



# Patching Off-the-Shelf Software Used in Medical Information Systems

A White Paper written and approved by the  
Joint NEMA/COCIR/JIRA Security & Privacy Committee (SPC)

Approved by NEMA, COCIR, JIRA,  
the Manufacturers Associations for USA, Europe, and Japan

Wolfgang Leetz  
Data Privacy & Information  
Security for Products  
Siemens Medical Solutions

# Security and Privacy Committee (SPC)

---

- Joint effort by NEMA-MII (USA), COCIR-IT (Europe), and JIRA (Japan)
- Mission: Ensure a level of data security and data privacy in the health care sector that
  - Meets legally mandated requirements
  - Can be implemented in ways that are reasonable and appropriate
  - Reduces healthcare costs of compliance
- Scope:
  - All systems, devices, components, and accessories used in medical imaging informatics
  - Not exclusive of other products and expected to be extendable to all equipment that maintains patient identifiable data
- Goal: provide a common understanding and solution for complying with data security and data privacy legislation, currently focusing on the European Community, Japan, and the United States of America

## SPC Efforts & Outcome

---

- Recent jointly-approved white papers ([www.nema.org/medical/spc](http://www.nema.org/medical/spc)):
  - Remote Service Interface – Solution (A): IPSec Over The Internet Using Digital Certificates (including NAT)
  - Identification & Allocation of Basic Security Rules in Healthcare Imaging Systems
  - Defending Medical Information Systems Against Malicious Software
  - Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems
  - Patching Off-the-Shelf Software Used in Medical Information Systems
  
- Active participants in 2004:  
Agfa, GE, Kodak, Konica Minolta, Merge eFilm, Nihon Kohden, Philips, Siemens, and Toshiba

# What you will learn today

---

- Why Patching is Necessary
- The Risk of Patching
- What is Different when Patching Medical Information Systems
- Patch Release Process
- Conclusion

