm, Dept. of Machine Design, Sweden

Abstract

MAX-lab, the Swedish National Electron Accelerator Laboratory for Synchrotron Radiation Research, Nuclear Physics and Accelerator Physics is planning the construction of a new synchrotron light source facility in Lund, Sweden. The new facility's IT infrastructure introduces design, construction and maintenance challenges related to large distributed control systems, process control and monitoring, data analysis and representation, system integration and significant changes throughout the entire life cycle. MAX-lab will have to cope with organizational growth, information complexity, technical complexity and resource constraints. This paper describes the systems and software engineering issues related to the construction and maintenance of the MAX IV facility, and outlines the development of an engineering approach suitable to the possibilities and constraints of the MAX IV project. Key subjects are requirements and specifications, architectural design, standardization, organizational structure, systems and software lifecycle management and development processes.

MAX IV AND SYSTEM LIFE CYCLES

The MAX IV facility design includes two 3rd generation electron storage rings operated at 3 GeV and 1.5 GeV and a LINAC based short pulse facility. The main MAX IV synchrotron light source is the new low-emittance electron storage ring with 20 straight sections. At the time of publication, the MAX IV facility's funding is decided, organizational structures for the construction phase are being formed, and the detailed technical design report is continually updated. In the IT and controls domain, a number of workflow processes are being initiated or intensified, on which an overview shall be given here. This overview is oriented at the ISO/IEC 15288-2008 [1] standard on "Systems and Software Engineering - Systems life cycle management". The ISO/IEC 15288 standard offers a common process framework for the life cycle management of man-made systems with an emphasis on process tailoring towards specific environments. The introduction to the life cycle processes of the MAX IV IT infrastructure shall also provide insight into the suitability of this standard as a process framework for the accelerator IT systems domain in general, as it gives the paper's scope on systems, organizational issues and work processes.

AGREEMENT PROCESSES

The agreement processes produce *supply agreements* with in-house parties or presumed future users of the services of the IT group, and *acquisition agreements* on services or products from external providers required by the MAX IV IT group. The *acquisition agreement process* is performed by the IT group based on architectural design decisions, technological in-house standards, in-house process considerations (e.g. maintenance) and in respect of existing supply agreements (e.g. network infrastructure). With the increasing level of detail of MAX IV requirements and specifications, the *supply agreement process* produces more detailed supply agreements with in-house groups.

ORGANIZATIONAL PROJECT-ENABLING PROCESSES

In a variety of enabling processes, provisions are being realized for the IT group to fulfil its tasks.

Infrastructure Management

In an *infrastructure management process* the working environment for the computing systems group is being formed by defining

- IT related budgets, accounts, and guidelines for the acquisition and supply process
- tool and technology-related tasks and responsibilities
- establishment of internal communication
- establishment of collaborative contacts
- provision of tools, workplaces, etc.

Human Resources

In the *human resources management process* it is assessed what organisational structure shall form a future computing division, assuming responsibility for all types of computing systems, including control systems, office IT, software systems and services, etc. on the level of a major support group. The internal group structure is based on IT and engineering expertise (as opposed to laboratory sections), with the main subgroups being a group for electronics and hard real time systems, a group for software and systems integration, and a service group (office PC's, etc). The reasons are typical educational or personal backgrounds, the alignment of individuals' skills and expertise along technological in-house standards, and the need for staff transitions between laboratory sections (e.g. over succeeding construction phases).

Further it is investigated, what combination of in-house development and outsourcing can be most profitable in relation to lifecycle cost minimization. For successful out-sourcing it is advisable to support in-house expertise in

- requirements and specification of complex systems
- integration of systems, including quality control
- maintenance of the acquired systems

leaving open as the preferable tasks for out-sourcing:

- detailed system design and architecture
- system implementation
- system installation.

Information Management

The *information management process* is concerned with the provision of information which is relevant, valid, complete, timely and accessible. For the electronic media used for MAX IV this covers various engineering disciplines and stakeholders (including, beyond IT development, scientists, technical staff, etc.), so the information management process' first goal is to reach agreements on the facility level on shared information management tools and content structure. This may includes CAD, office documents (e.g. reports, user manuals, publications), measured data, configuration files, software, etc. Available products and services from the Product Lifecycle Management (PLM) domain are being assessed for their suitability as common repository and management tool for electronic documents and files. Shared storage and access of these files necessitates the establishment of a shared information model as part of the process. A generic toolset oriented at office documents and CAD will be complemented by more specific systems, such as a cabling database, an equipment management tool, etc. where these render useful.

Configuration Management

For the systems and services provided by the IT group, a configuration management strategy is being developed in a configuration management process. As the degree of system variety is expected to have a major impact on manpower resources required for maintenance at operation time, we pursue an early-on standardization strategy on the system types, prioritizing the minimization of technology heterogeneity. Hence, a first goal in the *configuration management process* is to provide a catalogue of supported and preferred systems and services, covering the bulk of required functions. As this catalogue shall serve as the technology alignment tool between essentially all development projects, its provided systems and services need to be available and validated early.

TECHNICAL PROCESSES

Technical processes are primarily processes related to a system's life cycle, covering requirements, design, implementation, testing, installation, operation and maintenance.

