Thiết kế hệ thống an toàn cho giàn khoan BK16 áp dụng phương pháp Grafcet

Designing Safety System for BK16 Based on Grafcet

Phan Thị Huyền Châu

Trường Đại học Bách khoa Hà Nội - Số 1, Đại Cồ Việt, Hai Bà Trưng, Hà Nội

Đến Tòa soạn: 02-10-2018; chấp nhận đăng: 18-01-2019

Tóm tắt

Quy trình công nghệ trên giàn khoan BK16 là nhằm mục đích xử lý dòng hỗn hợp khí gas-nước lấy được từ các giếng dầu, qua quá trình tách để tạo ra sản phẩm là dầu và khí đốt. Vì vậy trong môi trường này, các công trình trên biển là một môi trường rất dễ xảy ra các nguy hiểm cháy và nguy hiểm khí. Để đảm bảo an toàn cho con người và thiết bị trên đó cần phải thiết lập một hệ thống an toàn có độ tin cậy tuyệt đối, đảm bảo mức độ an toàn cho giàn khoan đạt mức SIL3 (safety integrity level). Nhiệm vụ chính của hệ thống an toàn là phải đảm bảo dầu thô, khí gas không bị rò rỉ và chủ động hạn chế những ảnh hưởng nếu xảy ra rò rỉ bằng cách đóng mở hàng loạt hệ thống các van xả, dừng quá trình(dừng tuyến), dừng khẩn cấp đồng thời giám sát các thông số trong quá trình tách pha của bình tách thông qua các cảm biến về áp suất và mức gắn trên bình. Để giảm thời gian thiết kế và rút ngắn thời gian, khối lượng lập trình hệ thống an toàn, phương pháp Grafcet trong lĩnh vực thiết kế logic được áp dụng do đặc điểm của hệ thống an toàn đều là điều khiển các van có cơ chế hoạt động ON-OFF.

Từ khóa: Điều khiển logic, Giàn khoan, Hệ thống an toàn, Grafcet

Abstract

The technology process in BK16 wellhead satelite platform is to separate the gas and the oil from gas-water mixture. Therefore, the contruction in BK16 is very dangerous due to the flammable and exposive posibility. In order to ensure the safety for people and equipment, it is obligation to set up the the safety system with absolute reliability and satisfies SIL 3 – safety level for BK16. The main function of this system guarantees that crude oil and gas are not leak, and if there has a leak the system will be reacted by closing or opening a series of valves such as. blowdown valve, process shutdown valve, emergency shutdown valve and monitoring the signals from level and presure sensors of production separate tank to minimize losses. To reduce design time and programming, Grafcet method is applied because of the characteristics of safety system is to control many of ON-OFF valves.

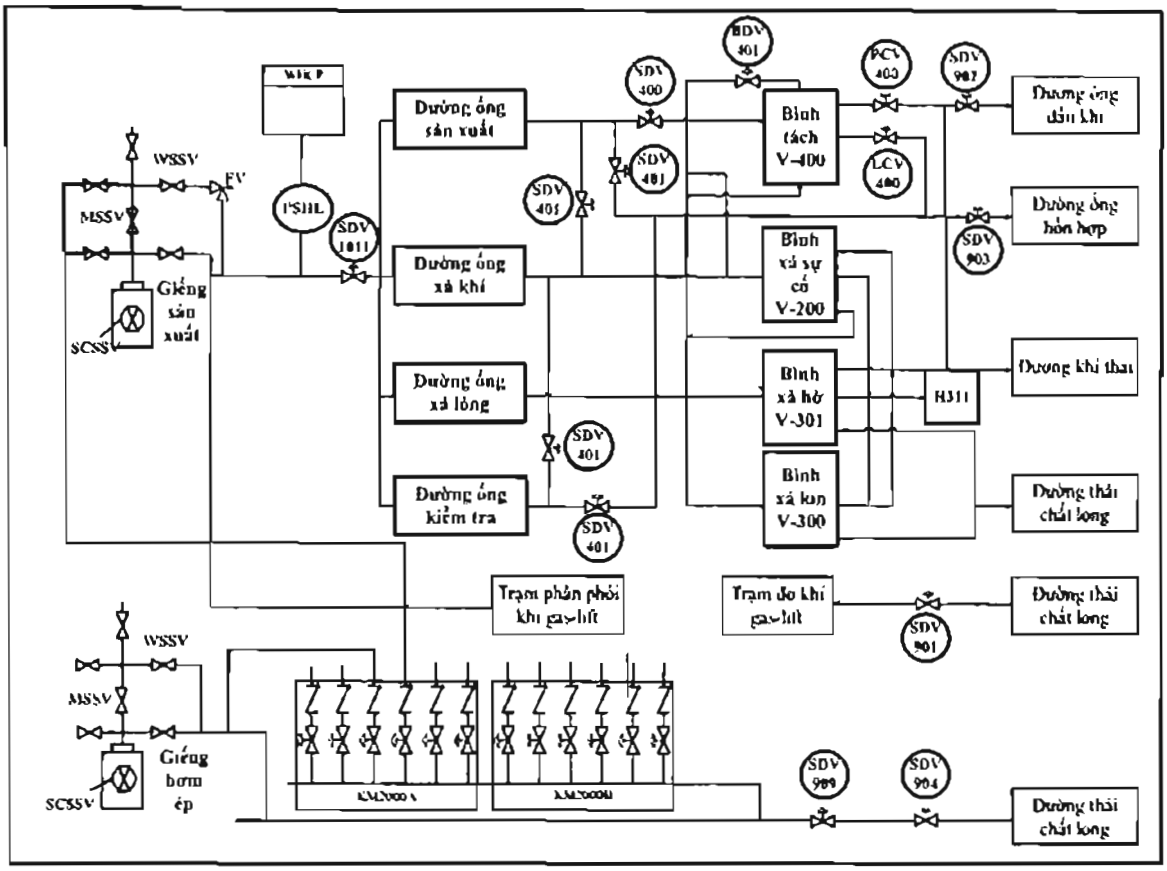
Keywords: Logic design, Offshore platform, Safety system, Grafcet

