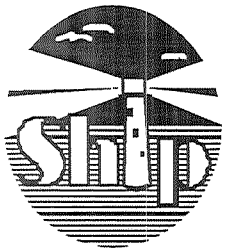

SHIP - Assessment of the Safety of Hazardous Industrial Processes in the Presence of Design Faults

DRAFT
SHIP Partners Only

SHIP/IEI/032/v0.1 *27 May 1994*

A software engineering framework for software safety claims

Franco Mazzanti, IEI-CNR

The SHIP project (ref. EV5V 103) is being carried out with financial support from the EEC in the framework of the Environment Programme, sub-theme: Major Industrial Hazards.

Abstract:

This document is intended to contribute to the development of the SHIP safety case by presenting a possible line of reasoning for the organization of software safety claims. Sections from 3 to 6 aim at the illustration of a generic picture of the expectable difficulties in the development of correct software and related solutions (Section 6 is the one which probably needs more work). Initially, drawing this general picture was the main goal of this report. During this writing, it has become evident that a design of a full picture including an evaluation of the effectiveness of all the mentioned methodologies is a too complex task. Therefore, while preserving its usefulness as a global refernce schema, this picture should not be expected to produce usable numerical inputs for the evaluation of the transition probabilities in the SHIP safety case.
Section 7, which is probably the most interesting from the SHIP point of view, investigates a possible way to formally structure and organize the reasonaing. This part is still in an extremely draft form, and will be improved in the next months.
The overall English style (sorry for the current one) also will be revised.

Date:	27 May 1994
Doc Type:	Technical Report
Doc. Id.:	SHIP/T/
Version:	v0.1
Release Status:	Draft
Availability Status:	SHIP Partners Only
Copyright:	1994, SHIP
Produced in Subtask[s]:	Task 2.3

Contents