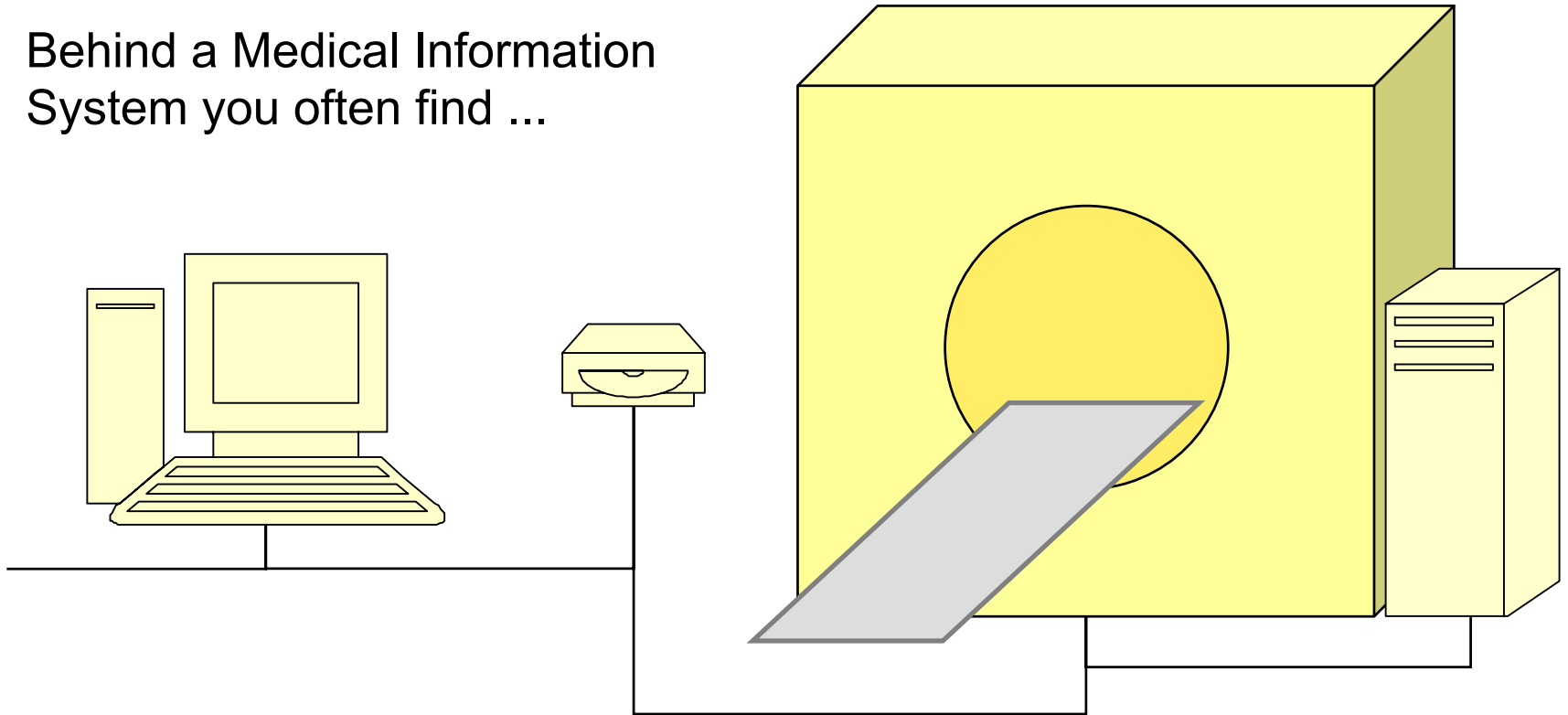
# What We are Talking About

---

- Medical Information Systems (MedIS) – What they are
  - Hospital Information Systems (HIS)
  - Radiology Information Systems (RIS)
  - Cardiovascular Information Systems (CVIS)
  - Picture Archiving & Communications Systems (PACS)
  - Imaging Modalities (CT, MR, Ultrasound, Digital X-Ray)
  - Medical Imaging Workstations
  - Radiation Therapy Systems
  - Patient Monitoring Systems

# Why Patching is Necessary

Behind a Medical Information System you often find ...

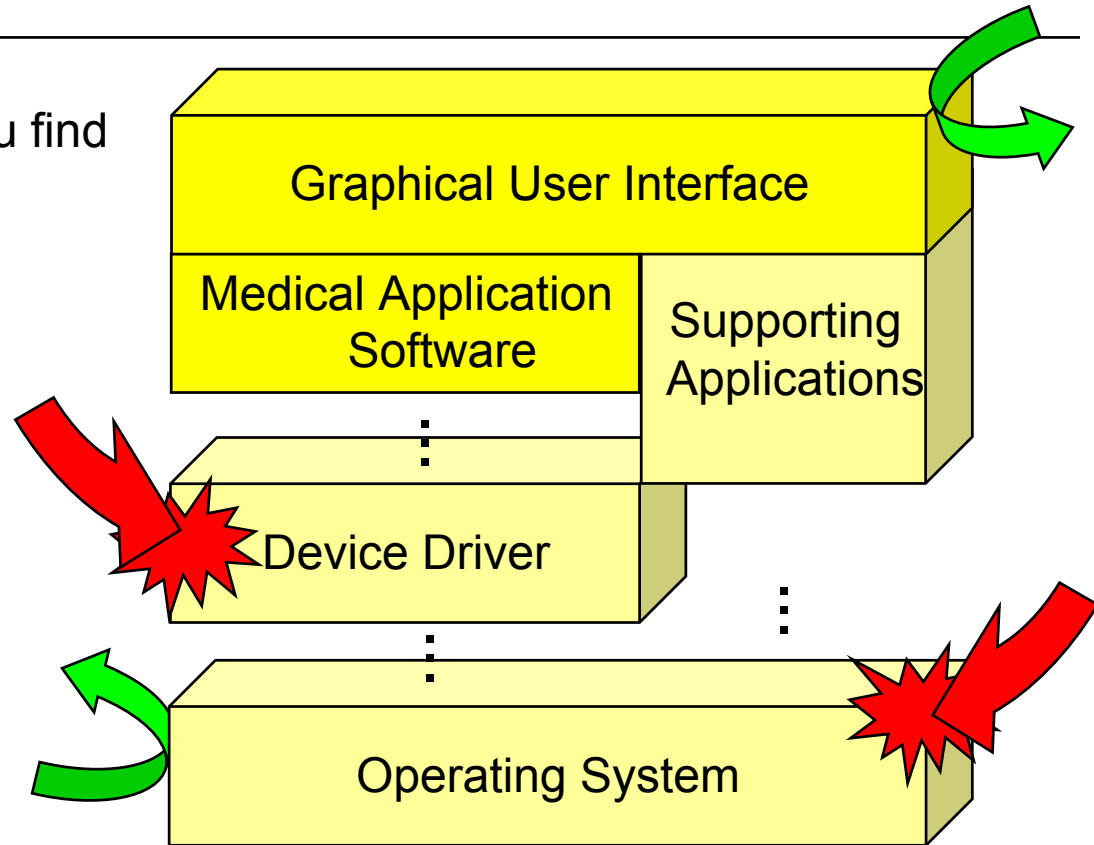
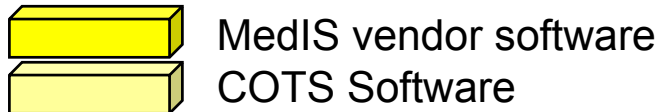


... a simple networked PC.