1. Đặt vấn đề

Các hệ thống sản xuất ngày nay không ngừng gia tăng về kích thước và độ phức tạp để đáp ứng nhu cầu ngày càng cao về năng lượng, hàng hóa và thực phẩm của xã hội. Cùng với đó sẽ xuất hiện những nguy cơ và rủi ro cần phải được ngăn ngừa và giảm nhẹ ảnh hưởng của chúng đến lợi ích kinh tế cũng như con người. Một hệ thống công nghiệp là một hệ thống mang tính chất động và các thuộc tính của nó không những chỉ phụ thuộc vào các thành phần bên trong nó mà còn phụ thuộc vào mối quan hệ giữa chúng, do đó để đánh giá an toàn vận hành cần một phương pháp tiếp cận có hệ thống. Phương pháp phân tích sự cố là một phương pháp thường được sử dụng trong thiết kế hệ thống an toàn, đặc biệt là đối với các quá trình đặc biệt nguy hiểm như quá trình sản xuất, quá trình khai thác dầu khí [1-4] và [7].

Việc thiết kế hệ thống an toàn cho giàn khoan dựa trên các yêu cầu đưa ra theo tiêu chuẩn IEC 61508. Chương trình điều khiển hệ thống an toàn thường được thiết kế sử dụng ngôn ngữ Ladder kết hợp với FBD trong lập trình cho PLC dựa theo bảng phân tích nguyên nhân kết quả. Tuy nhiên quá trình thiết kế an toàn cho giàn khoan đòi hỏi phải kết nối nhiều tín hiệu từ các thiết bị điều khiển, thiết bị đo và các thiết bị an toàn như còi, đèn, nút ấn dừng và dừng khẩn cấp. Việc sử dụng ngôn ngữ Ladder/FBD trong lập trình khiến cho chương trình cồng kềnh, không ứng dụng được các cấu trúc [illegible] song hành để giảm thời gian xử lý. Khi sử dụng ngôn ngữ lập trình SFC (Sequential Function Chart) [illegible] trên sẽ được giải quyết một cách triệt

* Địa chỉ liên hệ: Tel.: (+84) 917921581
Email: chau.phanthihuyen@hust.edu.vn



Hình 1. Sơ đồ tổng quan hệ thống khai thác dầu và khí.

Ngôn ngữ lập trình SFC được xây dựng dựa trên phương pháp thiết kế logic Grafcet. Nó là một cách tiếp cận được sử dụng nhiều trong điều khiển logic như một ngôn ngữ lập trình trong các bộ PLC, là một ngôn ngữ mô phỏng tiêu chuẩn do nó không chỉ cho phép mô phỏng đầu vào/ra và các mối quan hệ trong hệ thống mà còn mô phỏng được các sự kiện đồng thời và đồng bộ hóa [5]. Grafcet không chỉ thể hiện về mặt các mối quan hệ về mặt logic (giống như ngôn ngữ FBD đang sử dụng trong thiết kế ở giàn khoan) mà còn chỉ rõ các mối quan hệ liên kết về mặt vật lý nên giúp cá người thiết kế và sử dụng có hình dung rất trực quan về hệ thống. Riêng về thiết kế thì giảm thời gian lập trình vì khi thiết lập được Grafcet có nghĩa là có thể viết chương trình cho PLC thông qua ngôn ngữ SFC mà không cần viết hàm để lập trình như với ngôn ngữ FBD hay Ladder, dẫn đến giảm thời gian thiết kế, giảm thời gian xử lý sự cố. Điều này rất quan trọng trong thiết kế an toàn để đáp ứng tiêu chuẩn an toàn IEC 61508-3 dành cho phần mềm. Ngoài ra việc mô phỏng hệ thống sử dụng Grafcet/SFC cho phép cấu trúc các nhiệm vụ phức tạp thành các đơn vị nhỏ hơn và đồng bộ hóa các cấu trúc nhỏ này nhằm tăng tính linh hoạt của hệ thống, dễ dàng cho người sử dụng phát hiện ra lỗi ở chính xác đầu trong các chương trình nhỏ thay vì cả chương trình lớn như ở lập trình sử dụng FBD.

Bài báo này trình bầy quy trình thiết kế hệ thống an toàn cho giàn khoan khai thác dầu khí BK16 và mô phỏng ứng dụng điều khiển logic dựa trên phương pháp Grafcet, từ đó tiến tới lập trình sử dụng ngôn ngữ lập trình SFC. Nội dung của bài báo gồm các phần chính như sau: đặt vấn đề, giới thiệu tổng quan về giàn khoan BK 16, thiết kế hệ thống an toàn, thiết kế mô phỏng kiểm nghiệm tính đúng đắn của hệ thống sử dụng GRAFCET và kết luận.

2. Tổng quan về giàn khoan BK16.

Giàn khoan BK16 thuộc sở hữu của Vietsopetro J.V-Việt Nam và được giao nhiệm vụ khoan và vận hành khai thác dầu mỏ từ mỏ Bạch Hổ nằm trên thềm lục địa phía Nam của Việt Nam.

