ROCKWELL AUTOMATION
& AUTOMATION WORLD

SAFETY
AUTOMATIONFORUM™

# Integrating Machine Safety for OEMs and Manufacturers

Craig Dickson
Operations Manager



Allen-Bradley • Rockwell Software

Rockwell Automation

# Safety Comes Naturally ?

# Safety System Design Goals and Challenges

**Goal:**

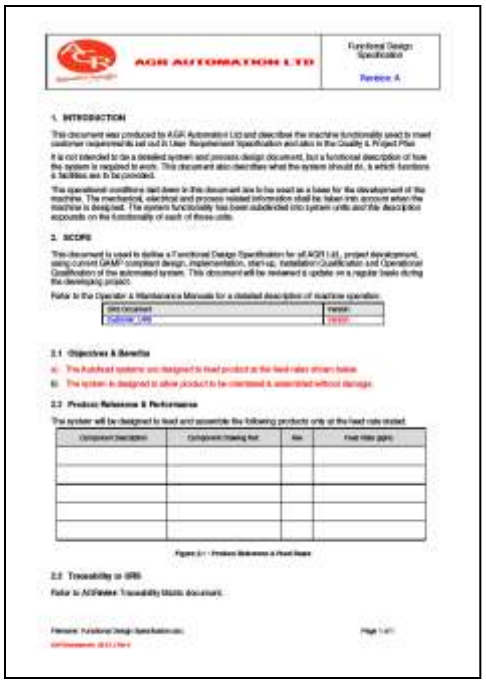
The process of specifying and selection of control systems to deliver automated machinery complying to ISO 13849-1:2006 / IEC 62061

**Challenge:**

- Deliver a compliant system without compromising the production capability and flexibility of the overall system.
- Deliver a system with capability for expansion and upgrading.
- Deliver a system with global support capability
- Deliver a system with adaptability and scalability

# The Process - Steps 1 - 3

1. Completed URS (User Requirements Specification) from the client.
2. FDS (Functional Design Specification) written by AGR and submitted to the client for approval
3. Completion of mechanical concept design, hardware and process specifications, (utilizing GAMP 5 Guidelines)