# Some Possible Threats

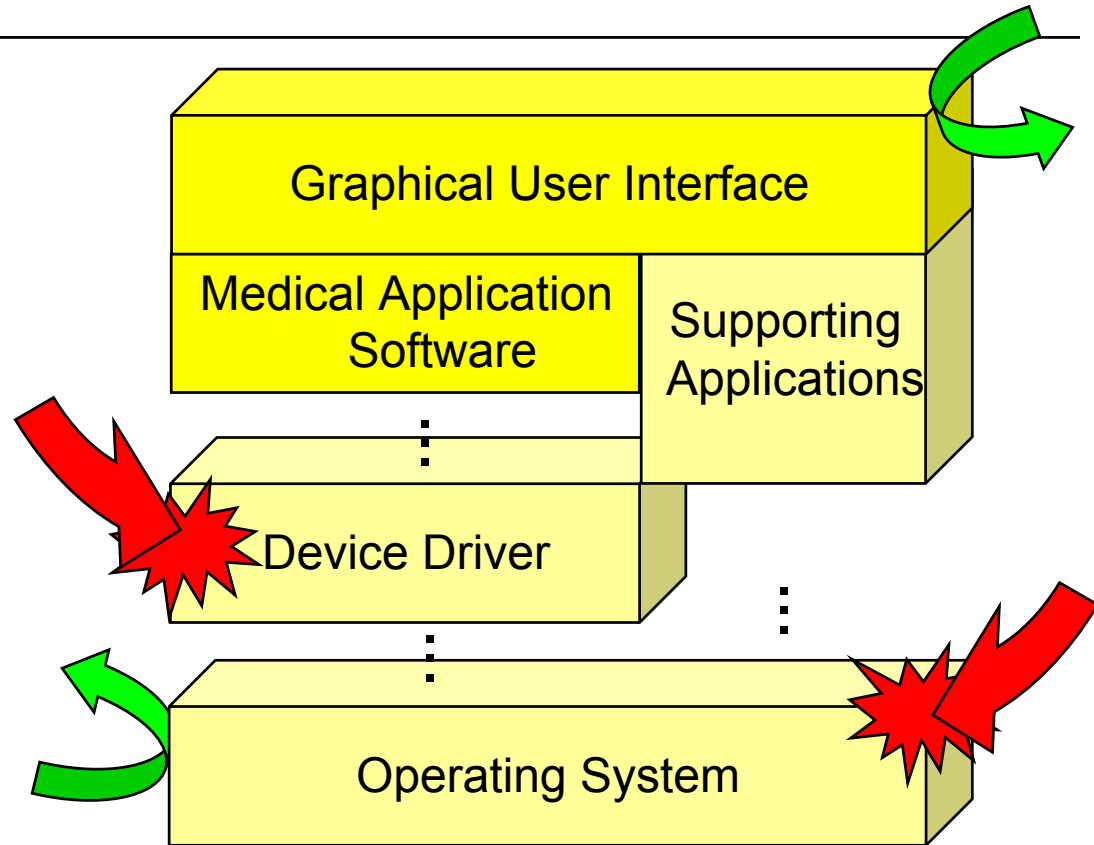
On that „simple networked PC“ you find

- software developed by the MedIS vendor
- software developed by 3rd parties (Commercial Off-the-Shelf (COTS) Software)
- vulnerabilities newly found from time to time
- possible targets for successful malicious attacks