Phương thức hoạt động của giàn khoan BK16 như hình 1. Chất lưu từ 9 giếng sản xuất đi theo chín đường tương ứng đến cụm phân dòng đầu vào để đưa ra bốn đường ống: sản xuất, kiểm tra, xả khí và xả lỏng để tách riêng khí gas, dầu thô và tạp chất. Các giếng sản xuất được điều khiển đóng mở bởi cụm ba van SCSSV, MSSV, WSSV và một van tiết lưu kí hiệu là FV. Giếng bơm ép cũng thiết kế các cụm van như giếng sản xuất.

Nhiệm vụ chính của bốn đường ống trong hệ thống khai thác dầu như sau:

- Đường ống sản xuất (Production Header): nhận dầu thô từ giếng khai thác đưa vào bình tách V-400 để tách hai pha lỏng khí hoặc đi thẳng (by pass) ra các thùng chứa để đưa về đất liền khi bình tách có sự cố cần cách ly.

- Đường ống kiểm tra (Test Header): sử dụng khi cần đo thông số của các giếng riêng biệt. Khi đó giếng cần đo sẽ theo đường ống sản xuất đi vào bình tách V-400, các giếng còn lại theo đường ống kiểm tra đi thẳng ra thùng chứa.

- Đường ống xả khí (Vent Header): làm giảm bớt áp suất gas xả ra của các van xả khí BDV từ các đường ống sản xuất và đường ống kiểm tra được đưa tới bình xả sự cố (Vent Scrubber V-200) khi có sự cố

- Đường ống xả lỏng (Drain Header): xả chất lỏng từ các đường ống hở trên giàn khoan và được đưa về bình xả hở V-301, xả chất lỏng từ cụm phân dòng đầu vào, bình tách V-400, bình xả sự cố V-200 về bình xả kín V-300.

Trên các đường ống như sản xuất, xả khí, xả lỏng và kiểm tra đều có công tắc (switch) PSHL và van dừng nhánh SDV để khi áp suất trên các đường ống nằm ngoài dải cho phép (10-47 bar) thì công tắc này sẽ tác động để xả khí và đóng van SDV. Riêng với các bình chứa trên giàn khoan thì bình tách là thiết bị quan trọng cần phải điều khiển mức và điều khiển áp suất nên có thêm van điều khiển áp suất PCV và điều khiển mức LCV.

Ngoài ra ở đường ống sản xuất và đường ống thải lỏng sau mỗi van dừng nhánh SDV sẽ có thêm van điều khiển bằng tay HV để đảm bảo thêm mức độ an toàn cho các đường ống này

Hệ thống phụ trợ phân phối khí gaslift dùng để cung cấp khí gas xuống các giếng khai thác dầu thông qua trạm phân phối khí gaslift và đo các thông số (áp suất, nhiệt độ, lưu lượng) của khí gas được phân phối đó thông qua trạm đo khí gas nhằm mục đích bơm khí xuống để nổi dầu lên đưa vào bốn đường ống phân phối và loại bỏ sự tích tụ kết tủa trong đường ra của khí gas từ bình tách.

Hệ thống phụ trợ bơm nước ép vỉa có nhiệm vụ bơm nước xuống các giếng dầu để rửa đường ống chứa dầu và khí còn lại một phần được trích ra đưa đến cụm Kill Manifold KM2000A, KM2000B để dập giếng khi có sự cố (do khi khai thác dầu thô thì dầu nhẹ nổi lên trên mặt nước nên phải đề phòng cháy nổ, dập nước bằng các vòi phun khi có cháy ở giếng) .

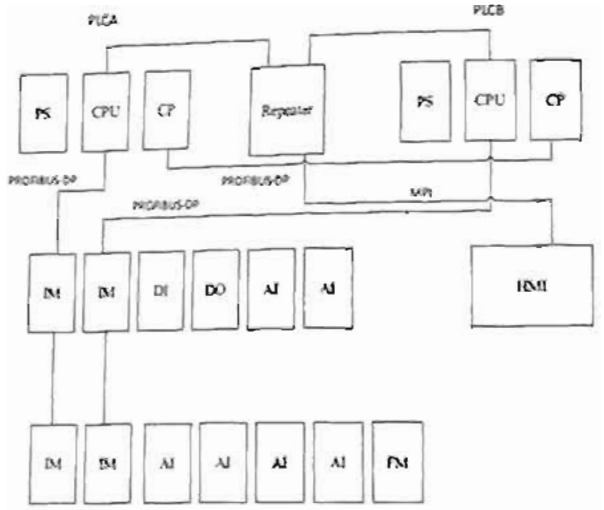
Hiện nay trong việc thiết kế điều khiển an toàn cho giàn khoan, phần lập trình điều khiển sử dụng số lượng các chương trình con rất lớn do dùng ngôn ngữ lập trình FBD, ảnh hưởng đến phần truyền thông và tác động nhanh của hệ thống an toàn. Đây là hai khó khăn trong thực tế tại giàn khoan BK16.

3. Thiết kế an toàn cho giàn khoan.

3.1 Thiết kế phần cứng.

Thiết bị sử dụng trên giàn khoan phải đáp ứng các tiêu chuẩn quy định về an toàn (IEC 65108 part 2 cho phần cứng) trong môi trường nguy hiểm. Do đó cần chọn PLC với chuẩn an toàn (safety PLC) được thiết kế đặc biệt, được chứng nhận đáp ứng các yêu cầu về an toàn (SIL3). Sự khác biệt chính giữa PLC thường và PLC an toàn là sự xuất hiện của cơ chế dự phòng và tự kiểm tra. Một điểm khác biệt quan trọng khác nằm ở đầu vào/ra của PLC an toàn. Ở đầu vào, PLC an toàn liên tục theo dõi trạng thái đầu vào để phát hiện các sự cố xảy ra trong dây chuyền. Đầu ra có thêm mạch an toàn giữa đầu ra và thiết bị kết nối để hạn chế thiệt hại cho thiết bị bên ngoài.

