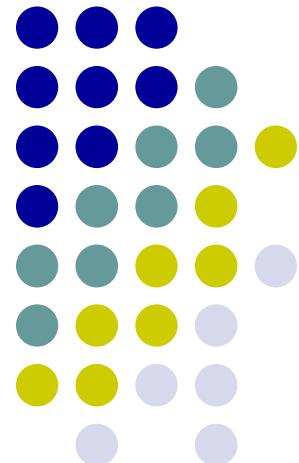
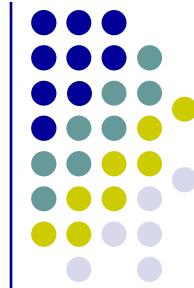


# Thiết kế tổng thể và Thiết kế kiểm soát

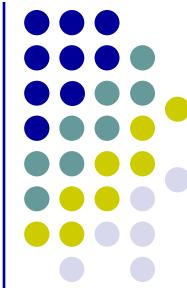
---





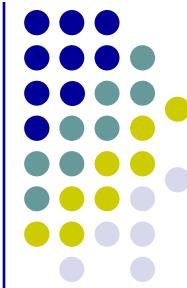
# NỘI DUNG

- **Tổng quan giai đoạn thiết kế**
  - Tài liệu đầu vào và nhiệm vụ
  - Các phần thiết kế
- **Thiết kế tổng thể**
  - Phân định công việc thủ công – máy tính
  - Hoàn chỉnh DFD hệ thống
- **Thiết kế kiểm soát**
  - Thiết kế bảo vệ hệ thống
  - Thiết kế bảo mật dữ liệu



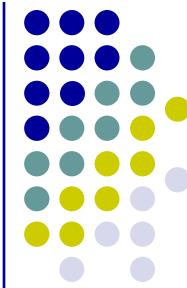
# TỔNG QUAN

- Tài liệu đầu vào
  - Tài liệu phân tích hệ thống  
BFD, DFD, P-Spec, RM, D-Spec.
  - Từ điển dữ liệu
  - Mô tả yêu cầu sử dụng dữ liệu  
loại, số lượng, vị trí, thời gian, cách dùng
  - Mong đợi của người dùng  
về sử dụng, tích hợp dữ liệu
  - Mô tả công nghệ và thiết bị sử dụng  
lưu trữ và quản lý dữ liệu, phương án cài đặt



# TỔNG QUAN

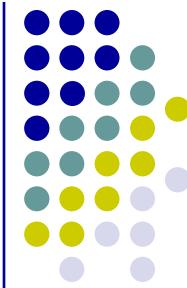
- **Nhiệm vụ**
  - Chuyển mô tả logic thành mô tả vật lý  
biện pháp, phương tiện, cài đặt.
  - Thiết kế logic  
dữ liệu, xử lý, thông tin, ràng buộc
  - Thiết kế vật lý  
cách đưa dữ liệu, xử lý, thông tin, ràng buộc



# TỔNG QUAN

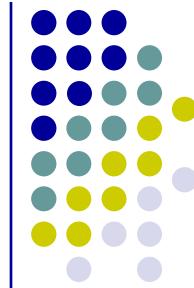
## ● Các bước tiến hành

- Thiết kế tổng thể
  - Ranh giới máy tính – thủ công
  - Hệ con máy tính
- Thiết kế kiểm soát
  - Bảo mật thông tin (quyền truy cập)
  - Bảo vệ hệ thống (hỗn hóc, thất thoát tài sản...)
- Thiết kế cơ sở dữ liệu
  - Biến đổi mô hình lý tưởng thành mô hình thực tế
  - Chi tiết các bảng dữ liệu phục vụ kiểm soát



# TỔNG QUAN

- Các bước tiến hành
  - Thiết kế chương trình
    - Thiết kế kiến trúc
    - Thiết kế xử lý
  - Thiết kế giao diện
    - Thiết kế hệ thống đơn chọn
    - Thiết kế màn hình giao diện
    - Thiết kế tài liệu in



