

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 June 2001 (21.06.2001)

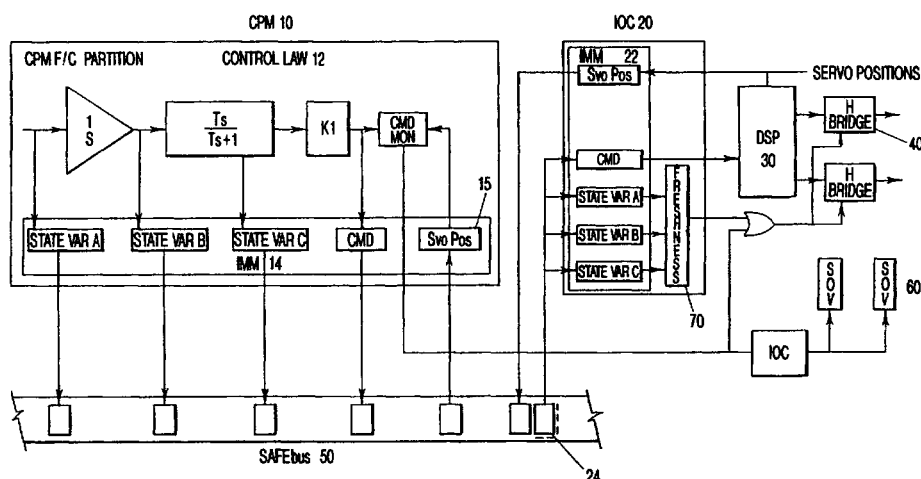
PCT

(10) International Publication Number
WO 01/44881 A1

- (51) International Patent Classification⁷: **G05B 9/02**, 9/03 [US/US]; 1604 Ranch Trail SE, Albuquerque, NM 87123 (US).
- (21) International Application Number: PCT/US00/33865
- (22) International Filing Date:
14 December 2000 (14.12.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/467,111 17 December 1999 (17.12.1999) US
- (71) Applicant (for all designated States except US): **HONEYWELL INTERNATIONAL INC.** [US/US]; 101 Columbia Road, P.O. Box 2245, Morristown, NJ 07960 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **BANNING, Ronald, Ray** [US/US]; 8216 Meadowbrook Avenue NW, Albuquerque, NM 87120 (US). **GOOSSEN, Emray, Rein**
- (74) Agents: **HOIRIIS, David** et al.; Honeywell International Inc., 101 Columbia Road, P.O. Box 2245, Morristown, NJ 07960 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:
— With international search report.

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR FAIL SAFE PROCESS EXECUTION, MONITORING AND OUTPUT CONTROL FOR CRITICAL SYSTEMS



(57) Abstract: Methods and systems for fail-safe process execution, monitoring and output control for critical systems operating on an open bus architecture with multiple, independent partitions on a single processor is presented. The control system state variables and their status of critical systems, within the control laws and mode logic, are monitored for process completion and health, and shut down if necessary. The embodiments provide for a dual path for shut down of, for example, flight critical systems so that the failure of one partitioned module does not affect the operation of the remaining partitioned modules. One path involves the CPM (10) and IOC (20) determination of command/response health. If persistent faults are detected, then either the DSP (30) monitoring or the CPM performance monitoring results in a discrete signal being sent to the H-bridge (40) disable (403) to shutdown the current output. The second path is CPM controlled via a separate discrete signal on the input/output controller (20) to the flight critical system shut-off valve (60). By implementing these separate paths, critical systems in one partition cannot be defeated by a single failure in another partition (102).



— Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.