Hệ thống an toàn cần phải được trang bị các modul dự phòng đảm bảo khi một mô-đun bị lỗi hệ thống sẽ tự động chuyển đổi sang thiết bị dự phòng giúp quá trình sản xuất diễn ra liên tục.



Hình 2. Cấu trúc phần cứng của thiết kế an toàn.

Hình 2 là sơ đồ kết nối hệ thống dự phòng cho toàn bộ hệ thống (redundant control system). Các mô-đun được kết nối trên 3 giá đỡ. Trên giá đầu tiên là 2 bộ mô-đun giống nhau bao gồm: nguồn (PS), CPU và mô-đun truyền thông (CP) gọi tắt là PLC A và PLC B cùng với 1 bộ "RS-485 repeater". Giá thứ hai là 2 mô-đun mở rộng (IM), mô-đun đầu vào số, đầu ra số và 2 mô-đun đầu vào tương [illegible] giá đỡ thứ 3 là 2 mô-đun mở rộng (IM), 4 mô- [illegible] vào tương tự và mô-đun có chức năng đặc biệt [illegible]). CPU của PLC A kết nối với mô-đun IM thứ nh [illegible]ên giá 2 và IM thứ nhất giá 3 thông qua cáp RS- [illegible] tương tự như vậy với PLC B. CPU trong PLC A [illegible] hệ truy cập dữ liệu tới các mô-đun được kết nối [illegible] giá 2 sử dụng mô-đun IM. Cũng như vậy nó có [illegible] truy cập dữ liệu vào các mondun mở rộng trên giá [illegible] ng tự với PLC B. Chúng ta cũng có 1 mạng [illegible] bus cho mô-đun [illegible] thông (CP) để truyề [illegible] liệu giữa CPU. MPI được sử dụng tru [illegible] liệu giữa PLC A

và B với màn hình HMI. Mạng này được kết nối từ các cổng MPI của 2 CPU tới đầu vào của Repeater và từ đầu ra của Repeater tới màn hình HMI.

3.2 Thiết kế phần mềm và các yêu cầu đối với thiết kế phần mềm cho hệ thống an toàn.

Sự khác nhau giữa thiết kế logic thông thường và thiết kế an toàn ứng dụng điều khiển logic thể hiện trong các nội dung như sau:

- Tự động dừng khẩn cấp đối với các quá trình và thiết bị tại các giá trị tới hạn đồng thời gửi tín hiệu tới các hệ thống khác nhau.

- Cung cấp khả năng chuẩn đoán và kiểm tra từ xa.

- Cung cấp chức năng tự phát hiện và truyền tín hiệu về lỗi nội bộ.

- Khi có sự cố, hệ thống sẽ đánh giá được mức độ nguy hiểm để người vận hành đưa ra các quyết định dừng trên giàn khoan để tránh thiệt hại nặng nề về người theo sự phân cấp về mức độ nguy hiểm như sau:

1. Dừng thiết bị (unit shutdown).

2. Dừng từng giếng riêng biệt (individual well shutdown).

Dừng thiết bị và dừng từng giếng riêng biệt thực hiện khi hệ thống có lỗi chưa được liệt vào mức độ nguy hiểm của hệ thống an toàn.

3. Dừng quá trình (Process Shutdown- PSD): mức độ nguy hiểm ít nhất, là quá trình dừng toàn bộ quá trình mà không làm giảm áp suất.

4. Dừng khẩn cấp mức thấp (Emergency Shutdown – Low level ESD-L): mức độ nguy hiểm thứ ba.

5. Dừng khẩn cấp mức cao (Emergency Shutdown – High level ESD-H): mức độ nguy hiểm thứ hai.

6. Rời bỏ giàn khoan (Abandon Platform Shutdown ESD-A): mức độ nguy hiểm nhất của giàn khoan. Dừng rời bỏ giàn khoan là mức cao nhất trong hệ thống an toàn khi sự cố vượt quá tầm kiểm soát. Toàn bộ hệ thống trên giàn khoan cần được dừng lại chỉ một vài hệ thống cảnh báo và chiếu sáng được giữ lại phục vụ hoạt động sơ tán khỏi giàn.

- Đảm bảo tiêu chuẩn an toàn IEC 61508 part 3 dành cho phần mềm khi thiết kế hệ thống an toàn.

3.3 Phân tích các nguyên nhân- tác động của quá trình dừng và phân cấp mức độ nguy hiểm

Việc tìm mối quan hệ giữa các nguyên nhân và tác động đi kèm là bước bắt buộc phải có trước khi lập trình cho hệ thống an toàn.

3.3.1. Dừng các giếng riêng biệt

Dừng quá trình xảy ra khi có một trong các tín hiệu sau:

Trường hợp 1

Nếu có tín hiệu từ nút nhấn ảo tại trạm làm việc tương ứng với giếng muốn dừng thì hệ thống sẽ thực hiện đóng van MSSV, WSSV.

Trường hợp 2

Nếu có 2 trong 3 tín hiệu áp suất trong giếng ở mức cao thì hệ thống thực hiện việc đóng van MSSV, WSSV, SDV.

Trường hợp 3

Nếu áp suất sau van tiết lưu cao/thấp thì hệ thống thực hiện việc đóng van MSSV, WSSV, SDV, SCSSV.

3.3.2. Dừng thiết bị

Dừng thiết bị xảy ra khi có một trong các tín hiệu sau:

Trường hợp 1:

Nếu có một trong các sự cố sau

- Mức chất lỏng bình Vent Scrubber rất thấp.

- Mức chất lỏng bình xả kín rất thấp.

