Improving the Management of the Software Acquisition Process: a Methodological Approach in Automotive

Fabrizio Fabbrini, Mario Fusani, Giuseppe Lami
System & Software Evaluation Centre - I.S.T.I. / C.N.R. Pisa (Italy)

Edoardo Sivera
Issues in Automotive

The number of software-based components in automotive systems is increasing:

- **Comfort electronics**
  - Seat and window movement

- **Real-time critical functions**
  - Cruise control
  - Antilock brakes
  - Engine management

- **Multimedia applications**
  - GPS, DVD
  - Internet

- **Wireless applications**
  - Tyre pressure control
  - Access control

- Need to control the development cost of software-based component.
- Need to manage the development of the software-based component, to increase the quality of the final products.
- Need to define new relationships with the suppliers, to better manage sw-based component.
The System & Software Evaluation Center (SSEC) performs independent certification activity in the area of Information Technology since 1984. In particular:

- Software Product Evaluation and Certification according to defined requirements and standards
- Software Process Assessment (process improvement, capability determination) [ISO/IEC 15504, SPICE]

SSEC is part of ISTI, an Institute of the Italian National Research Council that performs research in Computer Science, Information Technology and related application areas, mostly within the framework of national and international research projects. SSEC staff members participate in national and international Working Groups for ISO standard definition in the field of Software Engineering.
Fiat Auto
Product & Process Engineering
Electronic & System Engineering

Tasks

§ To define requirements (HW, SW, communication, reliability, etc.) for the electronic systems and components used in all Fiat, Lancia and Alfa Romeo vehicles.

§ To define requirements for the vehicle “body” electronic systems
   - Lock-unlock doors, passive entry system, anti-thief system, seat movement, windows, mirrors, etc.

Objectives

§ To monitor the Software technologies used in the embedded electronic systems

§ To use standard methodologies in order to evaluate the “process capability” of the suppliers

§ To control the software life-cycle of the embedded systems

§ To define and apply methodologies to validate functional requirements of the embedded systems.

§ To define the SW architecture used in embedded systems
The ESCAPE Project

Goals

- To set up a methodology supporting the management of software projects and suppliers
- To improve FIAT process to select suppliers
- To improve the software development process of suppliers
- To provide FIAT with methods to determine the risks associated to software suppliers
- To give FIAT a better control on the software development project and on the quality of the resulting product
The ESCAPE Project
Action Plan

- Phase 1: FIAT Suppliers' Capability Determination
- Phase 2: Monitoring Plan Definition
- Phase 3: Methodology Validation
Reasons for SPA

Software Process Assessment is a way to better understand (and manage) the software process development of a supplier. The assessment is done to:

- define a “capability” level and a “risk” level for each supplier
- have a criterium to choose suppliers based on their “capability”
- understand weak and strong areas of the development process
- define better functional requirements
- define better system verification and validation procedures
Phase 1: Supplier’s Capability Determination

Assessment Preparation

§ Planning the Assessment
On-site visit
Time/Cost constraints
Technical constraints
Assessment risk identification

§ Defining the Assessment Purpose
Capability Determination
[Process Improvement]

§ Defining the Assessment Scope
Requirements elicitation process (CUS.3)
System requirements analysis and design process (ENG.1.1)
Software design process (ENG.1.3)
System integration and testing process (ENG.1.7)
Project management process (MAN.2)
Phase 1: Supplier’s Capability Determination

Project implementation

pre-assessment activities

§ Introductory meeting
To introduce the SPICE (ISO 15504) approach
To review the assessment purpose, scope and constraints
To introduce the assessment activities and the provisional assessment plan

§ Pre-assessment questionnaire
To gather preliminary information on the projects to be used as process instances
Phase 1: Supplier’s Capability Determination

Project implementation

on-site activities

- **Briefing**
  - Assessment purpose, scope, constraints and model
  - Confidentiality policy
  - Assessment schedule

- **Data Acquisition & Validation**
  - Presentations
  - Document analysis
  - Interviews

- **Process rating**
  - (provisional)

- **Debriefing**

{Checklist-based}
The Rating Dilemma

- Different rating methods can be applied
- ranging from the mere processing of measured indicators up to the unaided assessor’s judgement
- Need to establish the requirements to be satisfied for a rating method to be valid
- Trade-off: assessor’s judgement driven by checklists
Phase 1: Supplier’s Capability Determination

Project implementation

post-assessment activities

elope rating (final)

For each process assessed, assign a rating to each process attribute

Record the set of process attribute ratings as the process profile and calculate the capability level rating

Report the results

Prepare the assessment report

Present the assessment results

Finalize and distribute the assessment report
Phase 1: Supplier’s Capability Determination

Phase 1 Outcomes (I)
Phase 1 Outcomes (II)

**Trends**
- Requirement analysis as a key issue
- Awareness of the customer role in the acquisition process
- Need for new SW development models

**Trade-offs**
- Platform-oriented vs customer-oriented
- Resource (memory size, processor performance, design complexity) saving vs maintainability and reliability

**Open issues**
- Interoperability at subsystem level (ECU)
- Safety and security implications
Phase 2: Monitoring Plan Definition

Phase 2: Objectives

This phase aims at defining a plan for monitoring a software project at different development phases to obtain quantitative measurements of the quality of the related work products and perform predictive evaluations of the quality of the final product.