# TỔNG QUAN

- **Các phần thiết kế**

- Thiết kế logic

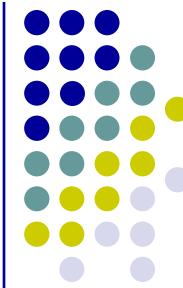
- Mẫu (form), báo cáo (report): nhập/xuất dữ liệu
- Giao diện: môi trường giao tiếp hệ thống – người dùng
- CSDL logic: cấu trúc thông dụng cài đặt trên các hệ

QTCS\_DL khác nhau

- Cơ chế kiểm soát dữ liệu, chương trình

- Thiết kế vật lý

- Tệp CSDL trên máy tính
- Modul chương trình
- Thiết kế CSDL và chương trình phân phối trên mạng



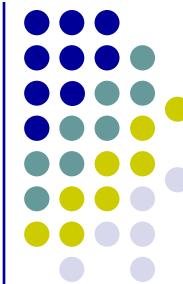
# THIẾT KẾ TỔNG THỂ

## ● Mục đích

- Kiến trúc tổng thể của hệ thống, trong đó
  - Phần việc xử lý thủ công, các thủ tục xử lý thủ công
  - Phần việc máy tính, tiến trình do máy tính thực hiện

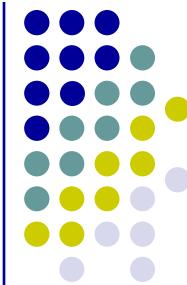
## ● Cách thực hiện

- Phân định công việc thủ công, máy tính
  - Sử dụng DFD tách công việc thủ công – máy tính
  - Kết quả: đường ranh giới thủ công – máy tính
- Hoàn chỉnh DFD hệ thống



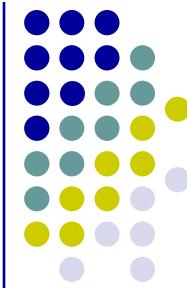
# THIẾT KẾ TỔNG THỂ

- Phân định công việc thủ công – máy tính
  - Cách thực hiện
    - Vạch đường ranh giới (nét đứt) thủ công – máy tính
    - Đối với **tiến trình**:
      - Người xử lý: chuyển sang thủ công
      - Máy xử lý: chuyển sang máy tính
      - Cả máy và người cùng tham gia: **phân rã** thành các tiến trình nhỏ hơn (một mức).
    - Đối với **kho dữ liệu**:
      - **Chuyển sang máy tính**: có mặt trong mô hình dữ liệu
      - **Chuyển sang thủ công**: không có mặt trong MH dữ liệu
        - Các tệp thủ công (sổ sách, bảng biếu...)
        - Hồ sơ, chứng từ văn phòng.



# THIẾT KẾ TỔNG THỂ

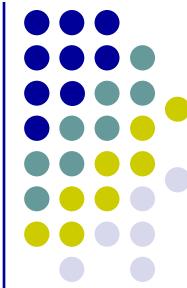
- Hoàn chỉnh DFD hệ thống
  - Mục đích
    - Mô tả **tiến trình** hệ thống thực hiện
      - Phương thức xử lý (theo lô, trực tuyến, thời gian thực...)
      - Đối tượng thực hiện, phương tiện, công cụ sử dụng
      - Nội dung xử lý (thuật toán, công thức)
      - Khi nào thực hiện
    - **Kho dữ liệu** lưu trữ bởi máy tính
      - Sẽ xuất hiện trong mô hình dữ liệu của hệ thống
  - Thực hiện:
    - Diễn tả ý tưởng thiết kế bằng DFD hệ thống



# THIẾT KẾ KIỂM SOÁT

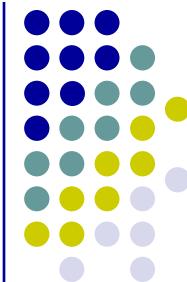
## ● Mục đích

- Tính chính xác (accuracy)
  - Hệ thống làm việc đúng đắn
  - Dữ liệu xác thực
- Tính an toàn (safety)
  - Hệ thống không bị xâm hại khi có lỗi kỹ thuật
- Tính bảo mật (security)
  - Khả năng ngăn ngừa xâm hại từ phía người dùng
- Tính riêng tư (privacy)
  - Quyền riêng tư của các loại người dùng khác nhau