- Mức chất lỏng bình xả hở rất thấp.

- Áp suất đầu ra của bơm xả rất cao.

thì hệ thống sẽ cho dừng bơm xả.

Trường hợp 2

Nếu mức chất lỏng bể chứa hóa chất giảm nhiệt, đô đông đặc rất thấp thì hệ thống sẽ thực hiện việc đóng toàn bộ van đường khí nén tới bơm H-700A1-01 tới H-700A1-11.

3.3.3. Dừng quá trình

Dừng quá trình xảy ra khi có một trong các tín hiệu sau:

Trường hợp 1

- Áp suất bình tách V-400 rất cao hoặc rất thấp.

- Áp suất đường khí Gas rất cao hoặc rất thấp.

- Áp suất đường hỗn hợp khí và dầu rất cao hoặc rất thấp

- Mức chất lỏng trong bình tách rất cao hoặc rất thấp.

- Mức chất lỏng trong bình lọc V-200 rất cao.

Tác động tới hệ thống công nghệ như sau:

- Dừng van MSSV, WSSV, SDV.

- Đóng van SDV 400, PCV 400, LCV 400.

- Đóng van SDV 800, SDV 802.

- Đóng van FV 811-819, XY 711-721, XY 761-771.

- Dừng máy bơm H-311.

Trường hợp 2

- Nút nhấn trên bảng điều khiển của hệ thống phát thanh/cảnh báo Public adress/General alarm (PA/GA) kích hoạt dừng quá trình.

- Nút nhấn tại trạm làm việc trong phòng điều khiển trung tâm.

- MANUAL CALL-POINT tại thang gần đầu giếng khoan (phía Đông và Tây).

Tác động tới hệ thống công nghệ như sau như trong trường hợp 1 cùng với tác động:

- Tạo báo động tại phòng điều khiển trung tâm (CCR) trên giàn khoan.

- Kích hoạt báo động dừng quá trình.

3.3.4. Dừng khẩn cấp mức thấp

Dừng khẩn cấp mức thấp xảy ra khi có một trong các tín hiệu sau:

Trường hợp 1

- Phát hiện 50% LEL Gas từ 2 đầu dò khí trở lên trong khu vực xử lý Zone1 (Khu vực 1 bao gồm các không gian nền nơi có các thiết bị quá trình đặt liền kề với đầu giếng khoan).

- Nút nhấn trên hệ thống PA/GA để kích hoạt để kích hoạt dừng khẩn cấp mức thấp

Tác động tới hệ thống công nghệ như sau:

- Tạo báo động tại CCR, trên giàn khoan

- Kích hoạt báo động dừng khẩn cấp mức thấp.

- Dừng van MSSV, WSSV, SDV.

- Mở van BDV 1001, BDV 1002.

- Đóng van SDV 400, PCV 400, LCV 400.

- Đóng van SDV 800, SDV 802.

- Mở van BDV 401, BDV 801

- Đóng van FV 811-819, XY 711-721, XY 761-771.

- Dừng máy bơm H-311.

Trường hợp 2

- Phát hiện cháy từ 2 đầu báo cháy trở lên trong khu vực xử lý (Zone 1)

- Nút nhấn trên hệ thống PA/GA để kích hoạt dừng khẩn cấp mức thấp.

Tác động tới hệ thống công nghệ như sau. tác động như trong trường hợp 1 cùng với tác động dừng máy phát AU-AE-01, AU-AE-02

Trường hợp 3

-Tín hiệu dừng khẩn cấp báo cháy từ hệ thống dễ nóng chảy.

Tác động tới hệ thống công nghệ như sau: tác động như trong trường hợp 2 cùng với tác động đóng van SCSSV.

3.3 5. Dừng khẩn cấp mức cao

Dừng khẩn cấp mức cao xảy ra khi có một trong các tín hiệu sau:

- Phát hiện cháy từ 2 đầu báo cháy trở lên trong khu vực xử lý (Zone 2: Khu vực 2 là khu vực có nguồn điện chính và khẩn cấp, phòng điều khiển, chỗ ở)

- Nút nhấn ảo tại trạm làm việc trong phòng điều khiển trung tâm.

- Nút nhấn tại thang gần đầu giếng khoan (phía Đông và Tây).

- Nút nhấn tại bình rửa di động.

- Nút nhấn trên hệ thống PA/GA để kích hoạt dừng khẩn cấp mức cao.

- Nút nhấn FM-200.

- Phát hiện 25% LEL Gas từ 2 đầu dò khí trở lên trong khu vực xử lý (Zone2).

- Nút nhấn tại trạm làm việc trong phòng điều khiển trung tâm

- Nút nhấn tại thang gần đầu giếng khoan (phía Đông và Tây).

- Nút nhấn tại bình rửa di

- Nút nhấn trên hệ thống PA/GA để kích hoạt dừng khẩn cấp mức cao.

Tác động tới hệ thống công nghệ như sau:

- Tạo báo động tại CCR, t[illegible]ian khoan.

- Kích hoạt báo động dừn[illegible] cấp mức cao.

- Dừng van MSSV, WSS[illegible]V

- Mở van BDV 1001, BD[illegible]5

- Đóng van SDV 400, PC[illegible] LCV 4[illegible],

- Đóng van SDV 800, SDV 802.

- Mở van BDV 401, BDV 801.

- Đóng van FV 811-819, XY 711-721, XY 761-771.

- Dừng máy AU-AE-01, AU-AE-02, H-311.

3 3.6. Rời bỏ giàn khoan

Đây là mức độ khẩn cấp cao nhất có thể xảy ra trên giàn khoan

Mức độ rời bỏ giàn khoan xảy ra khi có một trong các tín hiệu sau:

Trường hợp 1

- Nút nhấn báo động rời bỏ giàn khoan bị tác động: khu vực hạ cánh/nơi neo tàu LANDING\MOORING PLATFORM ở khu vực phía tây và phía đông.