AGR AUTOMATION LTD

Functional Design Specification

Revision: A

1. INTRODUCTION

2. SCOPE

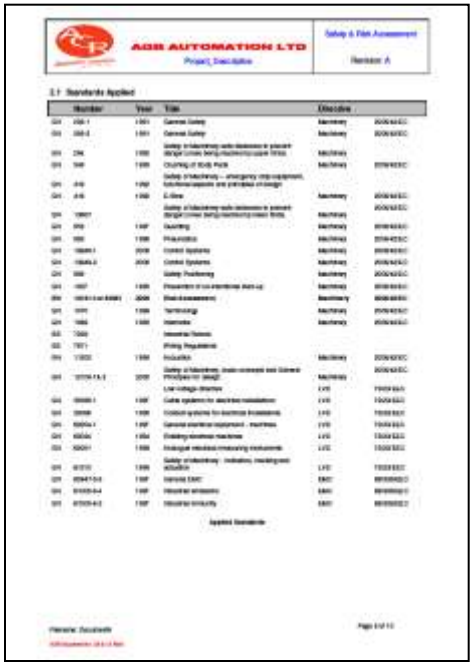
2.1 Objectives & Benefits

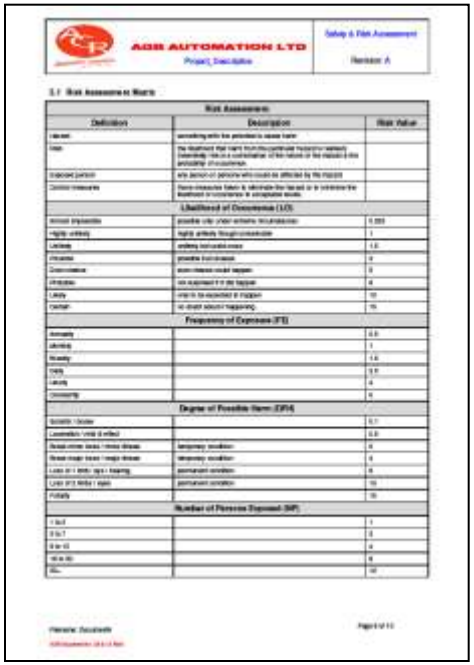
2.2 Product Reference & Performance

2.3 Traceability to URS

# The Process Cont.- Steps 4 - 7

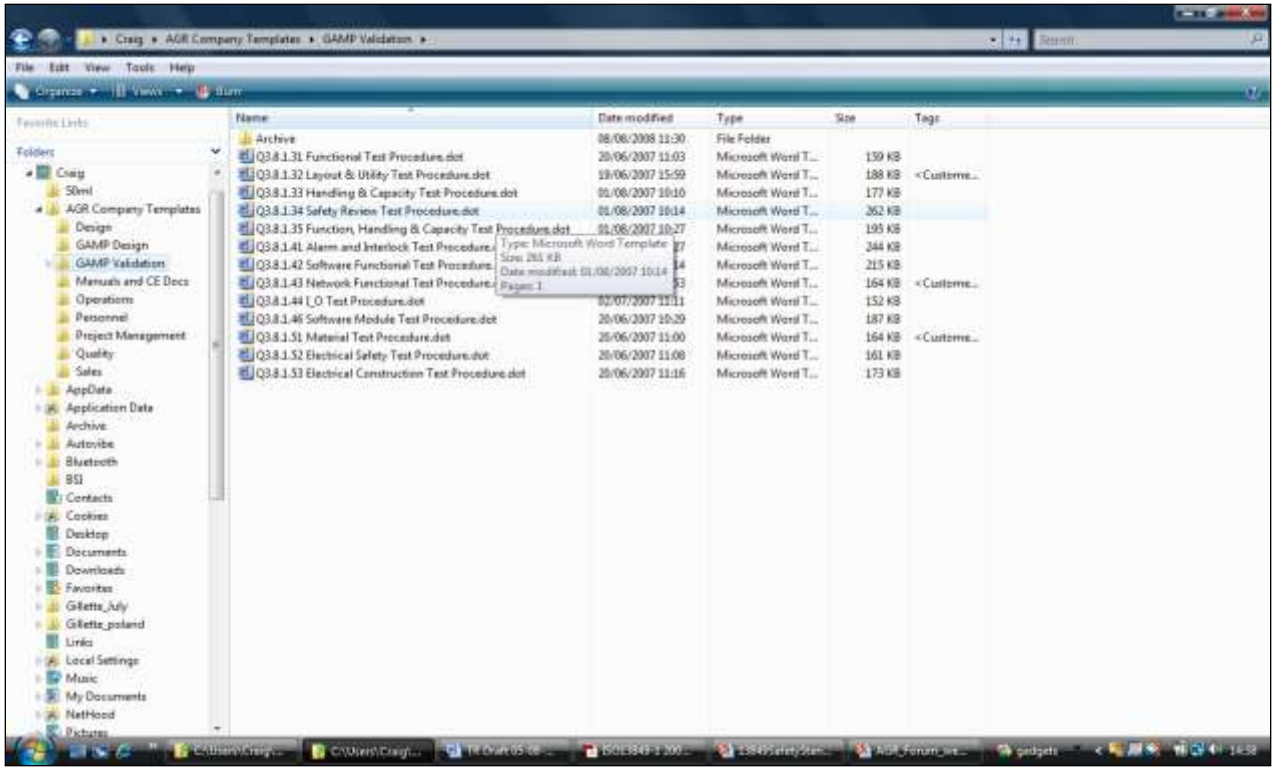
4. Mechanical design concept review meeting and process failure and risk analysis
5. Specification of electrical control equipment, software and safety platform
6. Control hardware and software review meeting and development of FMEA (failure mode and effects analysis



# The Process Cont.- Steps 7 - 9

7. Application of a Safety Risk Assessment and FMEA in determining safety category (Category or PL)
8. Completion of programming of process software modules in PLC and safety PLC
9. Testing and validation of process and safety systems