► Vulnerabilities of COTS software may influence the operation of MedIS

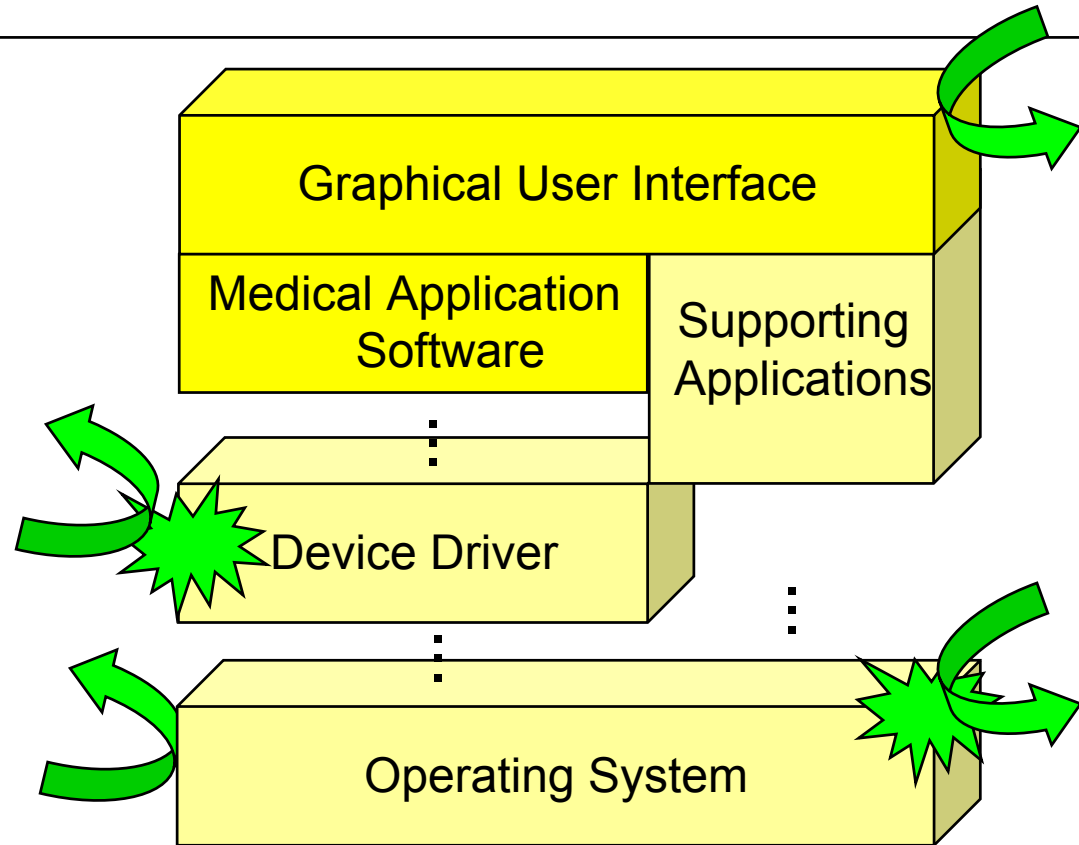
# What COTS Software Vendors Offer



# What COTS Software Vendors Offer

COTS software vendors  
→ offer patches to close vulnerabilities

MedIS users  
→ learn about these patches, e.g. from the daily news  
→ want to apply them to their MedIS as they do to their office applications

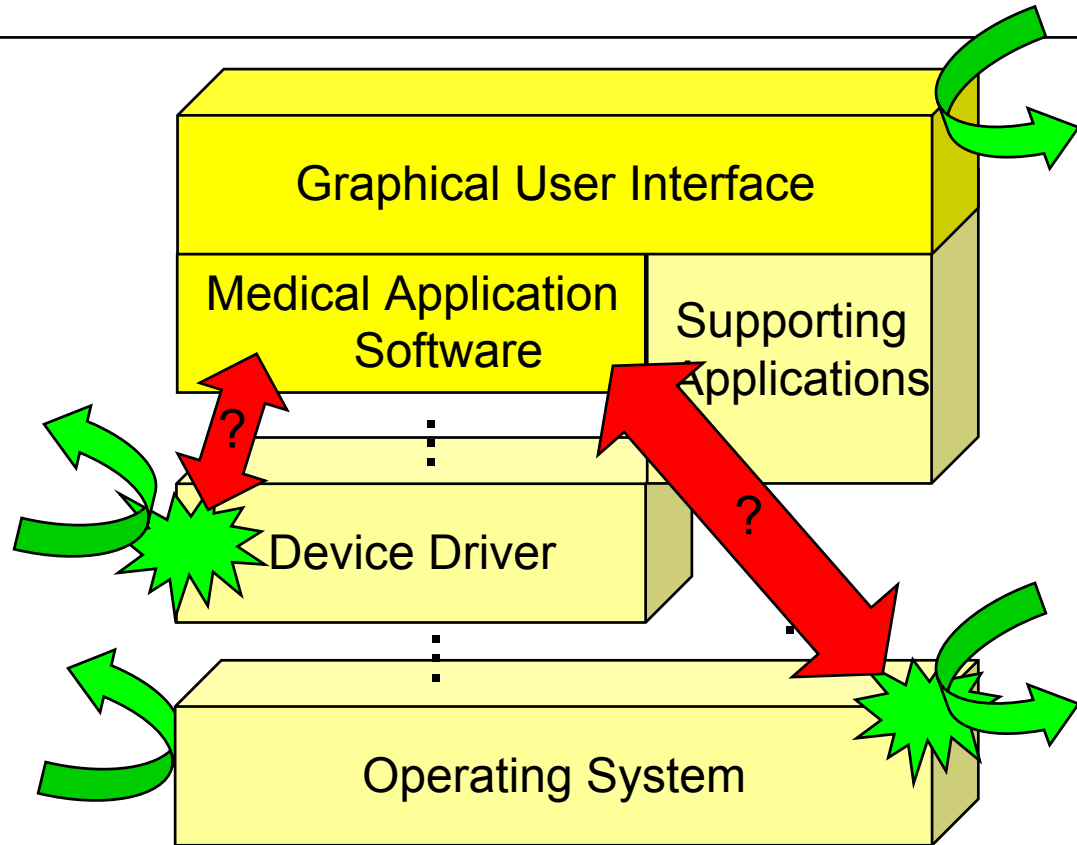


## Why MedIS Users Can't Simply Apply a Patch

COTS software vendors' test procedures do not address the patient safety and effectiveness requirements for MedIS