- Nút nhấn rời bỏ giàn khoan trên tủ PA/GA bị tác động gửi tín hiệu sang.

Tác động tới hệ thống công nghệ như sau:

- Tạo báo động tại CCR, CCR2, trên giàn khoan.

- Kích hoạt báo động rời bỏ giàn khoan.

- Đóng toàn bộ các van SCSSV, MSSV, WSSV, SDV của 9 giếng.

- Mở van BDV 1001, BDV 1002.

Trường hợp 2

- Nút nhấn tại trạm tàu cứu hộ, khu vực tập trung.

- Nút nhấn trên bảng điều khiển PA/GA kích hoạt dừng khẩn cấp-rời bỏ giàn khoan.

- Phát hiện 20% LEL GAS từ 2 đầu dò khí trở lên trong khu vực xử lý (Zone 2).

Tác động tới hệ thống công nghệ như sau:

- Đóng van SDV 400, PCV 400, LCV 400.

- Đóng van SDV 800, SDV 802.

- Mở van BDV 401, BDV 801.

- Đóng van FV 811-819, XY 711-721, XY 761-771.

- Dừng máy nén khí AU-AE-01, AU-AE-02, H-311.

Trường hợp 3

- Nút nhấn ảo tại trạm làm việc trong phòng điều khiển

- Nút nhấn tại khu vực hạ cánh máy bay.

Tác động tới hệ thống công nghệ như sau: tác động gộp cả trường hợp 1 và trường hợp 2.

3.4. Ứng dụng Grafcet để lập trình điều khiển

Grafcet là từ viết tắt của tiếng Pháp "Graphe fonctionnel de commande étape transition" là một đồ hình chức năng cho phép mô tả các trạng thái làm việc của hệ thống và biểu diễn quá trình điều khiển với các trạng thái chuyển biến từ trạng thái này sang trạng thái khác [8]-[9], đó là một Graph định hướng và được xác định bởi các phần tử sau:

$G := \{E, T, A, M\}$

Trong đó:

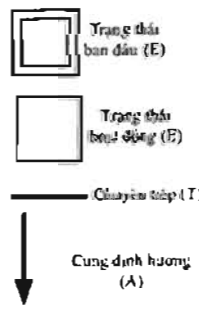
$E = \{E_1, E_2, \ldots, E_m\}$ là tập hữu hạn các trạng thái (giai đoạn) của hệ thống. Mỗi trạng thái tương ứng với những tác động nào đó của phần điều khiển và trong một trạng thái các hành vi điều khiển là không đổi Một trạng thái có hai khả năng là hoạt động và không hoạt động. Điều khiển chính là thực hiện các mệnh đề logic chứa các biến vào và các biến ra để hệ thống có được một trạng thái xác định trong hệ và đó cũng chính là một trạng thái Grafcet.

$T = \{t_1, t_2, \ldots, t_p\}$ là tập hợp hữu hạn các chuyển tiếp (chuyển trang thái). Hàm Bool gắn với một chuyển tiếp được gọi là "một tiếp nhận". Giữa hai trạng thái luôn luôn tồn tại một chuyển tiếp.

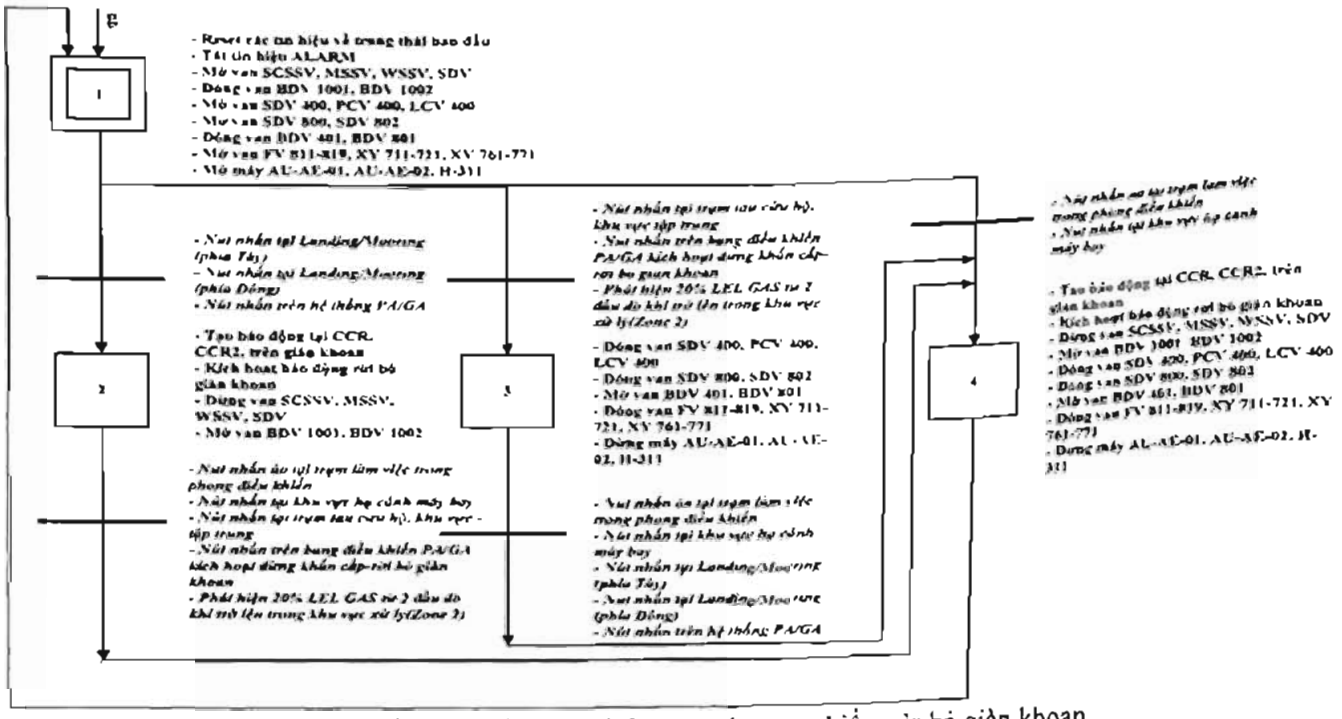
$A = \{a_1, a_2, \ldots, a_n\}$ là tập các cung định hướng nối giữa một trang thái này với một chuyển tiếp hoặc giữa một chuyển tiếp và một trạng thái.