# Extract of Simple Process Risk Assessment

**Table A.19 — Example of a completed hybrid method form**

**Risk assessment and protective measures**

Document No.: 684
Part of doc. No: 672

Product: Oscillating drive
Issued by: Johnny Persson
Date: 2003-03-17

Black area = Safety measures required
Grey area = Safety measures recommended

☐ Pre risk assessment
☒ Intermediate risk assessment
☐ Follow up risk assessment

| Consequences | Severity Se | Class Cl (Fr+Pr+Av) 3 - 4 | 5 - 7 | 8 - 10 | 11 - 13 | 14 - 15 | Frequency Fr | Probability Pr | Avoidance Av |
|---|---|---|---|---|---|---|---|---|---|
| Death, losing an eye or arm | 4 | | | | | | ≤ 1 h 5 | very high 5 | |
| Permanent, losing fingers | 3 | | | | | | > 1 h to ≤ 24 h 4 | likely 4 | |
| Reversible, medical attention | 2 | | | | | | > 24 h to ≤ 2 w 3 | possible 3 | impossible 5 |
| Reversible, first aid | 1 | | | | | | > 2 w to ≤ 1 y 2 | rarely 2 | possible 3 |
| | | | | | | | > 1 y 1 | negligible 1 | likely 1 |

| Ser. No. | Hzd. No. | Hazard | Se | Fr | Pr | Av | Cl | Protective measure | Adeq. safe |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | Shock from live parts | | | | | | | Yes |
| 2 | 1 | Finger crushing | 3 | 4 | 2 | 3 | 9 | Interlocking guard | |
| 3 | 1 | Finger between moving pin and | 2 | 3 | 2 | 3 | 8 | Interlocking guard | |
| | | frame | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Comments to ref. No.

| | |
|---|---|
| 2 | Finger crushing between belt and belt pulley |
| | |
| | |
| | |

# Influencing factors in Determination of Hardware and Software Selection

1. Category or SIL level requirement
2. System size/ footprint
3. System complexity
4. Process complexity
5. Zoning requirements
6. Smart or dumb safety monitoring
7. Cost

# System Complexity

- Achieving CAT 3 on small simple systems can be cost effective and relatively easily achieved without the use of a safety PLC
- Achieving CAT 3 on a complex system is more difficult but can be made simpler by utilizing a safety PLC. This option offers the functionality to achieve the CAT3 level without a loss of performance from the Automation System.
- Utilizing the safety PLC also delivers a scalable solution easily and quickly modified when system upgrades are applied.

# Complex Automation Employing Safety PLC

Complex Zoned Automated Assembly System

HMI Displaying Zoning

Master PLC with Safety PLC fitted

Distributed Safety I/O

# SmartPod – Multi-Disciplined

AGR Automation

- Multi-Disciplined Manufacturing
- Assembly
- Quality
- Profiling
- Gluing
- Utilising the Rockwell Control Platform