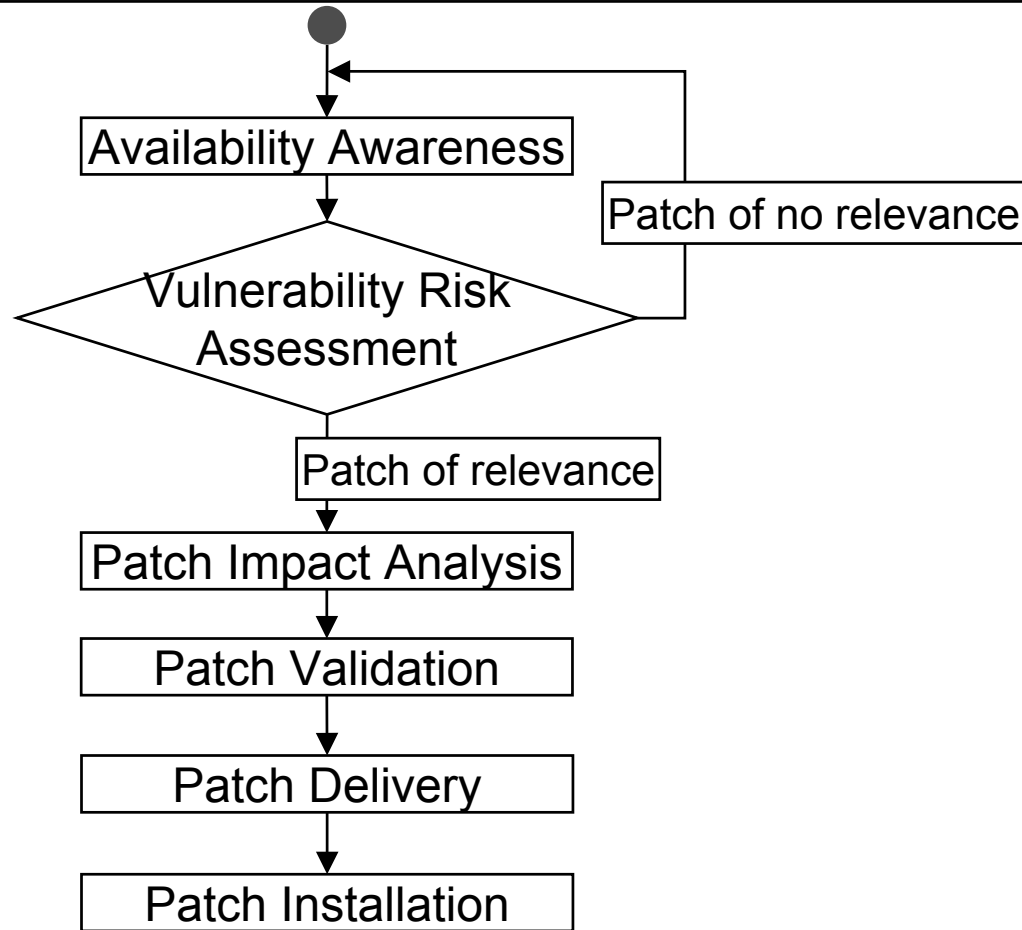
→ Risk of causing problems for the medical application software

→ Testing required to avoid unanticipated side effects of the patch on the MedIS



→ MedIS users must follow different patching procedures to ensure patients receive proper care even after applying a patch

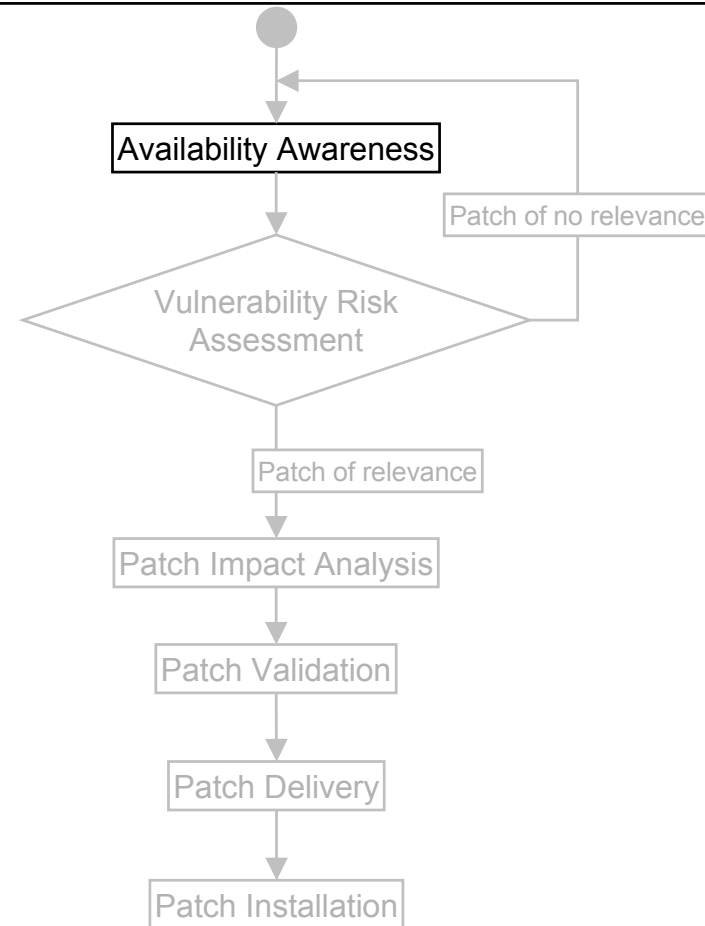
# Needs and Constraints Require the Vendors to Follow a Structured Process