$M = \{m_1, m_2, \ldots, m_n\}$ là tập các giá trị 0 và 1. Nếu $m_i = 1$ thì trạng thái i là hoạt động, nếu $m_i = 0$ thì trạng thái i là không hoạt động.

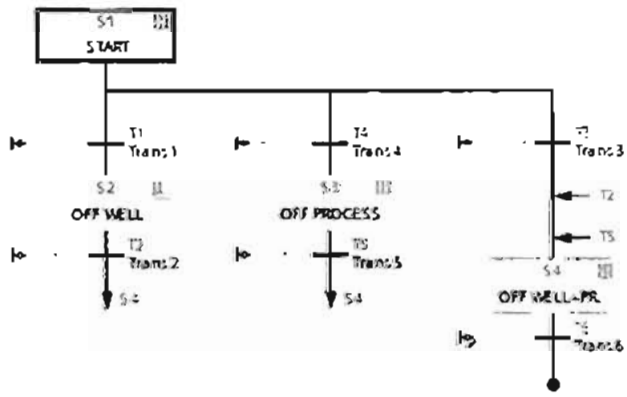
Do giới hạn về độ dài của bài báo nên tác giả chỉ lập biểu diễn mô tả Grafcet cho trường hợp dừng khẩn cấp mức rời giàn ESD-A, các mức khẩn cấp khác hoàn toàn tương tự. Các tín hiệu ở đây sẽ được định nghĩa là các chuyển tiếp, các tác động là trạng thái



Hình 3. Kí hiệu trong Grafcet.



Hình 4. Grafcet cho chương trình con mức nguy hiểm rời bỏ giàn khoan



Hình 5. SFC cho mức nguy hiểm rời giàn.

4. Mô phỏng kiểm chứng: sử dụng ngôn ngữ lập trình SFC.

Ngôn ngữ lập trình biểu đồ bàm tuần tư SFC là một công cụ rất mạnh trong miêu tả cấu trúc của hệ thống điều khiển tuần tự [6] SFC được phát triển từ ngôn ngữ Grafcet, một công cụ đồ họa để miêu tả chuỗi hành động.

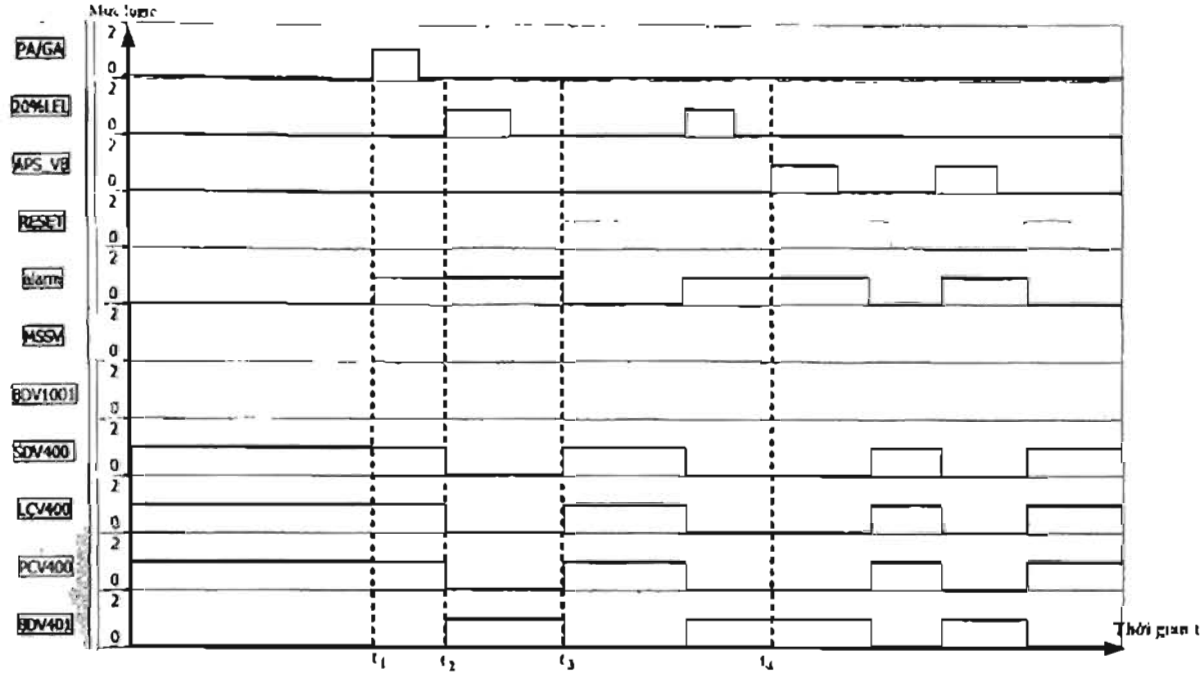
Ưu điểm của ngôn ngữ SFC là một công cụ mạnh trong lập trình các hệ thống tuần tự, đặc biệt là khi thiết kế sử dụng phương pháp Grafcet. Vì hệ thống điều khiển an toàn cho giàn khoan có rất nhiều tín hiệu vào ra và các các quá trình xảy ra chậm vì vậy ngôn ngữ lập trình SFC được lựa chọn giảm thời gian lập trình và khối lượng câu lệnh lập trình. Hình 5 là mô hình chuyển đổi từ Grafcet sang SFC để lập trình. S1, S2, S3, và S4 tương đương với trạng thái 1, 2, 3, và 4. T1 (transion 1) tương ứng với chuyển tiếp từ trang thái 1 sang trang thái 2 của mô tả Grafcet, tương tự như vậy với các chuyển tiếp T2, T3, T4.

