

THE MEGAJOULE FACILITY

PERSONNEL SAFETY SYSTEM

M. Manson, CEA, Le Barp, France

DE LA RECHERCHE À L'INDUSTRI





The Laser MegaJoule (LMJ) is a 176-beam laser facility, located at the CEA CESTA Laboratory near Bordeaux (France). It is designed to deliver about 1.4 MJ of energy to targets, for high energy density physics experiments, including fusion experiments.

LMJ process hazards types are laser, high voltage, and radiations. These hazards are transmitted between bays.







For reliability reasons, the PSS is built around two independent systems named "BT1" and "BT2".

The BT1 system is designed using programmable technology, following IEC61508 requirements to achieve Safety Integrity Level 2.

The BT2 system is designed using non-programmable technology, following IEC61508 requirements to achieve SIL3. BT2 logic is built using PLANAR4 products from HIMA. While implemented using non-programmed logic technology, BT2 system functions are complex and require a software-like development process. BT2 simulator software helps following this process.



Functional view window shows process states, and allow manually triggering of any external signal. A functional view is available for each BT2 subsystem.

Test window allows selecting and running tests. Tests can be interrupted and run step by step. Manual test instructions can be generated.

Functional Model

tial class Simulateur SGAN

public override FonctionsDeSecurite RecupereFonctionsDeSecurite (

fonctions.Add(Fonction 02()) :

Securite Fonction 02()

action 02.Titre = "Interdiction d'accès HE pendant la période de refroidissement (hors SPR)"; on_02.Corps = "Le SGAP doit interdire les accès dans le HE pendant la période post-tir correspondant au \"refroidissement\" radiologique. "Cette période est définie, pour le système, comme celle comprise entre le tir effectif et l'insertion, par le Chef d'Installation, de sa clé " "dans le boitier d'Autorisation d'Accès HE, en dehors des périodes d'accès SPR." ; ction_02.Capteurs.Add(new Hypothese(this.CR_BAACI, EtatSignal.False)) ; conction 02.Capteurs.Add(new Hypothese(this.CR BAASPR, EtatSignal.False)) ; ion_02.Capteurs.Add(new Hypothese(this.CR_BAT, EtatSignal.Undefined)) conction 02.Capteurs.Add(new Hypothese(this.CR BAAHE, EtatSignal.Undefined)) . fonction_02.Capteurs.Add(new Hypothese(this.CR_BISGAP, EtatSignal.Undefined)); fonction_02.Actionneurs.Add(new Hypothese(this.AU_Acces_Sas_HE_1, EtatSignal.False)); fonction_02.Actionneurs.Add(new Hypothese(this.AU_Acces_Sas_HE_2, EtatSignal.False)) ; turn fonction_02 ;

Interdiction d'accès HE pendant la période de refroidissement (hors SPR)

Technical Model

ublic partial class Simulateur SGAP : Simulateu

public SimulateurPlanar4.RackPlanar R1;

public Signal CR_Ch01_EnService = new Signal("CR_Ch01_EnService", "La chaine N°01 est en service", "La chaine N°01 est hors service")

public Simulateur SGAP(String nom

R1 = AjouteRack("R1") ; R1.Description = "SGAP#1";

Wiring

Module42100 R1_M01 = new SimulateurPlanar4.Module42100("R1.M01") ; R1.Module01 = R1_M01;

R1_M02.F1_OUT = this.INT_CHAINE_01_EN_SERVICE ; R1_M02.F1_OUTINV = this.INT_NOT_CHAINE_01_EN_SERVICE ; R1_M02.F1_IN = this.CR_Ch01_EnService;

void Test_Fonctionnel_001_VerificationEtatInitial() void Test_Fonctionnel_002_VerificationEntreesNormales()

public partial class FormSGAP Test : FormTes

Testeur.NouveauTest("Vérification des accès nominaux") ; Testeur.Title("Acces normal dans les locaux gérés par le SGAP") Testeur.Trace("Aucune clé d'accès n'est sortie"); Testeur.Test(!SGAP.AU_Acces_Sas_HE_1, "Accès interdit par le sas HE n°1" , "AU_Acces_Sas_HE_1 = 0 ?"); Testeur.Trace("Distribution d'une clé d'accès HE"); SGAP.CR BG Acces HE = false :

Tests

Testeur.Test(SGAP.AU_Acces_Sas_HE_1, "Accès autorisé par le sas HE n°1" , "AU_Acces_Sas_HE_1 = 1 ?");

void Test_Fonctionnel_003_VerificationTirHESansConsequencesRadio()... void Test_Fonctionnel_004_VerificationTirHEAvecConsequencesRadio()... void Test Fonctionnel 005 VerificationDebrayage()...

Safety Requirements Specification

Automatically generated tests from functional model are not on site runnable. Some tests are hand-written. These tests are run on technical model. The same tests are then exported as blank test files for factory and site runs.

System tests (on site)

System tests (factory)

System Architecture

Subsystem logic design

Subsystem tests

Simulator allows designing logic and proving its compliance with specification. Simulator generates compliance checking document.

Simulator generates wiring specification documents.

Wiring tests

Being the base of the development process, the BT2 simulator has to be validated as a tool following IE-C61508 part 3.

This validation is currently in progress.