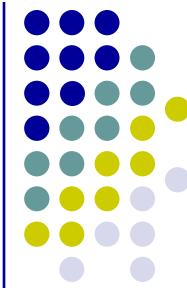
# THIẾT KẾ KIỂM SOÁT

- Các khía cạnh cần kiểm soát
  - Kiểm tra thông tin nhập/xuất
  - Tình huống gián đoạn chương trình
  - Tình huống xâm hại từ con người



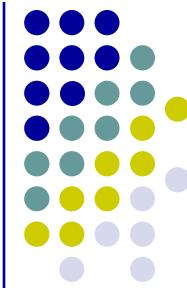
# THIẾT KẾ KIỂM SOÁT

- **Kiểm tra thông tin nhập/xuất**
  - Mục đích
    - Đảm bảo tính xác thực của thông tin
  - Yêu cầu
    - Kiểm tra mọi thông tin nhập/xuất
  - Nơi tiến hành kiểm tra
    - Nơi thu thập thông tin vào
    - Trung tâm máy tính
    - Nơi nhận dữ liệu xuất
  - Nội dung kiểm tra
    - Phát hiện lỗi và sửa lỗi



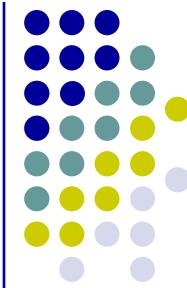
# THIẾT KẾ KIỂM SOÁT

- Kiểm tra thông tin nhập/xuất
  - Hình thức kiểm tra
    - Bằng tay/bằng máy
    - Đầy đủ/không đầy đủ
    - Trực tiếp/gián tiếp
  - Thủ tục kiểm tra
    - Trực tiếp trước
    - Gián tiếp sau



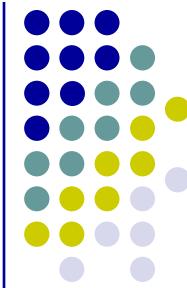
# THIẾT KẾ KIỂM SOÁT

- **Khả năng gián đoạn chương trình**
  - Nguyên nhân
    - Hỗng phần cứng
    - Giá mang tin có sự cố
    - Hỗng hệ điều hành
    - Nhầm lẫn trong thao tác
    - Dữ liệu sai
    - Lập trình sai



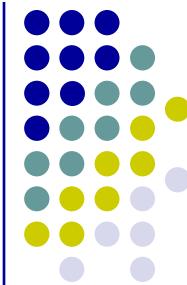
# THIẾT KẾ KIỂM SOÁT

- **Khả năng gián đoạn chương trình**
  - Hậu quả
    - Mất thời gian chạy lại chương trình
    - Mất, sai lạc dữ liệu
  - Cách thức đảm bảo an toàn thông tin
    - Khóa từng phần dữ liệu
    - Tạo các file sao lưu



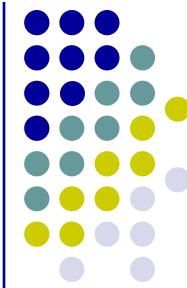
# THIẾT KẾ KIỂM SOÁT

- **Khả năng gián đoạn chương trình**
  - Thủ tục phục hồi chương trình
    - Đưa CSDL trở về trạng thái đúng đắn ngay trước khi bị hỏng vì gián đoạn chương trình.
  - Khi nào dùng thủ tục phục hồi
    - Giá mang của tệp có sự cố
    - Hỗng môi trường máy tính
    - Hỗng hệ điều hành
    - Thực hiện sai quy định của hệ điều hành
    - Lỗi lập trình
    - Nhầm lẫn trong thao tác



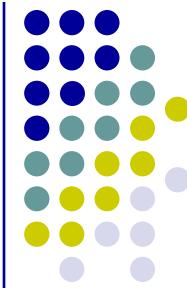
# THIẾT KẾ KIỂM SOÁT

- **Khả năng gián đoạn chương trình**
  - Nguyên tắc hoạt động của thủ tục phục hồi
    - Sao lưu định kỳ
    - Khi có sự cố gián đoạn
      - Đọc các giá trị cuối cùng của các biến mốc
      - Định vị lại đầu đọc các file đang dùng
      - Xử lý một số lỗi trên các file vận động
      - Khởi động lại chương trình từ chỗ bị ngắt.