Requirements Engineering

As part of the *requirements engineering process* MAX IV requirements are elicitated by interviews with various in-house stakeholders and by surveying corresponding systems and technologies in use at existing light source facilities. For the management of the MAX IV requirements and specifications, we consider the following aspects as challenges:

- the sheer number of requirements for 3rd/4th generation light sources and >30 beamline facilities
- the variety of stakeholders and domain interests
- the variety of viewpoints on the systems
  - physical functions
  - system type architecture
  - system deployment architecture, e.g. geographical deployment, name structure
  - operational dependencies

Desirable goals for the practical work with requirements, specification and documentation are

- shared access for analysis, editing and validation
- production of system documentation explaining the purpose of the system, architectural decisions, dependencies, interfaces; documenting up to, and not beyond, the level where documentation is likely to be used and to reduce operational or project risks
- inter-relating requirements and specifications of different projects in a homogenous, traceable way; of interest in particular for in-house standardization projects with a wide application range, and for complex systems relating to many other systems or subsystems

The goal to manage the *requirements*, *specifications* (and, to a degree, *documentation*) for the IT systems in a common way necessitates the combination of a suitable information structure with an appropriate toolset. For control system projects (machine control, beamline control, data processing and management software) we consider the following top-level information structure on systems to be an appropriate template to enable the goals above.

1. System goals
2. Stakeholders
3. Domain requirements and Use cases (motivating the *system user's need* for the system/project in question, and explains the anticipated usage)
   - 3.1. System configuration use cases
   - 3.2. Maintenance use cases
   - 3.3. Data acquisition use cases
   - 3.4. Data analysis use cases
   - 3.5. Stress cases (alarm conditions, etc.)
4. Machine specifications
   - 4.1. Deployment structure. This section describes the physical, geographical or instance structure of a system.
   - 4.2. Building blocks. Describes system 'types' and system composition, defining systems as well-defined, in principle re-usable, encapsulated entities. E.g. the integration component for a required type of hardware (sensors, actuators).
5. Feature requirements (specifies *system functions* such as communication interfaces, commands, methods, properties, data exchange)
6. Quality requirements (performance, usability, safety, security, reliability, integration and interoperability, maintainability, portability)
7. Constraints
   - 7.1. Project schedule constraints
   - 7.2. Financial constraints
   - 7.3. Other constraints (technological, legislative, organisational)

Relevant properties for requirements and specifications:

- definition and rationale
- source, owner and reference persons
- status
- priority
- dependencies

The template structure allows to include the various stakeholders' demands, to present the disparate system views in their own rights, and enables the tagging with appropriate and relevant properties. We assume a professional requirements management tool to be the best choice for the practical management. As the proposed information hierarchy maintains a common frame from user domain requirements to detailed system specifications, the resulting database should also serve as a *source of system documentation* for operation and maintenance life cycles, addressing a typical documentation issue at scientific facilities: Many systems are prototypical, to some extent permanently preliminary, subject to on-going optimization, or designed with partially unknown or intentionally-open specifications. In initial operation phases, documenting systems hence poses a potentially wasted effort, collides with new projects and emerging opportunities, and depending on workloads is deemed of low priority, thereby entering a postponement chain. The proposed approach to requirements and specification production might to some extent reduce this problem.

Architectural Design Process

For the architectural design, it is agreed to adopt design guidelines beneficial to cost-efficiency. The control system software architecture is designed in a multi-layer fashion spanning over distributed nodes, as found in other light sources as well, with some variations. Software systems shall constitute well-defined, separable entities within these layers:

- application layer (client-side user applications, in particular presentation)
- service layer (administrative, information processing and data archive services)
- process control layer (coordination of system interactions, soft real-time processes, data collection, etc.)
- system composition layer
- hardware integration layer (integration of physical actors and sensors)

The timing system for beam operation, the accelerator equipment protection system, the personal interlock system and the fast orbit correction system will be encapsulated systems with dedicated signal lines, and be connected to the integrative control system for monitoring and configuration purposes.

The technological choices for sub-system components, hardware platforms and software technologies will be largely defined by *in-house technology standards* in order to minimize system variety and system maintenance costs on the generic level. While specific hardware platform standards are still matter of discussion, some software standards are being settled on. For in-house operating systems, a Linux and a MS Windows platform is provided. As primary programming languages, C/C++ (low level), Java and Python (application level) are preferred, supplemented with bindings (e.g. MATLAB, LabVIEW) as required. For the control system framework, it is decided to utilize the TANGO framework.

Ongoing Process Management

Organizational project-enabling processes in the scope of the IT group, in preparation to varying degrees:

- a *project-portfolio management process* dedicated to initiation, evaluation and closure of projects
- sub-system specific *project processes*
- a *quality management process*
- a *risk management process.*

Further technical processes are in planning states:

- system *implementation process*
- system *integration process*
- *verification process*: definition and execution of testing procedures, commissioning
- *maintenance processes* for hardware and software systems. The process is though heavily influenced by standardization choices done today.

These processes are subject to discussion in their anticipated demands and execution guidelines.

LIFE CYCLE MANAGEMENT

Key risks for MAX IV are budget overruns and the ability to cope with a new degree of technical complexity in a time of organizational growth. For MAX IV's IT infrastructure, the ISO/IEC 15288 standard offers a comprehensive framework for the analysis of relevant work processes and can provide meaningful guidance for quality improvements (defining system quality related processes). The standard's view on organizational activities enables better estimations of future work packages, reducing the risk of incomplete planning or underestimated resource demands. It respects the need to tailor processes towards specific requirements where needed: Differences between a physics laboratory and other facilities or organizations can be seen in the non-profit aspect, the technological uniqueness, the life cycle spanning prototypical character of large parts of the machinery and the specifics of the cultural (scientific, national) environment. Hence we consider the ISO/IEC 15288 standard a suitable tool for the life cycle process management of IT systems at MAX IV, beneficial for the capability of the IT group to meet MAX-lab's objectives and to support upcoming projects by effective methods.

REFERENCES

[1] ISO/IEC 15288-2008. Systems and software engineering – Systems life cycle processes. ISO/IEC 2008.