For this purpose, a sample project is selected and used to identify key processes to be assessed in order to derive their capability and define an evaluation plan for achieving quantitative data.

The plan provides structured joint reviews and a set of characteristics and metrics along with the correspondent expected values.
Phase 2: Monitoring Plan Definition

Identification of Key Processes for Monitoring

- Requirements Elicitation and Analysis
- Software Design
- Coding
- Software Testing

Motivation

- Common milestones of the software process of most FIAT Auto’s suppliers
- Correspondence with the Assessment Scope of the Phase 1. A relevant amount of information has been already collected
Selection of the Pilot Supplier

Adopted Criteria for the selection of a pilot project:

- High capability levels resulting from Phase 1 in order to get confidence in suitable work products
- Medium-small dimension of the project (100-150 Kloc)
- Development process at an appropriate stage
- Belonging to the Body Computer/Comfort Electronics business area to maintain the same application domain as Phase 1
Quality Evaluation Methodology

Phase 2: Monitoring Plan Definition

ISO 9126

- Functionality
  - Suitability
  - Interoperability
- Usability
  - Accuracy
- Reliability
  - Maturity
- Efficiency
  - Analyzability
- Maintainability
  - Testability
- Portability
  - Changeability
  - Coexistence

1. Requirements Analysis tools
2. Software Design analysis tools
3. Coding verification tools
4. Software Testing Analysis tools
Phase 2: Monitoring Plan Definition

Monitoring Techniques and Tools

- Requirements analysis => Ambiguity and Expressiveness analysis made by means of the QuARS tool
- Software Design analysis => Checklists + QA-C tool
- Coding Style => SPLINT / QAC MISRA tools
- Software Testing analysis => Checklists
Phase 2: Monitoring Plan Definition

Requirements Analysis Tool: QuARS

Syntax Parser

Parsed.txt

Lexical Analysis

Syntactic Analysis

Views derivation

Indicator-related dictionaries

Domain dictionaries

Sentences.txt

Logs

Graphics

January 26th 2004

ASIS Intl. Conference
Phase 2: Monitoring Plan Definition

Requirements Analysis

- Suitability evaluation: the presence of potential ambiguity and vagueness defect in the requirements is measured.
- Testability evaluation: the requirements testability is evaluated by identifying requirements expressed in a non-imperative way, being too much complex or difficult to be understood.
Phase 2: Monitoring Plan Definition

Software Design analysis tools

- QA-C MISRA
- Checklists aiming at verifying:
  - The completeness and precision of the software architecture design and interfaces
  - The documentation of the software units and interfaces
  - The definition of test requirements
  - The satisfaction of software design requirements

- Interoperability evaluation: the accuracy and precision of the component’s interfaces description is evaluated.
- Changeability evaluation: the degree of modularity of the software.
- Co-existence evaluation: the completeness of the component’s interfaces description is evaluated.
Phase 2: Monitoring Plan Definition

Software Coding analysis tools

- SPLINT
- QA-C MISRA
- Checklists aiming at verifying:
  - The conformity to the best practices in software coding
  - Accuracy evaluation: the data type definition is checked out.
  - Maturity evaluation: programming errors are measured
  - Analyzability evaluation: the readability of the code and the degree of explanatory information provided in it is measured.
  - Changeability evaluation: the readability of the code is measured.
Phase 2: Monitoring Plan Definition

Software Testing analysis tools

- Checklists aiming at verifying:
  - The development of test cases covering the software requirements
  - The existence and the application of a regression test strategy
  - The existence and application of an integration testing strategy
  - The understandability and completeness of test logs

- Maturity evaluation: test adequacy and fault detection metrics are calculated.
- Analyzability evaluation: the accuracy and the completeness of test logs is evaluated.
Phase 2: Monitoring Plan Definition

Definition of the measurement scale and profiles

The measurement scale is common for all the sub-characteristics to be evaluated:

- **T**: top (the sub-characteristic has to reach the top score in all the related measurements)
- **H**: high (the sub-characteristic has to reach at least 75% of the top score)
- **M**: medium (the sub-characteristic has to reach at least 25% of the top score)
- **N**: not relevant

The collection of the evaluation results of the sub-characteristics (resulting profile) is compared with the expected profile.
Phase 3: Objectives

The third phase of the ESCAPE project aims at validating the evaluation plan defined in the previous phase, by providing a general methodology to allow FIAT Auto to monitor in a quantitative way a supply during the development process and ask for possible corrective actions earlier.

Possible critical factors in Phase 3:

- it takes a long time, especially in the verification of quality characteristics such as reliability or maintainability;
- it needs a comparison between products having a different metrics profiles in order to determine if and which correlation exists between metrics and quality;
- it needs a large set of product quality reports to achieve a sound statistic evaluation.
Phase 3: Validation of the Methodology

Validation mechanism

- Expected Profile
- Resulting Profile

SW Supplier’s Development Process

Final Product

Ex-Post Evaluation

Product’s Quality Records

Product’s Quality Expectations

Compliance Comparison

OK

NOK

- Inadequate expected profile
- Inadequate metrication plan
Thank you.
Questions?

giuseppe.lami@isti.cnr.it
fabrizio.fabbrini@isti.cnr.it
mario.fusani@isti.cnr.it
edoardo.sivera@fiat.com