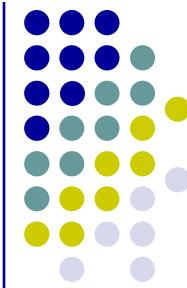
# THIẾT KẾ KIỂM SOÁT

- **Khả năng gián đoạn chương trình**
  - Vấn đề cân nhắc khi sử dụng thủ tục phục hồi
    - Thời gian bị mất do phục hồi
    - Chương trình không bắt đầu lại được khi đã gián đoạn
      - Xử lý theo mẻ có thể bắt đầu lại
      - Xử lý trực tuyến không thể bắt đầu lại
    - Tính phức tạp và các ràng buộc về khai thác
    - Cần thêm thiết bị ngoại vi.



# THIẾT KẾ KIỂM SOÁT

- **Xâm hại từ con người**
  - Các hình thức xâm hại
    - Vô tình: nhầm lẫn, tò mò không ác ý
    - Cố ý: tấn công hệ thống nhằm
      - Lấy cắp dữ liệu
      - Phá hoại dữ liệu
      - Gây các quyết định sai lạc
      - Gây thất thoát, lãng phí tài sản

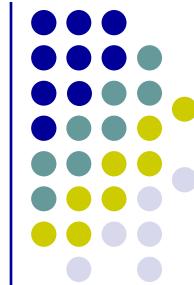


# THIẾT KẾ KIỂM SOÁT

## ● Xâm hại từ con người

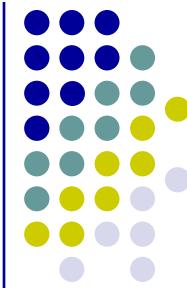
### ● Mục đích bảo vệ

- **Bảo vệ tính bí mật:** thông tin không bị lộ
- **Bảo vệ tính toàn vẹn:** ngăn chặn việc tạo và thay đổi bất hợp pháp hoặc phá hoại dữ liệu
- **Bảo vệ tính khả dụng:** người dùng hợp pháp không bị từ chối truy nhập.
- **Bảo đảm tính riêng tư:** các tài nguyên không bị sử dụng bởi các cá nhân không có quyền hoặc theo các cách không hợp pháp.



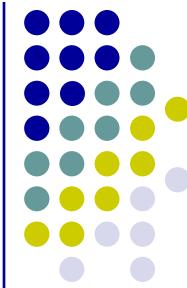
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Hai loại giải pháp
    - Liên quan đến phần cứng
      - Biện pháp vật lý: chống hư hỏng vật lý: bảo vệ ổ ghi dữ liệu, bảo vệ máy in...
      - Sử dụng thiết bị đi kèm bảo vệ phần cứng
    - Liên quan đến phần mềm và tổ chức dữ liệu
      - Tổ chức các hệ lưu trữ dự phòng
      - Tổ chức kiểm soát truy cập
      - Mã hóa thông tin trên đường truyền



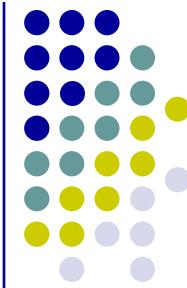
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Các giai đoạn thiết kế kiểm soát
    - Xác định các điểm hở của hệ thống
    - Xác định các kiểu đe dọa có thể xảy ra
    - Xác định các trạng thái phát sinh đe dọa
    - Lựa chọn thiết kế kiểm soát