# Patch Deployment

## Step 1: Availability Awareness

- COTS software vendor releases a patch
- MedIS vendors monitor patches for the COTS software their products use
- Users monitor patches necessary for their IT infrastructure



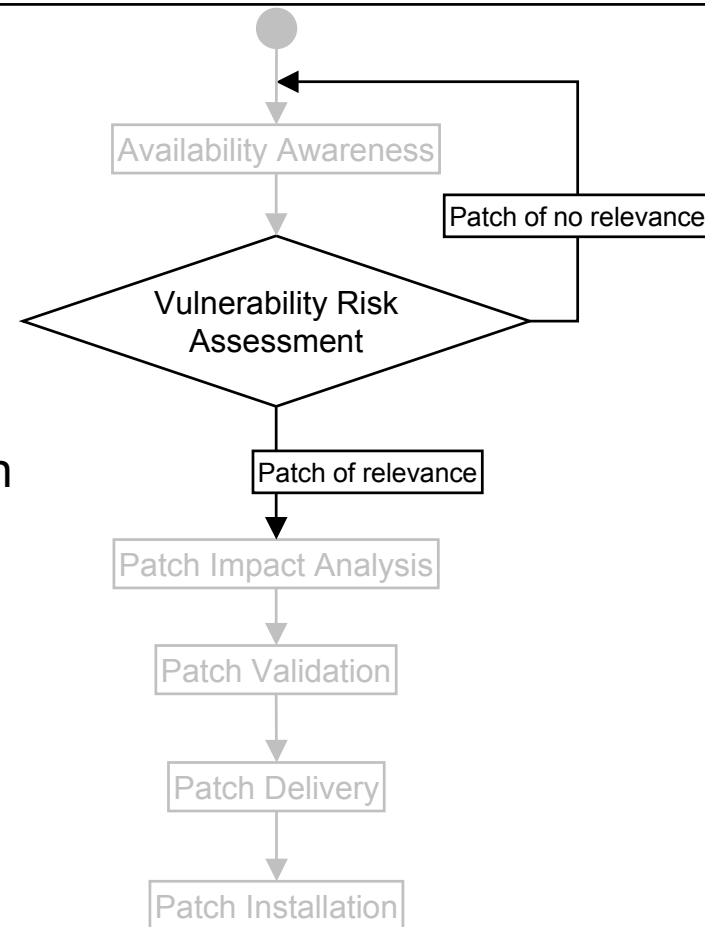
# Patch Deployment

## Step 2: Vulnerability Risk Assessment

- Assessment of the potential risk posed by the respective vulnerability
- Threat level depends on what COTS software is used, e.g. vulnerabilities of uninstalled modules don't add a risk to the MedIS
- Evaluation of the likelihood of exploitation and the impact when exploited

### Results:

- MedIS vendor decides if patch applies and threat is real
- Patches of no relevance won't be issued
- For real threats: proceed to further examination



# Patch Deployment

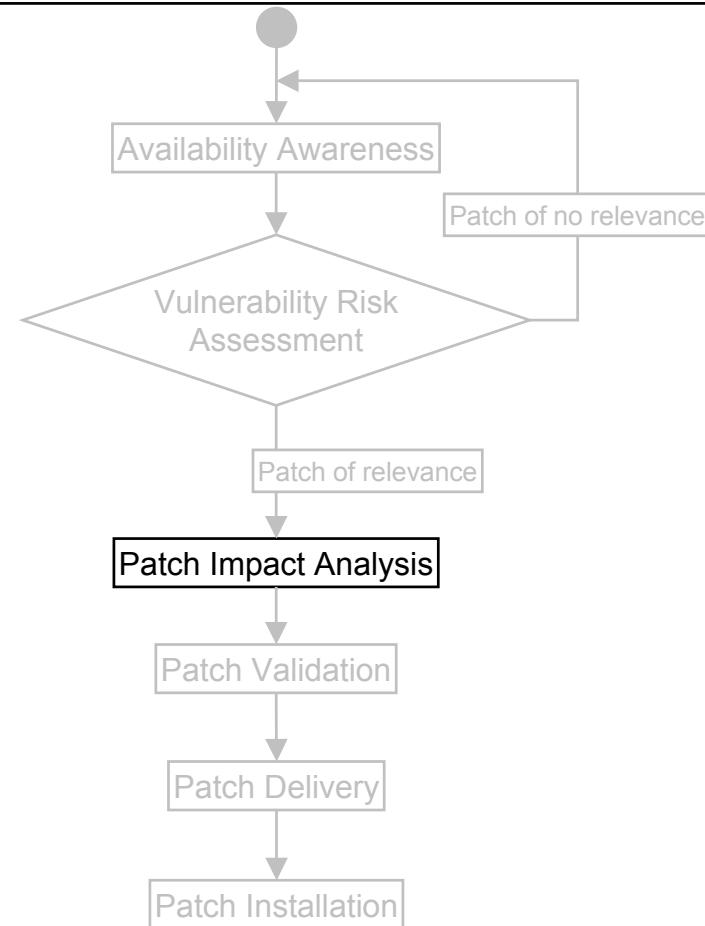
(only for relevant patches)