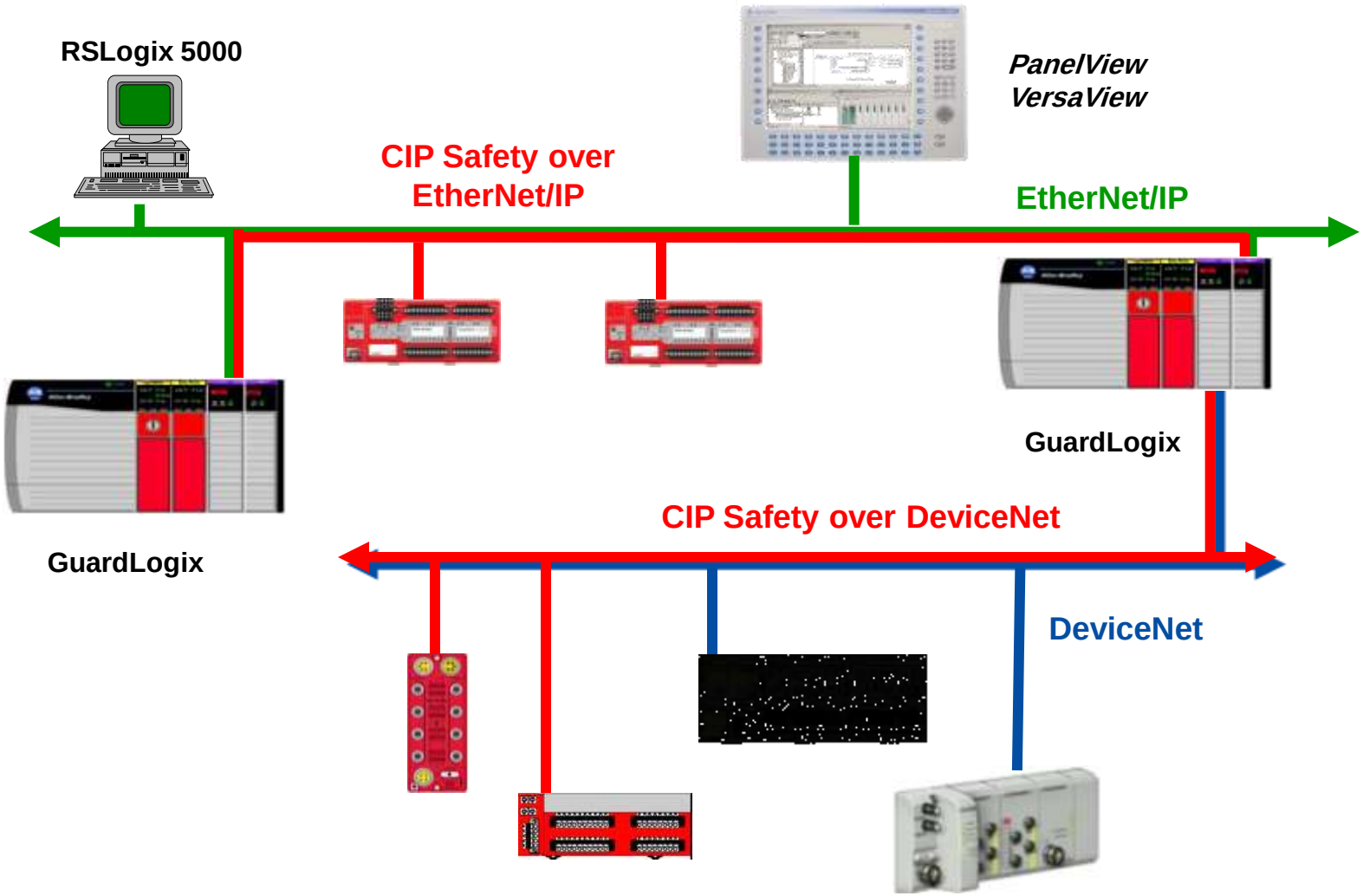
Rockwell Automation

- Multi-Disciplined Control
- Sequential Control
- Motion Control
- Drives Control
- Process Control
- AND Safety Control on the same platform

# Machine Safety and Machine Development

- **Safety LifeCycle**
  - Safety is an integral part of the machine design process
- **Functional Safety**
  - The concept of functional safety is changing the behavior of users and designers of automation systems
  - Functional safety standards are no longer national, but international i.e. IEC 62061
- **Automation**
  - Today's standards now allow safety systems to adopt state of the art technology
- **Integration**
  - The better safety is integrated into the control system, the more in-control a machine is, the safer it is.
- **Quality and compliance**
  - Increased data access and logging through an information enabled platform allow an easier route to confirm quality and compliance of product

# GuardLogix Architecture



# SmartPod – Information Enabled

- Standard and safety messaging on the same network
- Transparent and seamless access to standard and safety information throughout the complete network
- Allows for increased diagnostics and hence improved OEE as the ability to identify problems are greatly increased
- Easily accessible information allows for condition monitoring, historical trending, etc, to be carried out
- The trend in safety is moving from reactive to predictive, and an integrated information enabled machine allows for additional permissive signals from air/oil pressure, etc, to be used in a safety routine