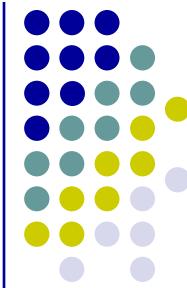
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Xác định các điểm hở yếu của hệ thống
    - Dữ liệu trên đường truyền từ nơi lưu trữ đến nơi sử dụng
      - Luồng dữ liệu từ DFD đi tới một tác nhân ngoài
      - Luồng dữ liệu đi từ máy tính sang người sử dụng
    - Thông tin trao đổi qua giao diện
    - Nơi lưu trữ thông tin



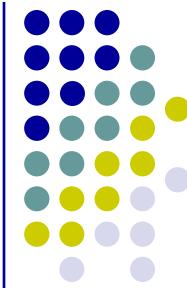
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Các kiểu đe dọa có thể xảy ra từ điểm hở
    - Ăn cắp thông tin và tài sản
    - Thất thoát tài sản
    - Quyết định sai
    - Tốn kém, lãng phí
    - Lộ bí mật
  - Đánh giá đe dọa
    - Xác định trạng thái đe dọa (Khi nào? Tình huồng nào?)
    - Mức độ thiệt hại (Cao, vừa, bình thường)



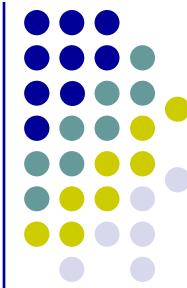
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Xác định trạng thái phát sinh đe dọa
    - Bước 1: Xác định tình huống đặc biệt phát sinh đe dọa
      - Sử dụng DFD hệ thống
    - Bước 2: Đánh giá xác suất xảy ra đe dọa
      - Cao: tình huống có thể xuất hiện một cách đều đặn và tương đối thường xuyên
      - Vừa: tình huống có thể xuất hiện nhưng không thường xuyên và không đều đặn
      - Thấp: sự kiện hầu như không xuất hiện nhưng cũng có khả năng đó.



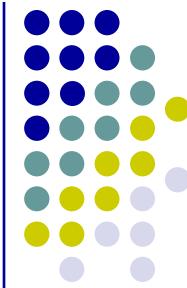
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Lựa chọn giải pháp kiểm soát hệ thống
    - Xác định điểm hở và đe dọa cần kiểm soát.
      - Khả năng kiểm soát: về kỹ thuật, về tài chính
      - Chi phí hiệu quả
    - Câu hỏi phải trả lời khi thực hiện yêu cầu
      - Điểm hở có cần kiểm soát không ?
      - Những đe dọa gì ở những điểm hở cần kiểm soát ?
      - Sử dụng biện pháp nào ?
      - Tổng chi phí cho kiểm soát ?



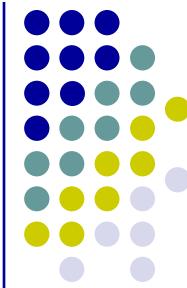
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Lựa chọn giải pháp kiểm soát hệ thống
    - Các biện pháp bảo mật
      - Bảo mật vật lý
      - Nhận dạng nhân sự
      - Mật khẩu
      - Mật mã
      - Bảo mật bằng gọi lại
      - Tường lửa



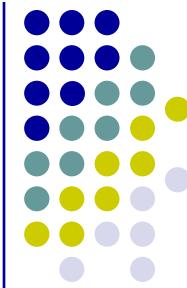
# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Lựa chọn giải pháp kiểm soát hệ thống
    - Phân biệt quyền riêng tư
      - Mức thấp: mỗi người một mật khẩu truy cập
      - Mức vừa: phân loại người dùng và gán mỗi loại người dùng một số quyền nhất định
      - Mức cao: sử dụng nhiều tầng truy cập



# THIẾT KẾ KIỂM SOÁT

- Xây dựng giải pháp kiểm soát hệ thống
  - Lựa chọn giải pháp kiểm soát hệ thống
    - Đối với dữ liệu
      - Quyền cơ bản: CERD (Create, Edit, Read, Delete)
      - Quyền nâng cao: Expand(thêm thuộc tính), Drop (xoá file), Index (tạo chỉ mục)
    - Đối với chương trình
      - Quyền truy cập: có thể thi hành (Run)



# THẢO LUẬN

- Quy trình thiết kế tổng thể
- Các công việc thiết kế kiểm soát