## Step 3: Patch Impact Analysis

- Understand the impact of the patch on the MedIS

### Results:

- validation strategy
- functionalities that need to be tested



# Patch Deployment

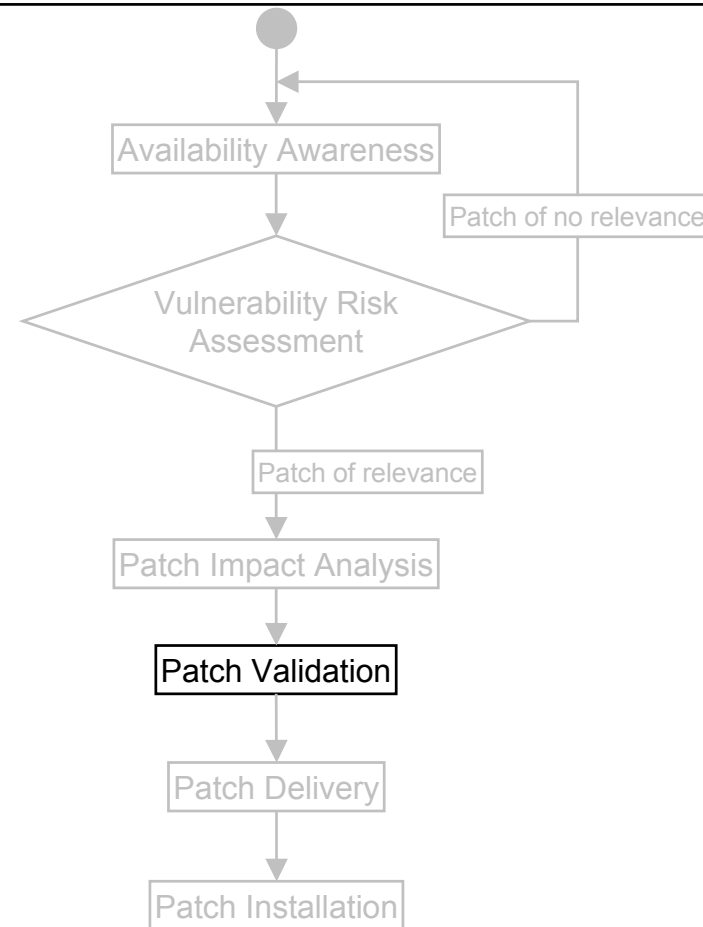
(only for relevant patches)

## Step 4: Patch Validation

- MedIS vendors are ultimately responsible for the approval of patches they provide
- **Formal validation process** follows quality management system and/or relevant regulations

### Required main results:

- Patched MedIS works as intended
- Patch doesn't compromise safety and effectiveness of MedIS
- Patched MedIS still meets legal requirements



# Patch Deployment

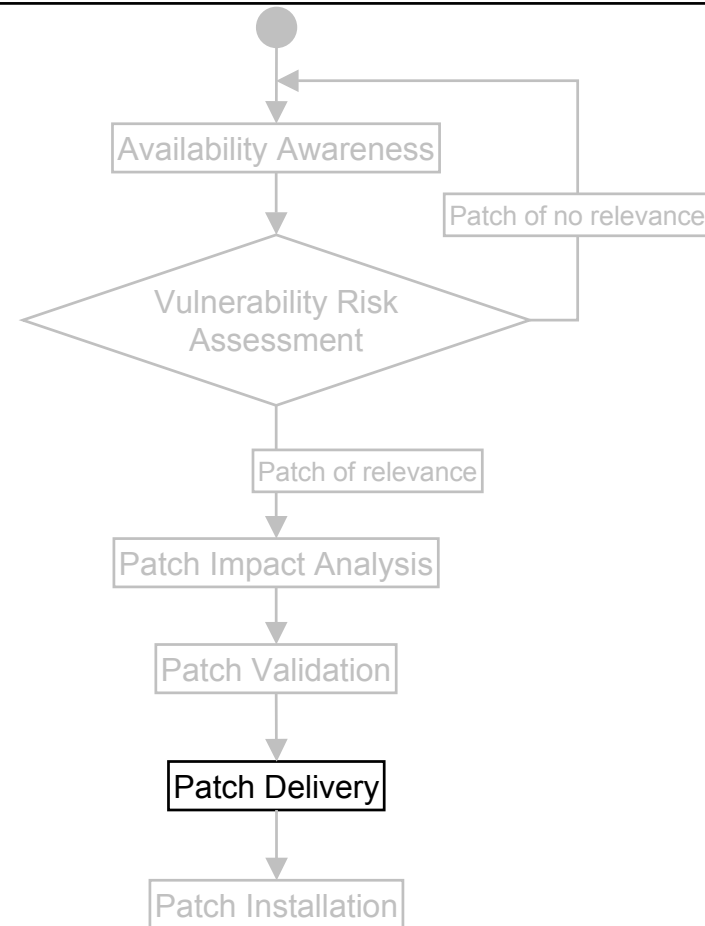
(only for relevant patches)