# One Platform now does it all

- Standard control and safety control in one controller
- Standard controllers and safety controllers in a common chassis
- Standard control and safety control on common networks

# SmartPod – Flexible Modular Platform

- Modular design allows flexibility, future proofing, commonality, etc
- Spares are standard off the shelf and globally available

## AGR Automation

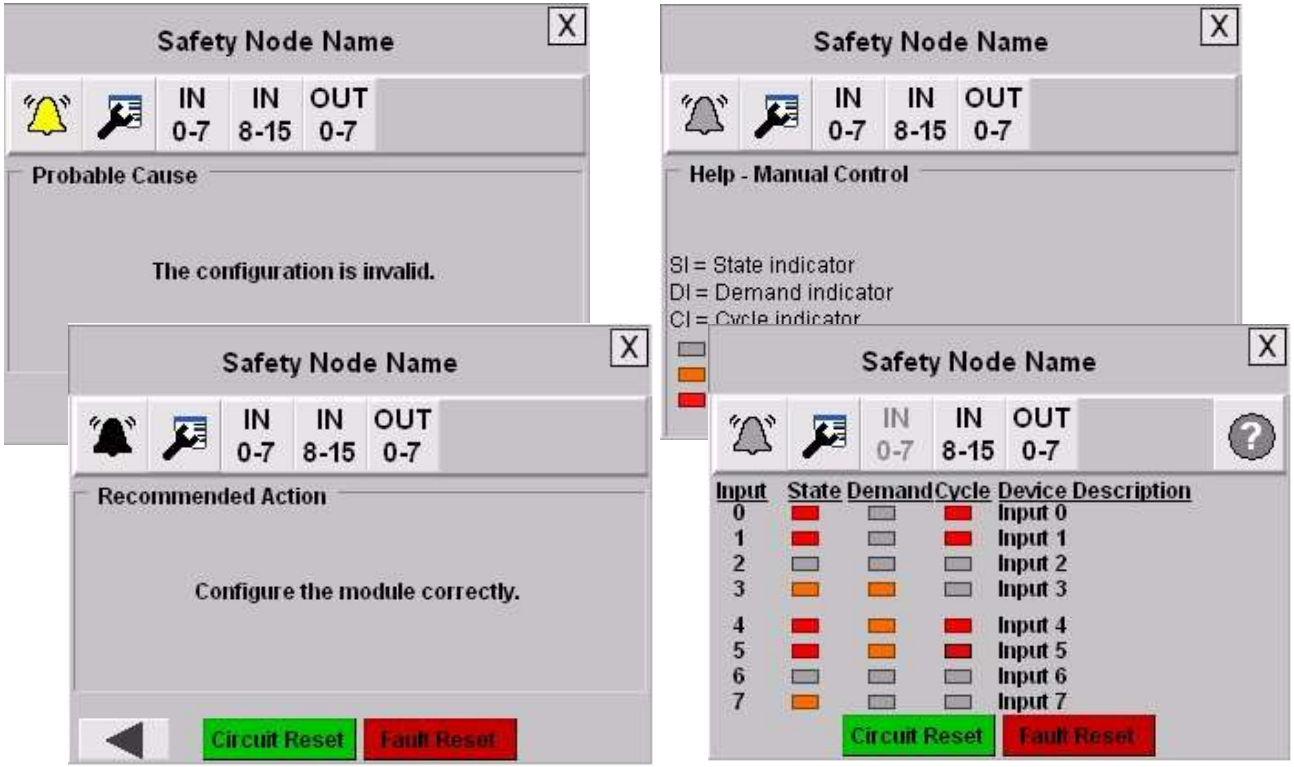
- Modular design of SmartPod allows unrivalled flexibility and saleability for the end user