Không ảnh hưởng đến tính tổng quát của bài toán thiết kế an toàn cho giàn khoan, mô phỏng kiểm chứng được thực hiện cho mức nguy hiểm cao nhất là rời giàn ESD-A, các mức nguy hiểm khác hoàn toàn tương tự Kịch bản mô phỏng như ở hình 6 được thực hiện như sau:

- Trường hợp 1, tín hiệu kích hoạt cho mức ESD-A này là tín hiệu lấy từ tủ điều khiển PA/GA có mức logic là 1 tại thời điểm t1, khi có tín hiệu này hệ thống an toàn sẽ thực hiện một loạt các hành động sau: kích hoạt hệ thống báo động (Alarm), đóng tất cả các van đầu giếng của 9 giếng (MSSV), mở hai van xả BDV 1001 và 1002 (kí hiệu trên đồ thị chung cho cả hai van là BDV 1001).

- Trường hợp 2, khi có thêm tín hiệu rò rỉ khí ga (20% LEL) tại thời điểm t2, Alarm vẫn được kích hoạt, giữ nguyên trạng thái của các van MSSV và BDV 1001 đồng thời đóng các van điều khiển của bình tách là SDV 400, LCV 400 và PCV 400, và mở van xả 401. Các van khác như van tiết lưu FV và van điện XY điều khiển các đường khí đóng/mở như các van của bình tách nên coi như [illegible] bình tách hoạt động thế nào thì các van FV [illegible] hoạt động như vậy.

Tại thời điểm t3 có tín hiệu reset thì các van về trạng thái ban đầu, mở van MS[illegible] (mức logic 1), các van xả BDV đóng (về mức [illegible]g), mở van điều khiển bình tách SDV 400, PC[illegible] LCV 400 (mức logic 1)



Hình 6. Kết quả mô phỏng trường hợp khẩn cấp rời giàn.

Sau thời điểm t3 một lần nữa tín hiệu 20%LEL bị kích hoạt khi đó ngay lập tức tín hiệu Alarm lại được kích hoạt và đóng các van của bình tách và mở van xả 401 còn van đầu giếng MSSV và van xả BDV 1001,1002 không thay đổi trạng thái.

-Trường hợp 3: Tại thời điểm t4 có tín hiệu từ nút ấn ảo tại trạm làm việc trong phòng làm việc thì khi đó hệ thống sẽ tác động gộp cả hai trường hợp 1 và 2, tuy nhiên trước đó thì có tín hiệu 20%LEL đã kích hoạt nên trường hợp 2 đã được kích hoạt rồi, chỉ còn trường hợp 1 chưa kích hoạt thì lúc này các van của trường hợp 1 sẽ kích hoạt: van đầu giếng đóng, van xả BDV 1001, 1002 mở.

5. Kết luận

Nghiên cứu trong bài báo đã chỉ ra được khó khăn trong thiết kế hệ thống an toàn trên giàn khoan đang gặp phải, từ đó xây dựng được quy trình thiết kế an toàn bao gồm thiết kế phần cứng và phần mềm theo tiêu chuẩn IEC 61508 part 2 và part 3, hệ thống an toàn sau khi xây dựng xong đáp ứng chuẩn an toàn SIL3 Phần kiểm nghiệm mô phỏng cho thấy hệ thống an toàn đã hoạt động theo đúng thiết kế yêu cầu.

Lời cảm ơn

Nghiên cứu này được tài trợ bởi trường Đại học Bách khoa Hà Nội trong đề tài mã số T2017-PC-098.

Tài liệu tham khảo

[1]. Blesson Joseph Thomas, Jibin Babu, Design of Safety System and Management in Petrochemical Industry, IJRST 2014.

[2] Feng Wang, Yajun Chen, Haochen Wang, Cunyin Chen, Bin Shi, The Intrinsic Safety Engineering Design Method for The Petrochemical Plant, 2012.

[3] Kamarizan Kidam, Markku Hurme, Journal of loss prevention industries 25 (2012), 655-666

[4]. Hale, A., Kirwan, B., & Kjellen, U. (2007a). Editorial Safety Science, 45(1), 3-9.

[5]. Janan Zaytoon, On the recent advances in Grafcet, Production planning and control, 2002, Vol 13, No. 1, 86-100.

[6]. Siemens, Industry Manual, Safety for the manufacturing industry – Functional Safety Services

[7]. Phạm Thanh Huyền, Nguyễn Hồng Liên, Giáo trình Công nghệ tổng hợp hữu cơ- hóa dầu, nhà xuất bản khoa học kỹ thuật 2006

[8]. Charles H. Roth, Jr, Fundamentals of logic design, 5th edtion, Thomas Learning 2003.

[9]. Randy H. Katz., Text book: Contemporary logic design, second edition, Prentice Hall 1993.