## Step 5: Patch Delivery

- Must maintain the integrity of the patch
- Must give a clear indication of successful or unsuccessful delivery to the person performing the delivery process

### Result:

- Validated patch is delivered to each relevant MedIS in use



# Patch Deployment

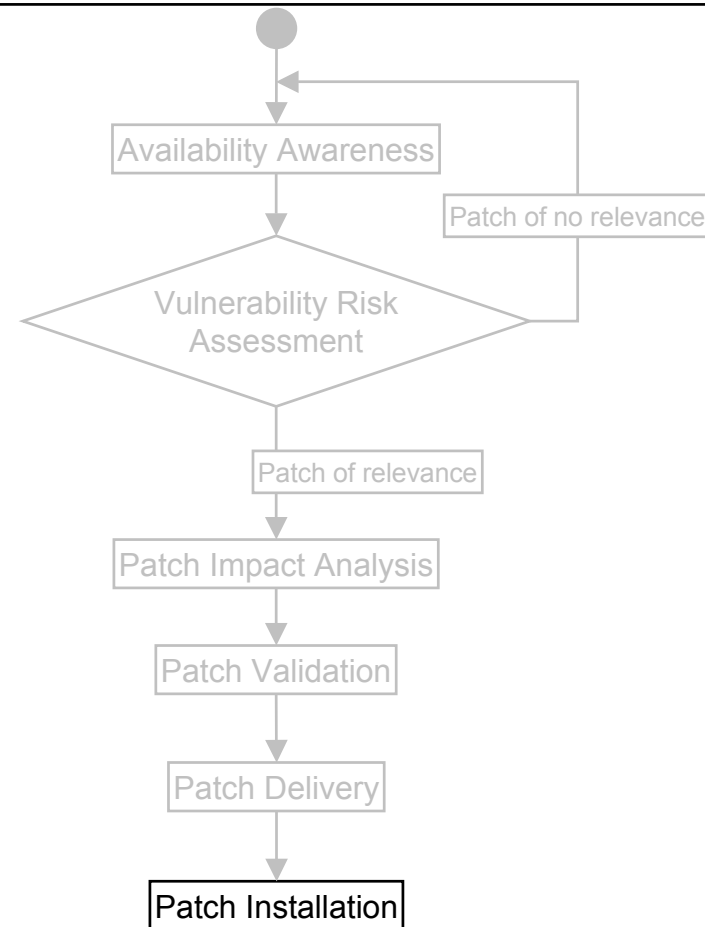
(only for relevant patches)

## Step 6: Patch Installation

- No interference with clinical use of MedIS while installing the patch
- Must give a clear indication of successful or unsuccessful installation
- Confirmation the device is performing as expected

### Main results:

- Newly patched MedIS is protected against specific malicious attacks



## Conclusion (1)

---

- Vendors are aware that users
  - may learn about patches from the daily news
  - expect as fast installation for MedIS as they are used to getting for general purpose IT equipment
- Vendors have specific responsibilities before installing patches
  - recognize the need to offer only safe relevant patches
  - do timely evaluation of patches for a MedIS
  - follow a somewhat time-consuming process to validate a patch
  - abstain from installing a patch that
    - ➔ might compromise patient safety
    - ➔ might impact the operation of a MedIS from doing its required function
    - ➔ is not relevant for security of a MedIS

## Conclusion (2)

---

- Users should develop a risk assessment strategy, including
  - Perform business continuity planning
  - Implement defense in depth strategy
  - Monitor status of active threats
  - Check MedIS patch availability
  - etc.

## For More Information or to Participate

---

- Contact the Secretariat:

Stephen Vastagh

National Electrical Manufacturer's Association

Suite 1847

1300 N. 17th Street

Arlington, VA 22209, USA

E-mail: [ste\\_vastagh@nema.org](mailto:ste_vastagh@nema.org)

Telephone: +1-703-841-3281

[www.nema.org/medical/spc](http://www.nema.org/medical/spc)