## Rockwell Automation

- Expandable utilizing DeviceNet or Ethernet connectivity

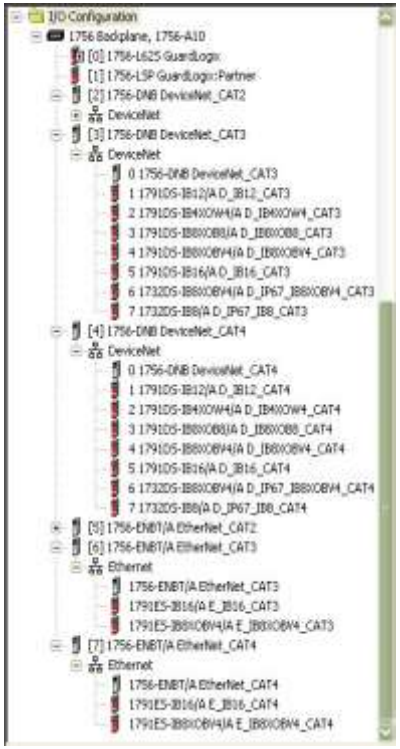
# IA Accelerated - Safety

- Faceplates to speed HMI screen development and commonality
  - Safety I/O faceplates
  - Safety Instruction faceplates

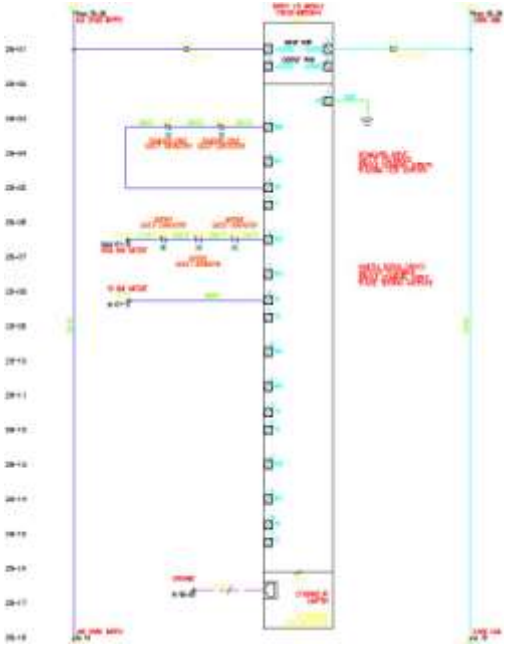


# IA Safety Accelerator - System Design Guidelines/Tools

- A suite of safety components that assist in safety Logic, I/O configuration, field device wiring (CAD drawings), HMI Diagnostic Screens.
- A device selection guide based on safety requirements.
- FactoryTalk View Faceplates for GuardLogix Controller and Safety I/O Blocks including companion Logix Add-On Instructions.







# GuardLogix - Summary

- GuardLogix - Safety Integrated Controller
  - Single controller view of standard and safety
  - GuardLogix based on standard Logix technology
- Common Programming / Design / Configuration Tool
  - RSLogix 5000+ safety extensions
  - Standard control via RLL, FBD, SFC, STL and safety control via RLL
- Leverages standard ControlLogix hardware
  - Racks, power supplies, communications
- Certified safety instructions
  - Simplify user application creation
  - Basic library available at release
- Security environment attached to safety

# GuardLogix – Safety PLC

- Reduces engineering efforts
  - Single engineering software RSLogix 5000
  - Less networks and communication between systems
  - Data exchange between standard and safety part using tags
- Reduces maintenance efforts
  - Single network for safety and standard
  - Less training requirements
- Reduces inventory
  - Shares components with ControlLogix
  - Single Network
- Increases diagnostics capability
- Increases flexibility without compromising security

# Summary

- By carrying out the required process steps to ensure the system delivered the required Safety PROTECTION  Level to protect Operators. Machinery and Process.
- The selection of the Hardware and Software Platform met the requirements of flexibility and expandability of the Smartpod Automation Platform.

Delivered

- Future proof flexibility and re-configurability of the Automation system.
- Cost advantages of manufacture, development and re-validation.
- Improved Safety Performance through the life cycle of the automation System

http://hseworld.wordpress.com